A novel watermarking algorithm based on characteristics model of local fragmentary images

Quanzhi Lei*

Embedded/IOT Application Technology Engineering Center,
Xiamen City University,
Fujian Province, Xiamen, 361008, China
Email: qzlei008@126.com
*Corresponding author

Lijun Xiao

Accounting Department,
Guangzhou College of Technology and Business,
Guangzhou, 528138, China
Email: ljxiaoxy@126.com

Osama Hosam

The College of Computer Science and Engineering College,
Taibah University,
Yanbu, 41911, Saudi Arabia
and
The City for Scientific Research and Technology Applications,
IRI, Alexandria, 41910, Egypt
Email: mohandesosama@gmail.com

Haibo Luo

Industrial Robot Application of Fujian University
Engineering Research Center,
College of Computer and Control Engineering,
Minjiang University,
Fuzhou, 350108, China
Email: robhappy@qq.com

Abstract: Watermarking is a popular technology to protect the copyright of digital image from illegal infringement. Traditional watermarking algorithms cannot better resist the illegal tampering attacks, causing serious security issues. This paper aims to propose an image watermarking algorithm with ability against illegal tampering attacks. The original image should be firstly pre-processed, and its fragmentary characteristic function of local image block is used to generate watermark locations randomly. When the watermark is illegally tampered and damaged, the generated fragmentary characteristic factor can be used to re-construct the original image. Finally, the forensics of original image is realised. The experimental results show that the proposed algorithm can effectively embed a watermark into image. Besides, the original image can be restored even if the watermark is damaged. It is also robust to the typical attacks and has ability against tampering over a large area of the image.

Keywords: local image; watermark; fragmentary image; characterisation factor; tampering attack.

Reference to this paper should be made as follows: Lei, Q., Xiao, L., Hosam, O. and Luo, H. (2020) 'A novel watermarking algorithm based on characteristics model of local fragmentary images', *Int. J. Embedded Systems*, Vol. 12, No. 1, pp.11–21.

Biographical notes: Quanzhi Lei received his BE degree in Xi'an Petroleum University. He is currently an Assistant Professor in Xiamen City University, Embedded/IOT Application Technology Engineering Center of colleges and universities in Fujian Province. His research interests include computer digital media, image processing and information security.

Lijun Xiao is an Assistant Professor in the Guangzhou College of Commerce, she received her BE in Information Management and Information System from Hunan University of Commerce, China, in 2010 and ME in Information Management and Information System from Hunan University of Science and Technology, China, in 2017. Her research interests include internet of things, cognitive internet of things, edge computing and mobile computing.

Osama Hosam is a Research Associate in SRTA-City, Alexandria, Egypt. In 2007, he received his MSc in Computer Systems and Engineering from Azhar University. In 2011, he received his PhD in Computer Science and Engineering, Hunan University, China. In 2013, he worked as an Assistant Professor in at the Collage of Computer Science and Engineering in Yanbu. He is currently an Associate Professor in Taibah University. His research interests include, stereo vision, pattern recognition and computer and information security, etc.

Haibo Luo received his BE in Communication Engineering from Wuhan University of Technology, China, in 2006, ME in Information and Communication Engineering from Hunan University, China, in 2009 and PhD degree from the College of Physics and Information Engineering, Fuzhou University, Fuzhou, China. His research interests include internet of things, cognitive internet of things, edge computing and mobile computing.

1 Introduction

With the development of high-performance computation and popularity of internet, the digital data (video and image etc.) can be easily distributed, tampered and copied by malicious users (Wang and Zhou, 2018). It causes serious economic loss and legal disputes. Therefore, intellectual property (IP) protection is an important issue to ensure the security of digital work. There are various tampering attacks for digital image, including cloning, splicing, polishing and generation. As common attacks, cloning and splicing have the largest impact on image judicature. Due to similar brightness and chromaticity of image blocks in the same image, the copy and paste cannot cause any obvious visual changes. So, it is difficult to detect the tampering attacks accurately. In the last decade, most watermark detection techniques for digital image focus on the pixel region of the whole image (Zuo and Yu, 2017). For the image watermark detection, it requires a reference to detect whether an image was tampered. Besides, the tampered regions were usually polished to match the original image, causing it harder to be detected. But it is undeniable that the splicing is the most popular tampering technique and has greater influence on society nowadays. Therefore, it is important to design an adaptive watermark detection technology to protection the copyright of image.

The method based on the characteristics model of local fragmentary images has three features.

1 The watermarks may be inserted into different local characteristic positions. So, the original image will be firstly transformed. The coefficients should be altered in transformation field for watermark insertion. The watermark in audio, video or image without any alteration is realised by altering the coefficients in spatial domain.

2 The local image characteristic based watermark detection needs no original carrier. But some original data is required for watermark extraction. The real-time image watermark detection has good prospects in real application. In this case, recent image watermarking techniques focus on local blind watermark.

3 On basis of the sensitivity to attacks, fragile image watermark has the lowest ability against attacks.

But the local image characteristic based watermarking technique has good resistance against various attacks. The watermark can also be extracted after it has suffered from attacks. In this case, the watermarking techniques are widely concerned presented by researchers. These techniques have two drawbacks. On one hand, the local image characteristic is measured by intensity gradient. In this way, the extracted position characteristic points are not stable enough and the distribution of these points is not uniform. On the other hand, the watermark embedding strategy is simple, which affects the imperceptibility and robustness of the whole system.

In this work, an image watermarking algorithm is proposed to prevent the splicing attacks. Firstly, the local characteristic value of the original image is pre-processed. The coefficient value of image fragmentary factor S and the reference image are compared quantitively. Finally, the watermarks can be restored by using the reconfiguration strategy.

The remainder of this paper is organised as follows. The related work of image watermarking is illustrated in Section 2. Section 3 analyses the proposed watermarking algorithm in details. The experimental results are analysed in Section 4. Section 5 summarises this work and raises the prospect for the future.

2 Related work

The digital image watermarking technique grows very rapidly in recent years, which attracts wide attention of various research institutes and colleges all over the world. American Scientific working group for image technology has proposed the optimal operation specifications to analyse photograph pictures, video, integrated circuit chip and

video/image specifically for the judiciary authority and some crime forensics departments (Liang et al., 2015, 2019). The splicing or tampering on a digital image may leave some traces, which can be detected as an evidence to prove the tampering attack. The researchers also found that some tampering behaviours usually implemented double compression. Therefore, the watermarking algorithms based on re-sampling also have the ability against the splicing and tampering attacks.

The splicing and tampering attacks on image always tamper the singular values of various statistical property from different source images. Generally, it extracts some features for quantitative description and uses machine learning technique to train the classifier. Finally, the classifier is used make second-class judgment. These illegal technologies make it difficult for the image detection. The authors in Liang et al. (2015) proposed a Cir-Hu based watermarking algorithm. The circle blocks of the normalised grey image are extracted as the local area. The Hu Moment descriptors of each area are extracted as the characteristic indicator of the image. Finally, a method to measure the distance between images is also proposed. The proposed algorithm has good robustness against common geometry attacks, but cannot resist large area of cropping or cycle spinning. In Wu et al. (2004) a mathematical model is proposed to detect image splicing and tampering. The magnitude/phase of double-consistency and the features such as forecast error margin feature etc. were used to classify and distinguish the tampered images with the accuracy rate of 75%–80%. Yang and Kot (2004) counted the number of continuous pixel points at same grey level in the same direction in the natural images. The support vector machine (SVM) is used to identify the tampering image. However, it generates lots of nonlinear and unstable features during the detection process. In order to improve the robustness and discrimination, Tzeng and Tsai (2003) adopted the ordinal measures of discrete cosine transform (DCT) coefficients to find the best threshold value by MAP. It has robustness against the attacks such as scaling, obscureness, Gaussian noise, histogram equalisation etc., but for rotation attacks, the method can only find the images rotated in 180° or less, which rotated in other angles cannot be found as well as the cropped or stretched images. Only with the same global-featured image and query image, the method above based on global image features can be effectively used to make detection, therefore, the image copy detection based on global features might be difficult to have good effect. To solve this issue, the authors Tsi et al. (2005) and ho et al. (2009) applied local descriptor to capture the image features, calculating the multi-descriptors of every image, every descriptor and the local correlated region of the image. The method (Pan et al., 2006) adopted the iteration geometric technique to resist geometric distortion. Recently, the authors Yan and Kot (2006) put forward the image Hash algorithm, using the network-based Hash extracting and matching for likelihood test. By comparing with other traditional media Hash technologies, this algorithm achieves better performance against geometric attacks. Note that the media Hash can be also regarded as a robust feature vector though it is rooted in cryptology, which can tolerate the errors caused by attacks.

The Digital image watermarking is copyright protection method based on vital features of the original data. It is why we used to take advantage of its the feature-based detectors to find the feature points of image carriers. It uses a part of features, based on points, to build area of parts of features, embedding the digital watermark information into each feature region. The information extraction is to find out positions of feature points contain watermark image by using of the same method of feature point detector, and build feature region, and detect digital watermark information. It can resist the illegal attack. Zhu et al. (2013) raises a new kind of method of image watermark based on feature. First of all, the multistage detector is to extract steady feature points from image carrier. It ensures a part of feature region by self-adaptive feature scale principles. Finally, the watermark is embedded by calculating pseudo-Zernike matrix on non-sub-sampled contour wave low frequency sub-band. Seo and Yoo (2006) make use of the feature of Harris-Laplace and Harris-Affine to build three kinds of locally invariant regions, adding two-dimensional watermark into feature region. Gao et al. (2010) firstly combine related theories such as Harris-Affine et al. construct the feature points detector, it can extract original image, obtain one set of feature region which is independent and stable based on Minimum spanning tree clustering theory, then we can obtain rotate and scale unchanged region by the method of main gradient direction alignment. Finally, we can add watermark information embed into this part in the blank field. In Krewinkel et al. (2006) a robust image watermarking algorithm is proposed with great resistance against synchronisation attack. Meanwhile, the scale space theory and image normalisation technique are considered. Santhi et al. (2013) proposed a robust self-adaptive image watermarking algorithm, which used the clustering method to extract image feature points and built a feature region. The wavelet transformation is used in each selected region. With the hyperbolic tangent function, the zoomed parameter of intermediate frequency sub-band of each region image can be calculated. Based on this zoomed parameter, the self-adaptive watermarks can be embedded to the intermediate frequency of selected area. The proposed algorithm has good robust ability against the removal attacks. Li et al. (2011) utilised the most notable local feature region to embed the watermark by defining robust quantitative detection indicator of visual attention value, etc. In Kurnia et al. (2015) the probability density of image feature points is used by extracting feature points of watermark image and a multifunction image watermarking algorithm based on image feature points is proposed. This algorithm firstly extracted local feature points to get the watermark list by constructing vector relationship. The singular value norm theory is considered to embed watermark in blank space of image. Tsai et al. (2012) proposed a feature points based digital image watermarking algorithm. It firstly uses the scale adaptive correlation

matrix and LOG operator to generate the local feature regions. The best local feature area is selected to embed watermark by using genetic algorithm.

In conclusion, many effective watermarking methods have been proposed for image to protect the copyright of image. But there are some security issues to be addressed in these methods, such as low security, vulnerability, instability, etc.

3 Image fragmentary characteristics model

3.1 Definitions

- Definition 1: There are two images X_1 and X_2, both satisfying $X_2 = t(X_1)$. It means that X_1 and X_2 are correlated, where $x \in X$. X is the aggregation of image fragmentary feature transformation, but with invariance of the contents. X_1 denotes the registered original image.
- Definition 2: The image database is denoted by $X = \{C, R\}$. C = $\{Q, C_1, \ldots, C_m\}$ represents one query (original) image Q and its copy (with certain or no modifications). $R = \{R_1, \ldots, R_n\}$ is the remaindering fragmentary image in the database. The detector (classifier) should have high distinguishability for these two classes (data set C called as 'Class C' and data set R as 'Class R').

Property 1 similarity theorem of fragmentary images: it is to describe the effect of scale changes of fragmentary characteristics function independent variables on Fourier transform.

$$X = F\left(f(at)\right) = \int_{-\infty}^{\infty} f(at)e^{-j2\pi ut}dt \tag{1}$$

Property 2 translation invariance of Fourier transform between the fragmentary images.

To prove it, if $f(t) \leftrightarrow F(j\omega)$, then the Fourier transform of delayed signal can be described as:

$$F\left(f(x-x_0)\right) = \frac{1}{N}\sum_{x=0}^{N-1} f(x-x_0)\,e^{-2\pi ux/N} \tag{2}$$

To prove it, if $y = x - x_0$ and then

$$\begin{aligned} F\left(f(x-x_0)\right) &= \frac{1}{N}\sum_{x=0}^{N-1} f(y)e^{-j(y+x_0)/N} \\ &= e^{-j}\left(\frac{1}{N}\sum_{x=0}^{N-1} f(x)e^{-jx/N}\right) \\ &= e^{-jx_0/N}F(j) \end{aligned} \tag{3}$$

Similarly, it concludes:

$$F\left(f(x+x_0)\right) = e^{jx_0/N}F(j) \tag{4}$$

It means, x_0 is the initial margin, but the magnitude spectra is still the same.

$$F\left(f(x_0)\right) = \left|F(j)\right| \tag{5}$$

We measure the similarity of both images by the correlative coefficient of fragmentary eigenvector. Given an original mage, the fragmentary factor S can be obtained. S^i is the factor after embedding the watermark. For a given test image, the fragmentary spectrum before embedding watermark is T and T^i is the fragmentary spectrum after embedding the watermark. Then the related coefficient of S^i and T^i can be calculated to obtain the image similarity. The formula is described as follows.

$$F_i = \frac{\sum_{j=1}^{n}\left(S_j^i - \overline{S^i}\right)\left(T_j^i - \overline{T^i}\right)}{\sqrt{\sum_{j=1}^{n}\left(S_j^i - \overline{T^i}\right)^2}\sqrt{\sum_{j=1}^{n}\left(S_j^i - \overline{T^i}\right)^2}} \tag{6}$$

where

$$\overline{S^i} = \frac{1}{n}\sum_{k=1}^{n} S_k^i \tag{7}$$

$$\overline{T^i} = \frac{1}{n}\sum_{k=1}^{n} T_k^i \tag{8}$$

Therefore, the average value of related coefficient is

$$\overline{F} = \frac{1}{m}\sum_{i=1}^{m} r_i \tag{9}$$

Given a present threshold value, judge whether it is fragmentary image; if yes, then the test image is fragmentary, otherwise not.

3.2 Matching of image block

In image watermarking process, the matching issue for the similarity F of image block is very important. Let a fragmentary image block of an image be denoted by A. A similar block B can be found in another image. The matching procedure is concretely described as follows: firstly, the distance between both fragmentary image blocks is calculated by solving the sum of absolute differences between the two blocks. The invariant regions of two blocks are respectively denoted by $A1$ and $B1$. $A1$ is the eigenvector of a certain fragmentary image block, namely $V_{A1} = \{\phi_1^{A1}, \phi_2^{A1}, \phi_3^{A1}, \phi_4^{A1}, \phi_5^{A1}, \phi_6^{A1}, \phi_7^{A1}, avg^{A1}\}$ and $B1$ is the eigenvector of a certain block after embedding watermarks, $V_{B1} = \{\phi_1^{B1}, \phi_2^{B1}, \phi_3^{B1}, \phi_4^{B1}, \phi_5^{B1}, \phi_6^{B1}, \phi_7^{B1}\}$. Finally the normalised correlation is calculated to evaluate the similarity. $L1$ is used to measure the distance. In formula (10), max is the maximum value; | | denotes the absolute value. ϕ_i^{A11} and ϕ_i^{B11} are respectively the *i-th* vector of block $A1$ and $B1$.

$$|V_{A1} - V_{B1}| = \frac{\sum_{i=1}^{7} |\phi_i^{A1} - \phi_i^{B1}|}{\max\left(|\phi_i^{A1}|, -|\phi_i^{B1}|\right)} + \frac{|avg^{A1} - avg^{B1}|}{\max\left(avg^{A1}, avg^{B1}\right)} \quad (10)$$

The shortest distance between image fragmentary block V_{A1} and the block V_{B1} means it is closest to this block in the original image. This value can be reserved as the distance S_{11}. The parameters of other fragmentary blocks are calculated to find the blocks with the closest distance, denoted by S_{12}, S_{13}, …, S_{nm}.

Therefore, the distance between both images is the sum of all the distances S = S_{11} + S_{12} + S_{13} + … + S_{nm}. At last, the distance S between both images is compared to the predetermined threshold value T. If $S < T$, both images are the same, otherwise they are different images.

3.3 Watermark embedding

Let the image of initial carrier be X and pre-processing image be X'. The binary image is divided into various sub-blocks. The information insertion and extraction could be made for every block. The fragmentary blocks of all '1' (all white) and all '0' (all black) are completely white and black smoothing ones. So, it is perceptible to modify the pixel of such kind of block. Therefore, it cannot be used to hide the secret information while the other kinds of blocks can be used for embedding information. The watermark '0' can be denoted by replacing the odd-even order of the fragmentary image blocks. When the order is replaced by even-bit type, it denotes a watermark '1'. Obviously only a watermark bit can be inserted by replacing an order. Every kind of odd-even order pattern blocks only utilises 1/2 embedding capacity. Hence, the watermark embedding can be made by the substitutes of two kinds of pattern blocks in the designated odd-even order, favourably to increase the pattern blocks of fragmentary images and the number of embedded watermarks.

The watermark embedding process is shown in Figure 1:

Step 1 The original watermark is divided into image block X and pre-processed image block X'. The pre-processed information W1 is scrambled under the control of Key 1 to obtain m. In this case, the security and robustness of watermark embedding are enhanced.

Step 2 Formulas (9) and (10) are used to calculate the similarity of fragmentary image eigenvector, and then the structure of binary coding string is constructed to choose a coding-string image block as the location for watermark embedding.

Step 3 Considering that the binary image has only white and black colour, per the odd-even substitute mode of fragmentary images and secret key K1, the fragmentary factor S and match value V can be calculated.

Step 4 According to the coefficient value of image fragmentary factor S and matching property F, a sub-block of the fragmentary image is chosen randomly. There are two different odd-even substitute modes due to the embedding strategy:

1 substitutes between the odd-pattern blocks, denoting a watermark '0'

2 the substitutes between the even-pattern blocks, denoting a watermark '1'.

Step 5 If the capacity of encoding string is limited, the encoding string can be combined adaptively to reduce the overhead. Steps 3–5 repeat until all watermarks are embedded.

Figure 1 Watermark embedding flow chart (see online version for colours)

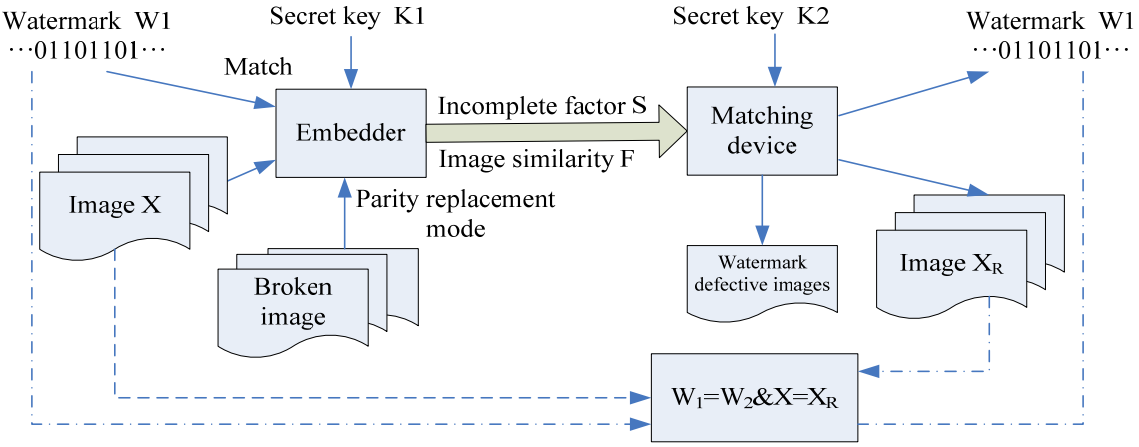
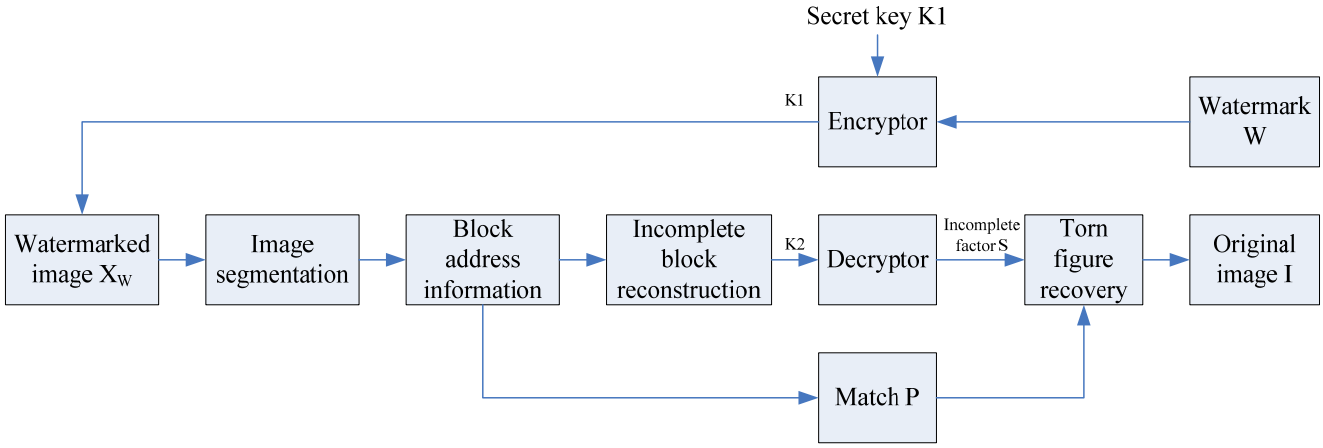


Figure 2 Watermark extraction flowchart (see online version for colours)



3.4 Watermark extraction

Watermark extraction is to divide the image with secret into blocks. After that, all hidden watermarks are ordered founded under the control of secret key K2. It is very easy to extract the embedded information. The blocks with all '1' and all '0' are considered without watermarks. If the number of '0' in the same alternative pattern blocks is odd, the pixel values on lower-left and upper-right in the blocks need to be extracted. If the number of '0' in the block is even, then there is no hidden information in the block. The extraction algorithm of hidden information in the pattern block is listed as follows:

Step 1 In above section, after alternative embedding of coding string and odd-even pattern blocks by K1 and encryptor, we divide the images into the same amount of sub-blocks for watermark embedding. In this case, the related address information m of fragmentary sub-blocks in the hidden watermarking images are generated.

Step 2 Based on the address m, we connect the data-bit level of the sub-blocks at different locations of the fragmentary image blocks, and use the binary interpolation to resize the image into the fixed blocks in order to standardise the fragmentary images.

Step 3 By the above method, the local fragmentary block region is marked to obtain the number of blocks $n \times n$. For any block X, $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, n$, we extract its invariant moment as the global feature. In order to make better distinction, the pixel mean avg^{ij} of fragmentary image block is added. Then the eigenvector of block (i, j) is V. So far, the matching factor p of fragmentary image can be calculated.

Step 4 After obtaining the address information and matching factor P, the reconstructed information of fragmentary blocks in every hidden image watermark can be encrypted with K2. The associated value of the fragmentary factor S can be calculated finally. In addition, the fragmentary block information can be calculated as follows with the block information and the function $S(r, \theta)$.

$$E_{hm} = \frac{1}{4\pi}\int_0^{2\pi}\int_0^1 S(r,\theta)A_h^*(r)\exp(-jm\theta)rdrd\theta \quad (11)$$

$$A_h^*(r) = \sqrt{\frac{2}{r}}\exp(-j2h\pi r) \quad (12)$$

Here, k represents the order of the radial basis function and m is the order of angular basis function.

The image can be reconstructed with the fragmentary block by using (13).

$$\begin{aligned} S_{rec}(i,j) &\approx \sum_{h=H_{\max}}^{H_{\max}}\sum_{m=M_{\max}}^{M_{\max}} E_{hm}Q_{hm}(x_i, y_i) \\ &= \sum_{h=H_{\max}}^{H_{\max}}\sum_{m=M_{\max}}^{M_{\max}} E_{hm}A_h(r_{i,j})\exp(jm\theta_{i,j}) \end{aligned} \quad (13)$$

Here $H_{\max}$ and $M_{\max}$ are the maximum order of the radial basis function and angular basis function. $S_{rec}(i, j)$ is the image reconstruction function.

1 The blocks are selected with specific rules. With the secret key *Key2*, the block function $A'' = \{a''(h), h = 1, \ldots.., L\}$ is selected and the amplitude is $|A''| = \{|a''(h)|, k = 1, \ldots.., L\}$.

2 With the decoding flow of the quantified modulation strategy, the watermark can be extracted by using the exponential moment A'' in (1). Assume the extracted watermark be $W' = \{w'(h), h = 1, \ldots\ldots, L\}$, the watermark can be extracted as follows.

$$\text{If } |a''(h)| - 2\times\Delta\times range\frac{|a''(h)|}{s\times\Delta} > 0, \quad (14)$$

we have $w'(h) = 1$

$$\text{If } |a''(k)| - 2 \times \Delta \times range\frac{|a''(k)|}{s \times \Delta} \le 0, \quad (15)$$

we have $w'(k) = 0$

Here, *range*(◦) is the rounding off operation. Δ is the quantified step length.

3 Repeat 1 and 2 above until all the local characteristic areas are detected. If the watermark can be extracted from an area, the ownership can be proven. Otherwise, the watermark detection is failed.

Step 5 With the matching value P and the associated values of S, the recovered group address information can be solved for the fragmentary image sub-blocks. The relevant binary image information can be extracted from every address in the order of secret key. It is used to recover the final original image information.

4 Experiments and analysis

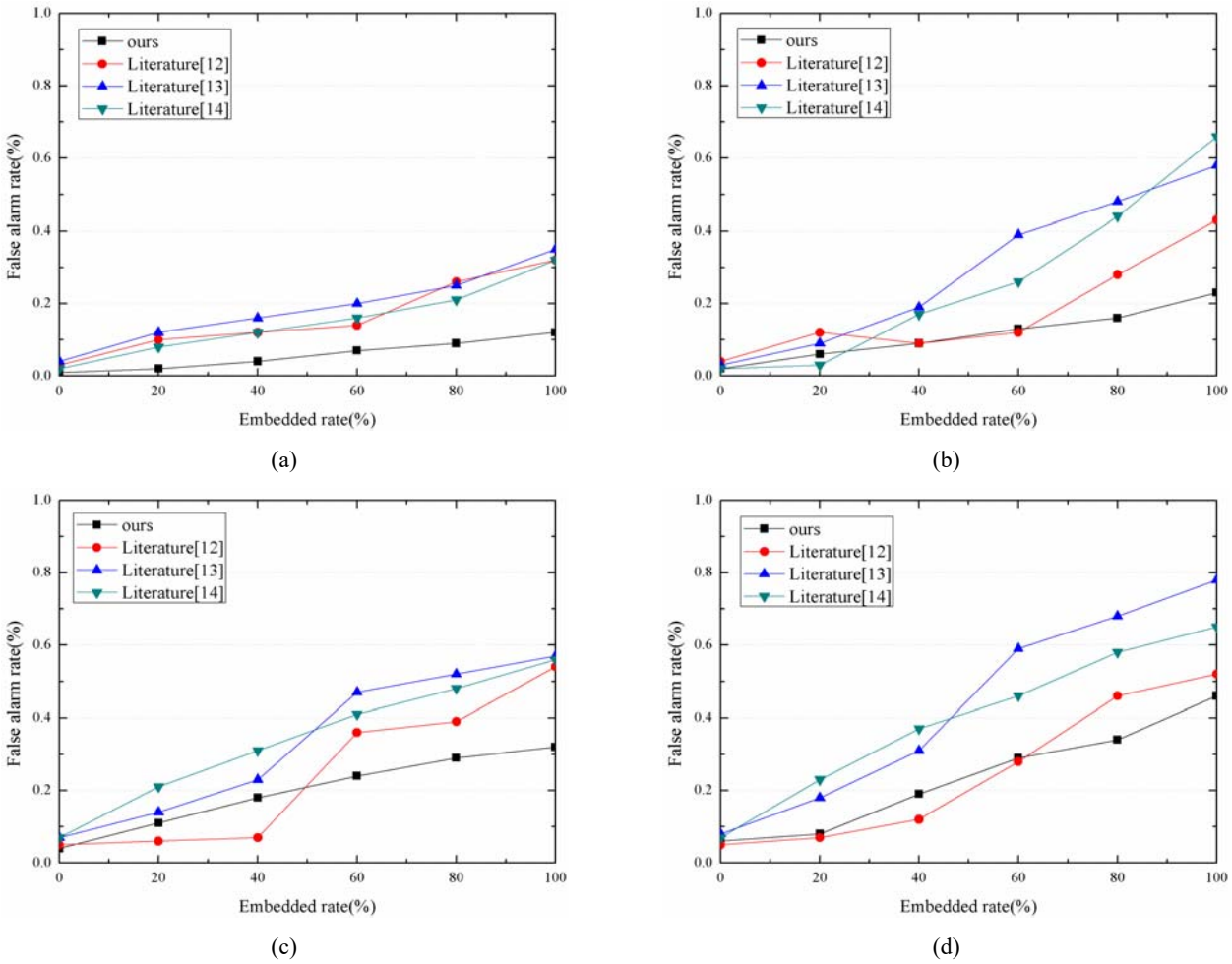
In the experiments, the database (UCID DC) is used and the machine has Dual-Core CPU E5700@3.00GHz, internal storage 1.96 GHz, Windows XP system. MATLAB7.0 is professional mathematical software designed by MathWorks, which is widely used in algorithm development, data analysis and data visualisation. So, MATLAB 7.0 is used in experiment. Figure 3 shows the watermarked designs. In order to verify the efficiency of the image watermarking algorithm, we have carried out a series of simulation experiments. The experimental results are mainly from two aspects, one is the detection performance test, the other is the robustness test.

4.1 Anti-tampering attack

This experiment adopted the data set (DC) of original image and DC of watermarking images for watermark embedding. The algorithms (Yang and Kot, 2007; Robertson et al., 1996; Lu et al., 2002) introduced the embedding rate and error rate curves of the three algorithms, also shown in Figure 3. When the embedding rate is 80%, the proposed algorithm has the lowest error rate. When it is 40%, the false alarm rates in algorithms (Yang and Kot, 2007; Robertson et al., 1996; Lu et al., 2002) are respectively 13.0%, 26% and 18%. When the embedding rate is 60%, the false alarm rates of the algorithms (Yang and Kot, 2007; Robertson et al., 1996; Lu et al., 2002) are respectively 17%, 27% and 28%, but only 15% in the proposed algorithm. Therefore, the proposed algorithm is a better choice among these four algorithms in security. Although the running time in this algorithm is a little longer than those in algorithms (Yang and Kot, 2007; Robertson et al., 1996; Lu et al., 2002) and as local character-based watermark algorithm, it can satisfy the requirements in actual application.

Figure 3 Watermark embedding effect diagram

Figure 4 False alarm rate experimental curves under various attack strength (see online version for colours)



4.2 Detection rate

In some cases, higher accuracy is more important than false alarm rate. In this experiment, we keep a balance between the embedding rate and false alarm rate. The threshold value in algorithms (Zhu et al., 2013; Seo and Yoo, 2006; Gao et al., 2010) are set as 0.5. Generally, if the threshold value of correlative coefficient of both images tends to be 1, then the tested image is original one. If the threshold value tends to be 0, then it can be confirmed that the test image has worse image effect. Figures 4(a–d) indicates the results after performing rotation attacks. With the increase of the watermarks, the probability of the false alarm rate also increases. Due to the use of the reconstructed factors of fragmentary image in the proposed algorithm, it achieves better performance by comparing to other algorithms. Figures 4(a–d) show the experimental results. With the increase of attack strength, the probability of the false alarm rate also increases. Besides, we use PR curve to evaluate the performance after suffering the rotation attacks. Let N_T be quantity of original quantity. N_c and N_{nc} are respectively the number of images detected as qualified image and the number of images embedded with watermarks. PR curve is defined as follows:

$$Precision = N_c / \left(N_c + N_{nc}\right) \tag{16}$$

$$Recall = N_c / N_T \tag{17}$$

Therefore, the curve (X-axis indicates embedding rate, and Y-axis indicates false alarm rate) in Figure 5 is realised by selecting the threshold value τ as 0.5. The definitions 1–3 show that with higher anti-attack capacity and image safety, less fragmentary blocks is detected. Obviously, the higher the rotation rate and false alarm rate, the better its performance.

ROC curve (receiver operating characteristic curve), also called as SC (sensitivity curve):

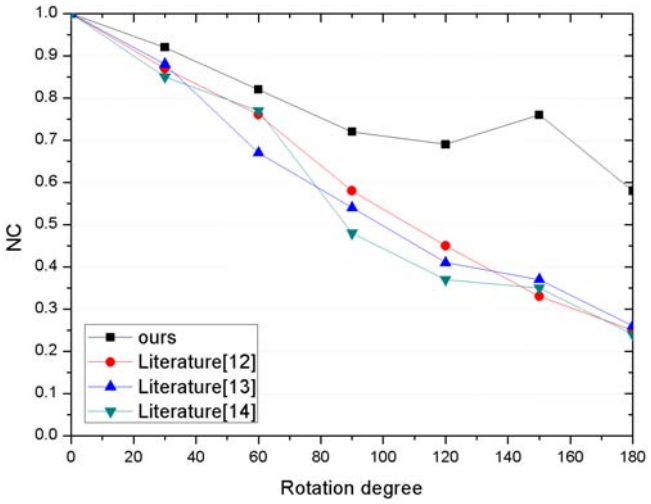
$$F\_rej = N_{fn} / \left(N_{rp} + N_{fn}\right) \tag{18}$$

$$T\_rej = N_{rn} / \left(N_{rn} + N_{fp}\right) \tag{19}$$

Wherein, N_{rm} indicates the number of images. In formula (18) and (19), *F_rej* stands for probability mal-detecting the original images, and *T_rej* for probability correctly detecting the original image. We select different threshold values to obtain ROC curve (X-axis: *F_rej* and Y-axis: *T_rej*). The ideal situation is to have smaller *F_rej* and larger *T_rej* as much as possible; considering the conflicts between their proportional relationship and actual requirements, it is necessary to select one proper similarity

threshold, i.e., weigh the advantages and disadvantages between these two cases.

Figure 5 Rotate the NC curve under attack (see online version for colours)



4.3 Recovery rate

After suffering illegal tampering attacks, it is very important to evaluate the image recovery capacity for the image forensics and detection, which can be applied to such fields as crime forensics etc. Figure 6 indicates that, when the images using the four watermarking algorithms respectively are suffered from the illegal tampering attacks, obviously, the proposed algorithm presents better advantage in terms of image recovery rate since the images to be embedded has been re-grouped in the fragmentary image sub-block form during the process of watermark embedding. The fragmentary image can make a fast construction according to the information in its neighbouring fragmentary blocks after the fragmentary images are damaged. But for the other three algorithms, the images have failed to be recovered for forensics with a damaged degree of 40%, Hence, the proposed algorithm has better ability against illegal tampering attacks.

After comparing the recovery capacity of the four kinds of algorithms, some simulations for illegal tampering attacks are also conducted. The results in Table 1 indicate that the proposed algorithm *i* can detect some modified images such as cropping, rotation etc. It is similar to the algorithms (Yang and Kot, 2007; Robertson et al., 1996; Lu et al., 2002) in terms of anti-signal attack. Even though parts of images have been cropped, it can still detect all image. But the algorithms (Yang and Kot, 2007; Robertson et al., 1996; Lu et al., 2002) are not satisfactory. The algorithm of Yang and Kot (2007) is robust with the rotated angle of 180°, 270° or smaller, but weaker in the wide-angle. Besides, it cannot detect all images with contrast and saturation enhancement etc. Its advantage is to detect the images after cycle spinning, while the other cannot realise it. The algorithm of Robertson et al. (1996) could best detect the rotated image at any angle in the aspect of anti-rotation attack. The algorithm of Lu et al. (2002) is robust against rotation, scaling and translation, but it could not resist against certain special signal attack in practice. For the proposed algorithm, it has better performance against cropping and translation etc. by comparing to other algorithms.

Figure 6 Self-healing curve under attack (see online version for colours)

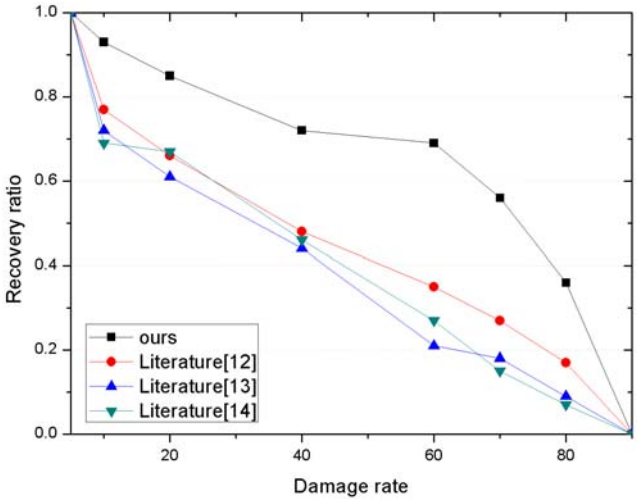


Table 1 Tampering detection results of image rotation

Attack	*Ours*	*Yang and Kot (2007)*	*Robertson et al. (1996)*	*Lu et al. (2002)*
Cut off on the left 25%	0.88	0.58	0.51	0.48
Cut off on the right 50%	0.74	0.34	0.44	0.31
Rotate 5°	0.92	0.71	0.67	0.78
Rotate 90°	0.85	0.35	0.46	0.32
Rotate 180°	0.78	0.21	0.15	0.12
Rotate 270°	0.68	0.12	0.08	0.04
Horizontal flip	0.88	0.53	0.69	0.45
Vertical flip	0.92	0.73	0.62	0.57

In order to verify the anti-splicing/tampering attack performance of our algorithm, the comparison test between this algorithm and the one proposed in Peng and Kang (2012) is made as show in Table 2. The test result shows that in the condition of wiping off legal watermarks, the quality of recovered standard image (about 52 dB) by our algorithm is higher than that (about 44 dB) by Peng and Kang (2012), while in the condition of wiping of illegal watermarks, the quality of recovered standard image (about 26 dB) by our algorithm is lower than that (about 37 dB) by Peng and Kang (2012), indicating our algorithm is superior to that in algorithm of Peng and Kang (2012). To sum up, the algorithm using fragmentary image block to reconstruct original image proposed in this paper is workable for anti-illegal watermark removal and copyright information protection.

Table 2 PSNR comparison between legal and unlawful watermark removal

	Legitimate image mosaic tampering		*Image stitching illegal tampering*	
	Peng and Kang (2012)	*Ours*	*Peng and Kang (2012)*	*Ours*
F-16	42.08	51.66	38.34	26.12
Lena	40.22	55.47	36.21	21.42
Peppers	43.65	48.19	3368	23.18
Girl	47.33	53.46	35.16	25.45
Sailboat	49.31	55.26	39.43	27.62

5 Conclusions

With the rapid growth of new media technology, the digital image technology becomes more absorbed in people's daily life. But in practice, the digital images are often tampered with by various image processing software and spread via network. Some attacks often tamper with certain information in the processing of watermark embedding. Therefore, it is very important to design a watermarking algorithm to protect the image copyright.

This paper proposes the watermarking algorithm characterised by fragmentary image features resistible against image splicing/tampering attacks. It firstly builds the fragmentary image block as local region, then obtains the residual of tampered image through different image characteristics that influence transformation methods. The characteristic value of fragmentary block image is used to distinguish the difference between normal watermarking image and tampered watermarking image after establishing relevant mathematical feature model of residual image. The experiments show that the proposed algorithm can resist the image spicing/tampering attacks. Besides, it has obvious superiority in security and self-recovery after suffering from illegal attacks.

Acknowledgements

This work is supported by Fujian provincial leading project (2017H0029) and Industrial Robot Application of Fujian University Engineering Research Center, Minjiang University (MJUKF-IRA201802).

References

Gao, X.B., Deng, C. and Li, X.L. (2010) 'Geometric distortion insensitive image watermarking in affine covariant regions', *IEEE Trans. on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, Vol. 40, No. 3, pp.278–286.

Ho, Y.A., Chan, Y.K., Wu, H.C. et al. (2009) 'High-capacity reversible data hiding in binary images using pattern substitution', *Computer Standards and Interfaces*, Vol. 31, No. 4, pp.787–794.

Krewinkel, A., Sunkler, S. et al. (2016) 'Concept for automated computer-aided identification and evaluation of potentially non-compliant food products traded via electronic commerce', *Food Control*, Vol. 2016, No. 61, pp.204–212.

Kurnia, S., Karnali, R.J. and Rahim M.M. (2015) 'A qualitative study of business to business electronic commerce adoption within the Indonesian grocery industry: a multi theory perspective', *Information and Management*, Vol. 52, No. 4, pp.518–536.

Li, L.D., Pan, J.S. and Yuan, X.P. (2011) 'High capacity watermark embedding based on invariant regions of visual saliency', *IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E94-A, No. 2, pp.889–893.

Liang, W., Huang, W., Chen, W., Li, K-C. and Li, K. (2019) 'Hausdorff distance model-based identity authentication for IP circuits in service-centric internet-of-things environment', *Sensors*, Vol. 19, p.487, DOI: 10.3390/s19030487.

Liang, W., Jiang, Y., Peng, L., Xie, Y. and Xiao, W. (2015) 'A fixed blocking based dispersed information hiding algorithm for multiple carriers', *J. Comput. Theor. Nanosci*., Vol. 12, No. 10, pp.3722–3726.

Lu, H., Wang, J., Kot, A.C. et al. (2002) 'An objective distortion measure for binary document images based on human visual perception', *Int. Conf. on Pattern Recognition*, IEEE Press, New York, Vol. 4, pp.239–242.

Pan, J.S., Luo, H. and Lu, Z.M. (2006) 'A lossless watermarking scheme for halftone image authentication', *Int. Journal of Computer Science and Network Security*, Vol. 6, No. 28, pp.147–151.

Peng, A. and Kang, X. (2012) 'Robust median filtering detection based on filtered residual', in *Digital Forensics and Watermarking*, pp.344–357, Springer, Berlin, Heidelberg.

Robertson, G.R., Aburdene, M.F. and Kozick, R.J. (1996) 'Differential block coding of bi-level images', *IEEE Trans. Image Processing*, Vol. 38, No. 11, pp.1368–1370.

Santhi, V., Thangavelu, A. and Arulmozhivarman, P. (2013) 'Adaptive invisible watermarking model for securing ownership rights of digital images using SIFT features in bi-orthogonal wavelet domain', *International Journal of Tomography and Simulation*, Vol. 23, No. 2, pp.64–73.

Seo, J.S. and Yoo, C.D. (2006) 'Image watermarking based on invariant regions of scale-space representation', *IEEE Trans. on Signal Processing*, Vol. 54, No. 4, pp.1537–1549.

Tsai, J., Huang, W., Kuo, Y. and Horng, M. (2012) 'Joint robustness and security enhancement for feature-based image watermarking using invariant feature regions', *Signal Processing*, Vol. 92, No. 6, pp.1431–1445.

Tsi, C.L., Chiang, H.F., Fan, K.C. et al. (2005) 'Reversible data hiding and lossless reconstruction of binary images using pair-wise logical computation mechanism', *Pattern Recognition*, Vol. 38, No. 11, pp.1993–2006.

Tzeng, C.H. and Tsai, W.H. (2003) 'A new approach to authentication of binary images for multimedia communications', *Letters*, Vol. 7, No. 9, pp.443–445.

Wang, Y. and Zhou, Z. (2018) 'Spatial descriptor embedding for near-duplicate image retrieval', *International Journal of Embedded Systems*, Vol. 10, No. 3, pp.241–247.

Wu, M., Tang, E. and Liu, B. (2004) 'Data hiding in binary image for authentication and annotation', *IEEE Trans. Multimedia*, Vol. 6, No. 4, pp.528–538.

Yang, H. and Kot, A.C. (2004) 'Data hiding for bi-level documents using smoothing technique', in *Proc. of Int. Symposium on Circuits and Systems*, IEEE Press, New York, Vol. 5, pp.692–695.

Yang, H. and Kot, A.C. (2006) 'Binary image authentication with tampering localization by embedding cryptographic signature and block identifier', *IEEE Signal Processing Letters*, Vol. 13, No. 12, pp.741–744.

Yang, H. and Kot, A.C. (2007) 'Pattern-based data hiding for binary image authentication by connectivity-preserving', *IEEE Trans. Multimedia*, Vol. 9, No. 3, pp.475–486.

Zhu, D.D., Zhang, X.P. and Zhang, Y.L. (2013) 'A new image watermarking algorithm using NSCT and Harris Detector in green manufacturing', *Applied Mechanics and Materials*, Vol. 340, pp.277–282.

Zuo, J. and Yu, G. (2017) 'A novel chaotic key-based algorithm for still images', *International Journal of Computational Science and Engineering*, Vol. 15, Nos. 1/2, p.96.