Multimed Tools Appl (2015) 74:1725–1739
DOI 10.1007/s11042-013-1714-3

A secure removable visible watermarking for BTC compressed images

Hengfu Yang · Jianping Yin

Published online: 19 September 2013

Abstract A novel removable visible watermarking (RVW) algorithm by combining Block Truncation Coding (BTC) and chaotic map (RVWBCM) is presented in this paper. It embeds a visible watermark in the BTC codes of images, namely both the host image and the watermarked image are BTC compressed images. First, the original image is divided into watermarked region and non-watermarked region, and a predicted version of original image can be obtained by predicting pixel values in watermarked region. Second, adaptive embedding factors are computed according to the image features. Third, the watermark is adaptively embedded into two quantization levels of the BTC compressed image in visible manner. Meanwhile, to further prevent illegal watermark removal, original bi-level watermark is encrypted and then losslessly embedded in invisible manner by adjusting the relationship of two quantization levels. At the receiver's end, only authorized users can exactly extract original bi-level watermark according the relationship of two quantization levels of BTC codes and succeed in remove the embedded visible watermark to reconstruct the original image. The experimental results show that this scheme can achieve a good balance between perceptual transparence and the watermark strength (watermark visibility) and can resist common image processing attacks. The proposed algorithm has low complexity and simplicity of implementation due to the use of BTC. It can be applicable to copyright notification and secure access control in mobile communication.

Keywords Removable visible watermark · Block truncation coding · Chaotic maps · Image smoothness

1 Introduction

Visible watermarking techniques are particular embodiments of digital watermarking [8, 10], which overlay perceptual copyright information on the media in such a way that the watermark

H. Yang · J. Yin
School of Computer, National University of Defense Technology, Changsha 410073, China

H. Yang (✉)
Department of Information Science and Engineering, Hunan First Normal University, Changsha 410205, China
e-mail: hengfuyang@163.com

is intentionally perceptible to human observers but must not significantly obscure the image details beneath it. In addition, the watermark must be hard to remove [13, 15]. A visible watermark can deter attempts of copyright violations, but generally it is designed to be irreversible so as to resist unintentional modifications or malicious attacks [7, 16]. Distortion is unavoidably introduced into the host content during the visible watermark embedding and causes degradation of media. Although the distortion is normally small, there are some applications such as medical imagery, remote sensing, military and law enforcement, where any permanent distortion introduced by watermarking is not allowable. This calls for new visible watermarking techniques called removable [1] or reversible watermarking [11, 17], which can revert to the high quality or exact copy of the original media by removing distortion caused by the watermark embedding.

Hu et al. [6] proposed a user-key-controlled RVW scheme in discrete wavelet transform domain by embedding a visually same but numerical different watermarked versions for different users. Yang et al. [19] proposed a RVW algorithm in discrete cosine transform (DCT) domain where the key dependent preprocessed watermark is adaptively superposed on host image by considering human visual system characteristic of DCT coefficients. Both the two visible watermarking schemes [6, 19] need original watermark during original image recovery. However, the original watermark is not available in some real-time or low-bandwidth environments. Moreover, unauthorized users can obtain an acceptable original image by watermark removal with a tiny different secret key.

Yip et al. [22] presented two lossless visible watermarking algorithms, Pixel Value Matching Algorithm (PVMA) and Pixel Position Shift Algorithm (PPSA). They use the bijective intensity mapping function and circular pixel shift to insert visible watermarks, respectively. Liu and Tsai [9] exploit one-to-one compound mappings for overlaying visible watermarks by mapping image pixel values to those of the desired visible watermarks. Lossless though they are, these algorithms [9, 22] resort to the visible watermark for original image recovery, and have low watermark visibility.

Some lossless visible watermark schemes [5, 18, 20, 23] remove visible watermark overlaying on the cover image and recover original image by embedding some additional information about the watermark and host image with reversible data hiding techniques. But due to the embedded additional information, the visible watermark on the watermarked image produced by these approaches is inevitably blurred in certain and is low visible especially in texture region.

The above-mentioned visible watermarking algorithms do not work in compressed domain and are not suitable for real-life applications via internet. Yeh et al. [21] claimed that a reversible visible watermarking method in JPEG compression domain was proposed, though it inserts the visible watermark in DCT domain rather than compressed domain in fact. Farrugia [2] tries to extend Yang et al.'s scheme [19] to compressed domain. His scheme completely uses the same embedding strategy as Yang et al.'s and inserts the visible watermark in spatial domain, although it adds JPEG compression after watermark embedding and decompression process before watermark removal. Generally, mobile terminals have only limited batteries life, limited memory, and limited computational power. Some complex computation is hard to implement on these portable devices. BTC is a simple and fast compression method with relatively good compression ratio [3]. In order to provide secure and real-time copyright protection for digital media via internet or mobile terminals, a novel RVW algorithm applicable for BTC compressed images is proposed in this paper. The visible watermark image is adaptively added to the BTC compressed image by exploiting the image smoothness and luminance features so that the watermark visibility is good. To prevent unauthorized users from recovering the original BTC compressed image, the watermark is encrypted and then losslessly hidden by modifying the relationship of two quantization levels of BTC codes.

The rest of this paper is organized as follows. The principle of BTC is introduced in Section 2. In Section 3, the proposed RVW scheme is presented. Experimental results are given in Section 4, and finally the conclusion is made in Section 5.

2 Block truncation coding

BTC is a simple compression method based on moment preserving quantization [12]. There are many different variants of BTC in the literature. We embed the visible watermark into absolute moment block truncation coding (AMBTC) compressed images. There are encoding phase and decoding phase in the AMBTC. During the encoding phase, the original image is first divided into non-overlapping blocks of s × s pixels. The pixels in each block are then classified into two groups according to the relationship between their values and the certain threshold, such as the mean value of each block. The pixel values greater than or equal to the threshold are marked as 1's, otherwise denoted as 0's. Meanwhile, a bitmap B is used to record whether a pixel value is less than a certain threshold or not. So the pixel values marked as 1's are grouped into group 1, and others into group 2. The two quantization levels a and b for each block can be computed using means of the corresponding group, and higher mean a and lower mean b are computed as follow.

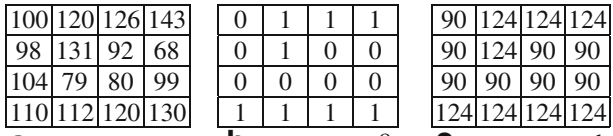
$$\begin{cases} a = \dfrac{1}{q}\displaystyle\sum_{x_k \geq l} x_k \\ b = \dfrac{1}{s*s-q}\displaystyle\sum_{x_k < l} x_k \\ k = 1, 2, \ldots, s \times s \end{cases} . \tag{1}$$

Where $s \times s$ is the total number of pixels in the block and q is the number of pixels greater than the mean l. x_k is the intensity values of the pixels in the block of original image. Finally, each image block is compressed by using two quantization levels a and b, and one binary bitmap B.

In the decoding processing, one can reconstruct image blocks from the compressed code (a, b, B). The corresponding pixels marked as 1's in the bitmap B are reconstructed by the higher mean a, Otherwise, reconstructed by the lower mean b. Figure 1 shows an example of AMBTC coding and decoding procedures. One can notice that the reconstructed AMBTC image blocks will remain the same when interchange two quantization levels a and b, and perform Logical NOT operation on the bitmap B. That is to say, the following equation always holds [4].

$$OP(a, b, B) \equiv OP\left(b, a, \overline{B}\right). \tag{2}$$

where $\overline{B}$ is the result of the logical NOT operation on the bitmap B, and the operator $OP()$ denotes the reconstruction function for AMBTC compressed image blocks.



a original image block (l=107) **b** bitmap (q=8, a=124, b=90) **c** reconstructed image block

Fig. 1 An example of AMBTC

3 Removable visible watermarking scheme for BTC compressed images

In order to achieve fast and secure visible watermarking schemes, this paper presented a new RVW algorithm based on AMBTC. It prevents illegal watermark removal by embedding the encrypted watermark signal into AMBTC codes according to the relationship between two quantization levels in invisible manner, and produces the watermarked image with visible watermark by superposing the visible watermark on two quantization levels. The details of watermark embedding and removing processes are described in the following subsections.

3.1 Visible watermark embedding

During watermark embedding, pixels in compressed image I are overlapped with the corresponding black logo pixels in the watermark W. The overlapped region in image I is the watermarked region called I_c and the other is the non-watermarked region called I_n. Given an AMBTC code C of host image I of $m \times n$ and a binary visible watermark W of $m/s \times n/s$. The flowchart of the visible watermark embedding is illustrated in Fig. 2 and details of the watermark embedding procedure are described as follows.

Step 1: For the sake of simplicity, the visible watermark can be viewed as p-dimensional vectors, where $p=m/s \times n/s$ is also the total number of blocks to be encoded. Read the AMBTC code C of host image I and obtain a sequence of AMBTC code (a_i, b_i, B_i), $i=1, 2, \ldots, p$.

Step 2: Generate a mean array L from AMBTC codes, which have values $l_i = \left\lfloor \frac{q_i a_i + (s \times s - q_i) b_i}{s \times s} \right\rfloor$ in non-watermarked region I_n, otherwise $l_i=-1$, and then an estimated mean image $\widetilde{L}$ is produced from the mean array L by approximating the corresponding pixel values in I_c with the estimated pixel values and the non-watermarked pixel values in their neighborhood. The intensity values $\widetilde{l}_i$ of the estimated mean image $\widetilde{L}$ can be calculated as follows.

$$\widetilde{l}_i = \begin{cases} \left\lfloor \dfrac{q_i a_i + (s \times s - q_i) b_i}{s \times s} \right\rfloor, & block_i \in I_n \\ \dfrac{1}{|O_1| + |O_2|} \left(\displaystyle\sum_{block_j \in O_1} l_j + \sum_{block_j \in O_2} \widetilde{l}_j \right), & block_i \in I_c \end{cases} . \tag{3}$$

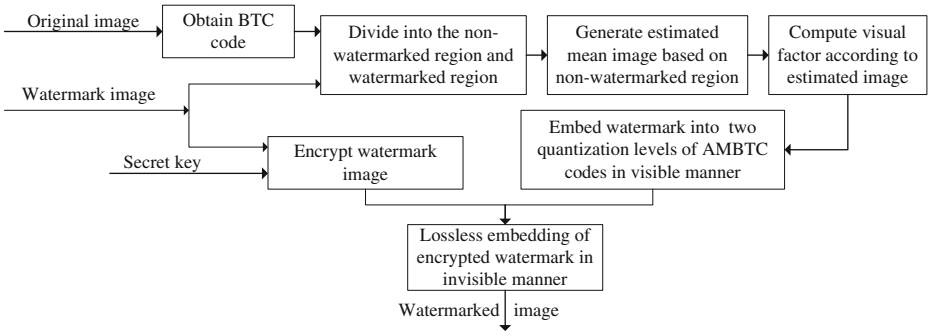


Fig. 2 Fowchart of visible watermark embedding

Where O_1={non-watermarked blocks in the neighborhood of block i}, O_1={watermarked blocks with estimated means in the neighborhood of block i}. The block j belongs to the neighborhood of block i. An R × R neighborhood centered as block i is illustrated in Fig. 3. [•] denotes the round function, |•| operator returns the cardinality of this set, and q_i is the number of 1's in the bitmap of block i. Note that we do not use the information of pixels in the watermarked regions for generating the estimated mean image $\widetilde{L}$. So the identical mean image $\widetilde{L}$ can be obtained from a watermarked image by the receiver for the purpose of watermark removal.

Step 3 Considering the nature of human vision that human eyes are more sensitive to changes in smooth areas of an image than in textured areas, we can compute the block smoothness according to the bitmaps of AMBTC codes as follows.

$$\alpha_i = \frac{|s \times s - 2q_i| + \tau}{s \times s + \tau}. \tag{4}$$

Where τ is a user-defined parameter for avoid zero smoothness factor and division by zero in Eq. (6). The block smoothness α_i will be unchangeable before and after watermark embedding because that watermark insertion does not change the absolute difference of the number of pixels in group 1 and group 2.

The eye is most sensitive to distortion in middle intensity regions and less sensitive to distortion for brighter or darker background. So the luminance factor can be roughly measured by the following equation based on the estimated mean image $\widetilde{L}$.

$$\beta_i = \frac{\left|\widetilde{l}_i - 255/2\right|}{255/2}. \tag{5}$$

Step 4: Based on the above consideration of human visual perception, the visual factor for watermark embedding strength can be written as

$$\gamma_i = \frac{\beta_i}{\alpha_i}. \tag{6}$$

To avoid obtrusive embedding, the visual factor γ is normalized to a narrow range $[r_1, r_2]$ by using Eq. (7).

$$\widetilde{\gamma}_i = \frac{r_2 - r_1}{\max(\gamma) - \min(\gamma)} \times (\gamma_i - \min(\gamma)) + r_1. \tag{7}$$

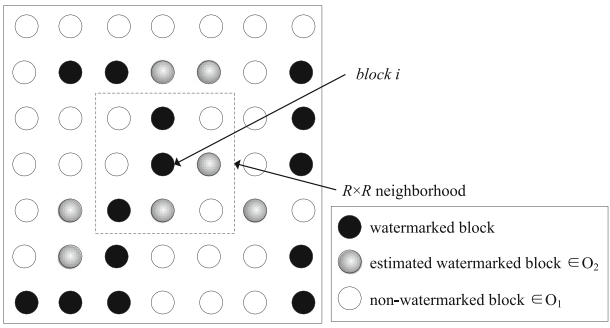


Fig. 3 An $R \times R$ neighborhood centered as block i, where R=3

Where *max*() and *min*() are maximum and minimum functions respectively, and r_1, r_2 ($0<r_1, r_2<1$) are predetermined parameters. It can be seen that the greater the value of the visual factor $\widetilde{\gamma}$, the higher the watermark strength.

Step 5: For each triple (a_i, b_i, B_i), Embed adaptively the visible watermark signal to produce the triple (a_i',b_i',B_i) by modifying the two quantization levels of AMBTC codes according to Eq. (8) as below.

$$t' = \begin{cases} t, & w_i = 1 \\ (1-\widetilde{\gamma}_i)\ \ \rho_1 t + \widetilde{\gamma}_i W_A, & w_i = 0, \widetilde{l}_i >= G_1 \\ \left(1-\widetilde{\gamma}_i\right)\rho_2 t + \widetilde{\gamma}_i(255-W_A), & w_i = 0, \widetilde{l}_i < G_1 \end{cases} \tag{8}$$

Where $t \in \{a_i, b_i\}$, $t' \in \{a_i', b_i'\}$, ρ_1 and ρ_2 are user-defined constants, and $\rho_1 \in [0.5, 1]$, $\rho_2 \in [1, 5.1]$. To achieve good balance between visual quality of stego image and watermark visibility, generally the watermark component $W_A \in [15, 40]$ and gray threshold G_1 is the mean of minimum grayscale and maximum grayscale value. Especially W_A=20 and G_1 is set to 128 in the experiments. This embedding strategy makes the intensity of the visible watermark high and low for dark and light gray background respectively, and ensures good watermark visibility.

Step 6: Use a chaotic logistic map [14]

$$y_{n+1} = \mu y_n(1-y_n). \tag{9}$$

with the secret key key_1 in the open interval (0, 1) as the initial value y_0 to generate a pseudo-random binary sequence $D_1=\{D_1(i)|\ D_1(i)=0, 1, i=1, 2, \ldots, p\}$. And then apply the chaotic map with another secret key key_2 to produce a pseudo-random integer sequence D_2 whose elements have different integer value in the closed interval [1, p]. The bifurcation parameter μ should be chosen from the half-open interval (3.599456, 4) so as to ensure that the logistic map falls in a chaotic state.

Step 7: Perform element-wise XOR operation on two sequences D_1 and W to produce modulated watermark signal W', and then the encrypted watermark W'' can be obtained by scrambling the modulated signal W' using the pseudo-random integer sequence D_2.

Step 8: To prevent illegal watermark removal, the encrypted watermark W'' is losslessly embedded in BTC codes in invisible manner. For each block i with triple (a_i',b_i',B_i), we change the triple (a_i',b_i',B_i) to $\left(b_i', a_i', \overline{B}_i\right)$ if the corresponding encrypted watermark bit w_i''=0. Otherwise, the triple (a_i',b_i',B_i) remains unchanged. So, the lossless embedding strategy can be written as

$$(a_i', b_i', B_i) = \begin{cases} \left(b_i', a_i', B_i\right) & if\ w_i'' = 0 \\ (a_i', b_i', B_i) & else \end{cases}. \tag{10}$$

The entire watermarked AMBTC code stream C' will be obtained when all the encrypted watermark bits are embedded, and finally the watermarked BTC compressed image I_w is generated.

3.2 Visible watermark removal and image recovery

The procedure of removing the visible watermark is roughly the inverse operation of the embedding procedure. Given private keys key_1 and key_2, and the watermarked image I_w, the steps for watermark removal are as follows:

Step 1: Read AMBTC code stream C' from he watermarked image I_w, and get the triple (a_i', b_i', B_i) for each block i.

Step 2: For each triple (a_i', b_i', B_i), extract the encrypted watermark bits according to the relationship of two quantization levels by

$$w_i'' = \begin{cases} 1, & a_i' > b_i' \quad or \quad (a_i' = b_i' \; and \; q_i > 0) \\ 0, & a_i' < b_i' \quad or \quad (a_i' = b_i' \; and \; q_i = 0) \end{cases}. \tag{11}$$

Step 3: Use Eq. (9) with the same secret key key_1 and key_2 to generate a pseudo-random binary sequence D_1 and a pseudo-random binary sequence D_2, and then the modulated watermark signal W' can be got by descrambling the encrypted watermark W'' with D_2. Furthermore, apply an element-wise XOR operation between the watermark signal W' and the sequence D_1 to generate the original watermark W. Note that unauthorized users without correct secret keys can not extract the exact watermark signal, so illegal users can not remove the visible watermark from the watermarked image.

Step 4: Produce the estimated mean image $\widetilde{L}$ based on the BTC codes of non-watermarked regions in the watermarked image using Eq. (3), and go further to deduce the visual factor $\widetilde{\gamma}$ using the same methods as step 3 and step 4 in watermark embedding process.

Step 5: Remove the visible watermark component for each image block with the triple (a_i', b_i', B_i) using

$$t = \begin{cases} t', & w_i = 1 \\ \dfrac{t' - \widetilde{\gamma}_i W_A}{\rho_1\left(1 - \widetilde{\gamma}_i\right)}, & w_i = 0, \widetilde{l}_i >= G_1 \\ \dfrac{t' - \widetilde{\gamma}_i (255 - W_A)}{\rho_2\left(1 - \widetilde{\gamma}_i\right)}, & w_i = 0, \widetilde{l}_i < G_1 \end{cases}. \tag{12}$$

Where t ∈ $\{a_i, b_i\}$, $t' \in \{a_i', b_i'\}$.

Finally, the unmarked image can be reconstructed according to the BTC codes (a_i, b_i, B_i) for each block when the visible watermark is removed.

4 Experimental results and analysis

The proposed removable visible watermarking algorithm (RVWBCM) has been implemented and intensively tested on many different types of grayscale images of 512×512 from the USC-SIPI image database and some binary watermark patterns of 128×128 for evaluating its

performance. Figure 4 shows some AMBTC compressed image and two visible binary watermark images for evaluation. The block size for AMBTC compression is 4×4 (i.e. $s = 4$). In the experiments, we set parameter $\tau = 0.01$ to avoid division by zero in Eq. (6), and r_1=0.1, r_2=0.3, W_A=20, G_1=128, ρ_1=0.9, ρ_2=1.3 are empirical values determined by statistical experiments (see Eq. (7) and Eq. (8)). The bifurcation parameter μ=3.618742 in Eq. (9) is arbitrarily chosen from the range (3.599456, 4).

4.1 Watermarked image quality

Figure 5 shows the visible watermarked images generated by the proposed RVWBCM scheme using AMBTC compressed images with different texture characteristics and various watermark logos from Fig. 4. From these resultant images, we find that visibly embedded watermark logos do not obscure obviously the image details, and that the watermarked images have good visual quality for different types of images although the overlaid visible watermark patterns are visible enough. The corresponding PSNR values of these watermarked images are list in Table 1. From the data in the Table, we can see that the RVWBCM scheme obtains about 24.50 dB PSNR for different host images and watermark patterns on average, and that it can achieve pleasant visual quality of watermarked images under various types of images range from highly textured images to smooth images.

Fig. 4 Some test images. **a**–**d** are 512×512 AMBTC compressed images, and **e**–**f** are binary watermark images

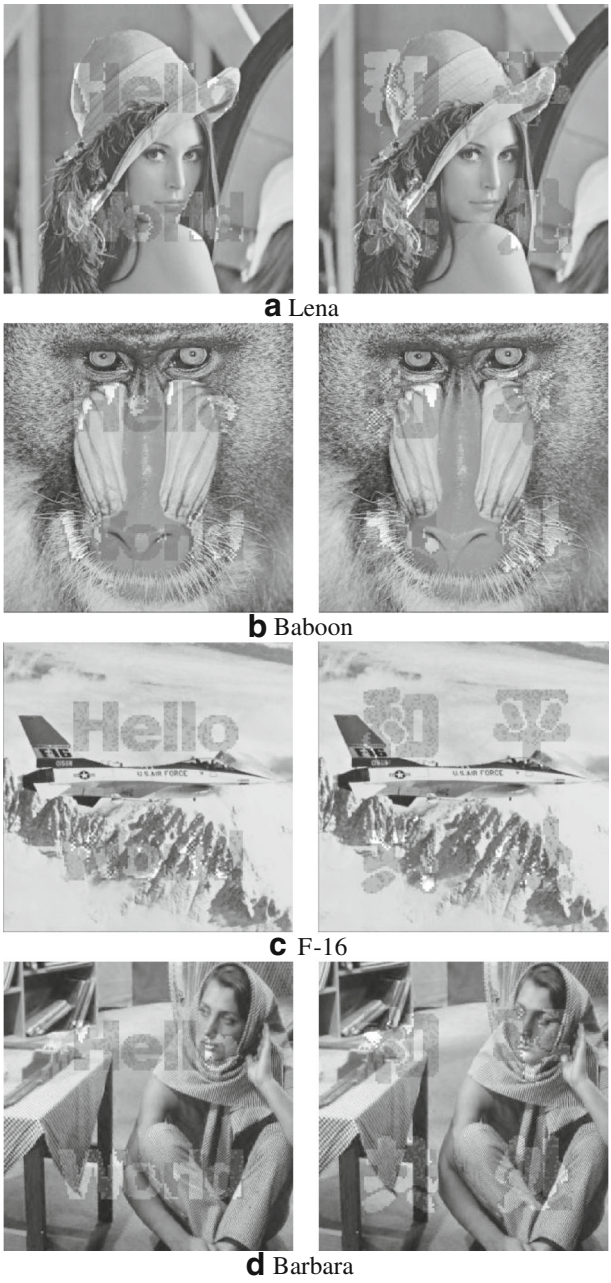


Fig. 5 Watermarked images generated by embedding various watermark patterns into different BTC compressed images

4.2 Watermark visibility

Visibility is a term associated with the human visual perception, and means that the embedded watermarks should have high intensity contrast under satisfactory visual quality of watermark images. At first, we can evaluate subjectively the visibility by carefully observing the

Table 1 PSNR value of watermarked images (Unit: dB)

Watermark pattern	Lena	Baboon	F-16	Barbara
logo 1	25.5945	25.6151	24.8103	24.8246
logo 2	24.0509	24.1264	23.5584	23.6865

watermarked image as shown in Fig. 5. Figure 5 demonstrates that the watermarked images produced by the RVWBCM scheme have satisfactory watermark translucence for various types of test images range from fairly smooth images like Lena to highly textured images like Baboon. Furthermore, the watermark visibility can be measured by the visible watermark content in the difference image between host image and watermarked image as shown in Fig. 6. From Fig. 6, it can be seen that the watermark strength is adaptive to host images and the watermarks are apparently recognizable in different types of watermarked images.

Finally, an objective measurement called normalized energy (NE) is designed to evaluate the watermark visibility and it can be computed based on the difference image E as follows.

$$NE = \frac{\sum_{1\le x\le m}\sum_{1\le y\le n} e^2(x,y)}{\sum_{1\le x\le m}\sum_{1\le y\le n} 255^2 \times (1-w(x,y))}. \tag{13}$$

Where $e(x, y)$ denotes the pixel value of difference image E.

We test the normalized energy of difference image of different methods when the PSNR values of watermarked images generated by different methods are roughly the same.

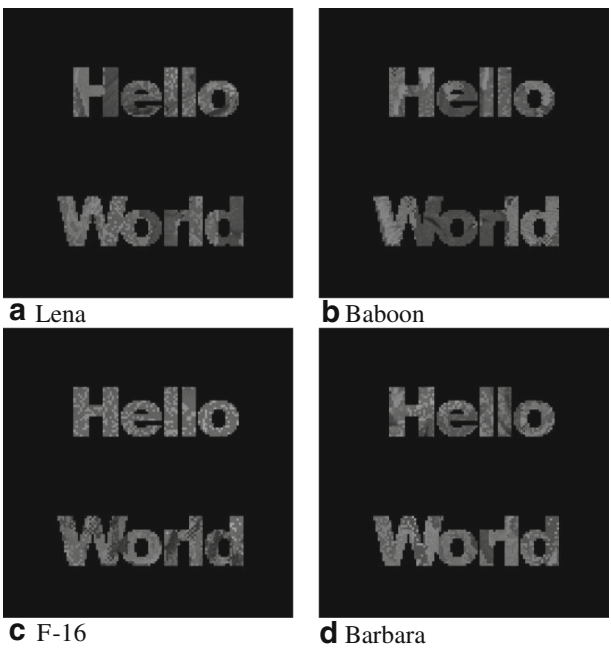


Fig. 6 Difference images between host image and watermarked image by embedding logo of Fig. 4e

Table 2 Comparison of watermark visibility using different methods

	Lena	Baboon	F-16	Barbara	Average
PVMA[22]	0.0148	0.0138	0.0141	0.0187	0.0154
RVWBCM	0.0217	0.0213	0.0243	0.0236	0.0227

Comparisons of watermark visibility are provided in Table 2. The proposed RVWBCM scheme can achieve 47 % higher normalized energy than Yip et al.'s PVMA method [22]. From the table we can observe that the RVWBCM method has better watermark visibility than PVMA scheme [22] for different types of images.

4.3 Comparison of unmarked image quality

In this RVWBCM scheme, given the watermarked image and secret keys, one can remove successfully the visibly embedded watermark pattern from the watermarked image. The visible watermark removal and high-quality restoration of the host image are only dependent on the secret key, and visible watermark removal do not resort to original watermark. This is because that authorized users can extract the binary watermark from the watermarked image before visible watermark removal. In order to evaluate effectively the removability of this proposed visible watermarking scheme, we compare the performance of the proposed algorithm with that of Yang et al. algorithm [19] in terms of PSNR values of unmarked images and the comparison results are listed in Table 3. Note that the RVWBCM scheme uses logo 1 as the watermark pattern and Yang et al. scheme embedded the gray-level version of logo 1 into host images in comparison experiments. From Table 3, we find that the unmarked images legally recovered by the proposed algorithm with the correct secret keys, have 8.20 dB higher PSNR values than those of Yang et al. algorithm on average. This shows that the proposed RVWBCM algorithm is superior to Yang et al. *method in terms of the unmarked image quality.*

4.4 Robustness

An excellent visible watermarking scheme demands that the visible watermarks overlaid on host images be hard to remove illegally. Figure 7 gives some robustness experimental results by visibly embedding logo1 of Fig. 4e into Lena BTC compressed image. The visible watermark on the attacked images is clearly recognizable. This implies that the watermark component is still in these images. So from Fig. 7 we can see that the proposed algorithm is robust against common image processing attacks such as image enhancement, image filtering, collusion attack, and image compression.

4.5 Security analysis

The proposed RVW algorithm has two different combinations of secret key. If each key is a floating-point number of 15 digits, then there are 15+15=30 uncertain digits. So the possible

Table 3 Comparison of visual quality of unmarked images by legal removal (Unit: dB)

Methods	Lena	Baboon	F-16	Barbara	Average
Yang et al. [19]	54.8047	49.5999	50.7429	47.4573	50.6512
RVWBCM	58.9229	58.9100	58.7905	58.8642	58.8719

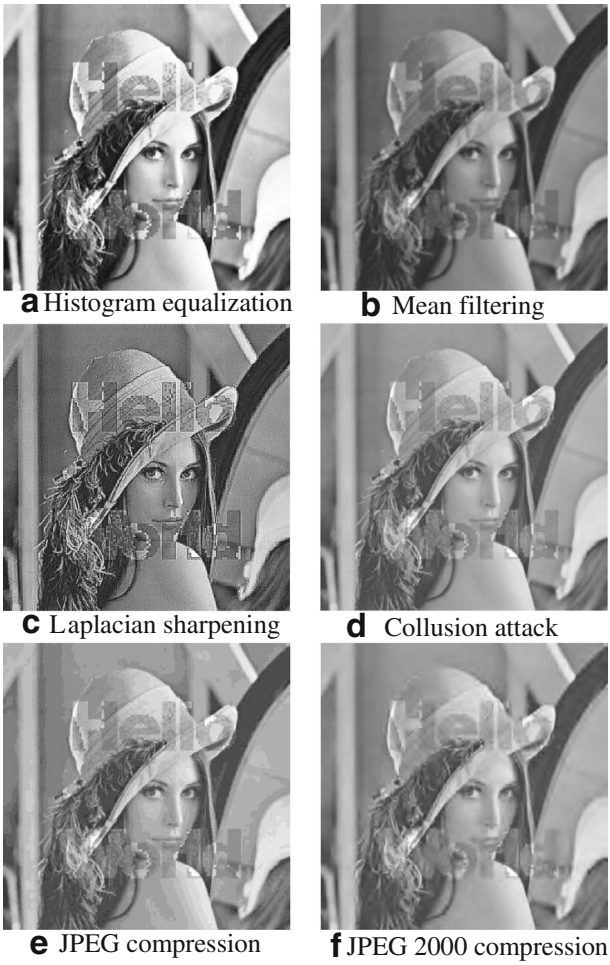


Fig. 7 Robustness against image processing attacks. The watermarked images (**a**), (**b**), (**c**), (**d**), (**e**) and (**f**) are generated by histogram equalization, 5×5 mean filtering, Laplacian sharpening, averaging 20 different watermarked image versions, JPEG compression with quality factor 10 and JPEG2000 compression with compression ratio 60:1, respectively

key space is 10^{30}. The RVW algorithm with such a large key space is sufficient for reliable practical use and has the ability to resist brute-force attack. Figure 8 demonstrates that

Fig. 8 Legal and illegal watermark removal. Correct keys for legal removal and incorrect keys for illegal removal are different by only the last single digit

Table 4 Comparison of visual quality of recovered images by illegal removal (Unit: Db)

Method	Lena	Baboon	F-16	Barbara	Average
Yang et al. [19]	33.2247	32.9391	32.9437	32.8409	32.9871
Hu et al. [6]	38.3400	37.9600	37.8900	38.1500	38.0850
RVWBCM	18.8457	18.4270	17.3493	18.5821	18.3010

authorized users with correct keys can remove effectively the embedded visible watermark on the watermarked image. However, illegally recovered image with incorrect user keys contains much too energy residue of the visible watermark, and has low PSNR value of 18.8457 dB. In addition, we compare the proposed algorithm with existing reversible visible watermarking schemes such as Yang et al.'s scheme and Hu et al.'s scheme [6] in order to verify the security against illegal removal, and the comparison experimental results are also listed in Table 4. From Table 4, the average PSNR value of the recovered images by illegal visible watermark removal with the proposed RVWBCM algorithm are about 18.30 dB, and is much lower than that of Yang et al.'s method (about 32.98 dB) and Hu et al.'s approach (about 38.08). This indicates that the proposed RVWBCM algorithm is superior to previous RVW schemes in terms of illegal watermark removal.

Moreover, as we all know, computational complexity of BTC coding is much less than DCT, DWT and VQ. Generally, BTC-based visible watermarking schemes can achieve less time cost than existing schemes based on common image coding standards. Perhaps visible watermarking schemes based on BTC are expected to provide real-time copyright protection via internet.

5 Conclusion

This paper presented a removable visible watermarking scheme applicable for BTC compressed images. The visible watermark strength is adaptive to host image content by exploiting image features in BTC compressed domain. To prevent unauthorized users from recovering the original pixels in the watermarked region, this method invisibly embeds the binary watermark sequence in the visibly watermarked image. This ensures that only authorized user can succeed in remove the visible watermark and obtain high quality unmarked image. The key space is large enough to be able to resist brute-force attack. Moreover, the visible watermark removal doesn't need the information of original binary watermark, and watermark embedding and watermark removal operate in BTC compressed domain. In a word, the proposed RVWBCM scheme is secure and has low computational cost, and it can provide real-time copyright protection and secure access control of digital media via internet or mobile terminals. In the future, to achieve broader applicability of RVW schemes, we will develop RVW scheme applicable for common compression standard such as JPEG.

Acknowledgments This work was supported in part by the National Natural Science Foundation of China under Grant No. 61073191, 61170287 and 61232016, Hunan Provincial Natural Science Foundation of China under Grant No. 10JJ6090, Scientific Research Fund of Hunan Provincial Science and Technology Department of China under Grant No. 2011GK3140, 2010GK3049 and 2011GK3139, Key Program of Hunan Provincial Education Department of China under Grant no. 12A029, Research Program of Humanities and Social Sciences of Chinese Ministry of Education under Grant No. 12YJAZH065, Science and Technology Innovative Research Team in Higher Educational Institutions of Hunan Province under Grant No. [2010]212.

References

1. Chang C-C, Lin C-C, Li K-M (2010) A removable visible watermark for digital images. J Comput 21(3):37–49
2. Farrugia RA (2010, 26–28 April) A Reversible Visible Watermarking Scheme for Compressed Images. In: Proc. 15th IEEE Mediterranean Electrotechnical Conference (MELECON 2010), Valletta, Malta, pp. 212–217
3. Fränti P, Nevalainen O, Kaukoranta T (1994) Compression of digital images by block truncation coding: a survey. Comput J 37(4):308–332
4. Hong W, Chen TS, Shiu CW (2008, 27–30 May) Lossless Steganography for AMBTC-Compressed Images. In Proc. 2008 Congress on Image and Signal Processing, vol. 2. Sanya, Hainan, China, pp. 13–17
5. Hu Y, Jeon B (2006) Reversible visible watermarking and lossless recovery of original images. IEEE Trans Circ Syst Video Technol 16(11):1423–1429
6. Hu YJ, Kwong S, Huang J (2006) An algorithm for removable visible watermarking. IEEE Trans Circ Syst Video Technol 16(1):129–133
7. Huang BB, Tang SX (2006) A contrast-sensitive visible watermarking scheme. IEEE Multimedia 13(2):60–67
8. Lian S (2009) Quasi-commutative watermarking and encryption for secure media content distribution. Multimed Tools Appl 43(1):91–107
9. Liu TY, Tsai WH (2010) Generic lossless visible watermarking - a new approach. IEEE Trans Image Process 19(5):1224–1234
10. Liu Y, Zheng D, Zhao J (2007) An image rectification scheme and its applications in RST invariant digital image watermarking. Multimed Tools Appl 34(1):57–84
11. Luo Y, Zhao Y, Cheng L, Wang J, Liu X (2012) Lossless visible three-dimensional watermark of digital elevation model data. LNCS T Edutainment 7220(8):138–147
12. Mitchell OR, Delp EJ, Carlton SG (1978, June 4–7) Block truncation coding: a new approach to image compression. In: Proc. the IEEE International Conference on Communications, vol. 1. Toronto, Ontario, Canada, pp. 12B.1.1–12B.1.4
13. Mohanty SP, Ramakrishnan KR, Kankanhalli MS (2000) A DCT domain visible watermarking technique for images. In: Proc. IEEE Int. Conf. Multimedia and Expo., vol. 2. New York City, NY, USA, pp. 1029–1032
14. Pareek NK, Vinod Patidar, Sud KK (2006) Image encryption using chaotic logistic map. Image Vis Comput 24(9):926–934
15. Shie S-C, Lin SD (2008) Improving robustness of visible image watermarks. Imaging Sci J 56(1):23–28
16. Tsai M-J (2009) A visible watermarking algorithm based on the content and contrast aware (COCOA) technique. J Vis Commun Image Represent 20(5):323–338
17. Tsai H-M, Chang L-W (2007, 2–5 July) A High Secure Reversible Visible Watermarking Scheme. In: Proc. 2007 I.E. International Conference on Multimedia and Expo. Beijing, China, pp. 2106–2109
18. Tsaia HM, Chang LW (2010) Secure reversible visible image watermarking with authentication. Signal Process Image Commun 25(1):10–17
19. Yang Y, Sun X, Yang H, Li CT (2008) Removable visible image watermarking algorithm in the discrete cosine transform domain. J Electron Imaging 17(3):033008-1–033008-11
20. Yang Y, Sun X, Yang H, Li CT, Xiao R (2009) A contrast-sensitive reversible visible image watermarking technique. IEEE Trans Circ Syst Video Technol 19(5):659–667
21. Yeh FH, Lee GC, Lin YT (2008, 9–12 Dec) Removable Visible Watermarking in JPEG Compression Domain. In: Proc. 2008 I.E. Asia-Pacific Services Computing Conference (APSCC '08), Yilan, Taiwan, China, pp. 1328–1331
22. Yip SK, Au OC, Ho CW, Wong HM (2006) Lossless visible watermarking. In: Proc. Int. Conf. Multimedia and Expo. Toronto, Ontario, Canada, pp. 853–856
23. Zhang X, Wang S, Feng G (2011) Reversible visible watermarking with lossless data embedding based on difference value shift. Intell Autom Soft Comput 17(2):233–243

Hengfu Yang was born in Hunan, China, 1974. He received the M.S. degree in Computer Application from Guizhou University, China, in 2003, and the Ph. D. degree in Computer application from Hunan University, China, in 2009. He is currently with an associate professor in Department of Information Science and Engineering, Hunan First Normal University, China, and also with a postdoctoral fellow in the School of Computer, National University of Defense Technology, China. His research interests include digital watermarking, information hiding, information security, image processing.

Jianping Yin was born in Hunan, China, 1963. He received his MSC and PHD degrees in computer science from the National University of Defense Technology, China, in 1986 and 1990, respectively. He is currently with a professor in the School of Computer, National University of Defense Technology, China. His main research interests include information security, image processing and pattern recognition.