Journal of Information Hiding and Multimedia Signal Processing ©2016 ISSN 2073-4212
Ubiquitous International Volume **7**, Number **3**, May **2016**

Double Reversible Watermarking Algorithm for Image Tamper Detection

Zheng-Wei Zhang[1,2]

[2]College of Computer Engineering, Huaiyin Institute of Technology
Huaian, Jiangsu 223003, China
zzw49010650@sina.com

Li-fa Wu[1], Hai-guang Lai[1], Hua-bo Li[1], Cheng-hui Zheng[1]

[1]College of Command Information System, PLA University of Science and Technology
Nanjing, Jiangsu 210007, China
wulifa@vip.163.com, lite@263.net, huabolee@163.com,chh.zheng@163.com

Received September, 2015; revised December, 2015

Abstract. *Since existing methods show low tamper detection efficiency and inaccurate positioning, a dual reversible watermarking algorithm with tamper detection based on the multi-scale decomposition is proposed. To begin with, the original image is decomposed into multi-scale image blocks that are non-fixed size but yield high homogeneity. Afterwards, the singular value decomposition is performed on each sub-block and the singular value norm is extracted. Meanwhile, logistic chaotic mapping is used to generate the first authentication watermark. Then, the mean pixel values of each sub-block are calculated for the second authentication watermark. Finally, the logistic chaos is used to design a mapping function between sub-blocks and sub-blocks, and the dual authentication watermarks are embedded into the corresponding mapping block through the generalized difference expansion. The simulation results show that the algorithm not only has high embedding capacity and superior visual quality, but also is very sensitive to tampering, yields high detection efficiency, and can accurately locate the tampered areas..*
Keywords: Reversible watermarking; Tamper detection; Dual authentication; general difference expansion; Multi-scale decomposition.

1. **Introduction.** Traditional reversible watermarking algorithms can restore the original image with lossless fidelity but cannot accurately detect tampering in the process of watermark embedding and extraction [1, 2]. For instance, in regard to regional health information sharing, in addition to being able to prove the true origin of the original medical image, it is also very important to authenticate the integrity of the image in the transmission process. Authenticating the integrity of medical images is also known as tamper detection. Early tamper detection algorithms only judged whether an image had been distorted or not. Currently, however, tamper detection algorithms require precisely positioning the tampered area. Generally, the tamper detection algorithms for reversible watermarking can be divided into two types: one is fixed-sized blocking, and the other is blocking of non-fixed sizes. However, both of these algorithms require extracting the feature value from the image block and embedding it as a tamper authentication watermark. In the authentication phase, whether an image block has been tampered or not can be judged by comparing the recalculated feature value and the extracted feature value. In terms of tamper detection based on fixed-sized blocks, Chiang *et al.* [3] divided the

image into blocks of 4×4 pixels, counted the average pixel value of each block as the recovery feature, and embedded the feature by the difference expansion method. Guo *et al.* [4] first divided the image into blocks of 2×2 pixels, used hash function to calculate the features of each block and embedded the feature as a watermark. In order to improve detection accuracy, the method was to divide each image block into multiple levels after blocking. Li *et al.* [5] divided the image into the important region and the background region, and employed the method by Chiang *et al.* to authenticate the important region. The fixed-size blocking method is simple to operate, has low computational complexity but also some drawbacks: 1) the accuracy of tamper detection lies in the block size. The smaller the block is, the more accurate tamper detection would be and the more authentication watermark information it requires embedding; 2) it does not fully consider the high correlation between the image pixels and their regional features. Due to the deficiencies of the fixed-sized blocking method, Kim *et al.* [6] and Deng *et al.* [7] had introduced the blocking method without fixed size, and blocking size was selected according to their feature self-adaption. The two algorithms not only had fully considered the regional features of the image blocks, but also had rather large advantages in the embedding capacity and tamper detection accuracy.

Traditional tamper detection algorithms are to divides the original images into blocks, and then embed loss less them into corresponding sub-blocks by extracting sub-block features by form of the single authentication watermark, thus completely embedding the authentication watermark. Such algorithms are characterized by low tamper positioning accuracy, accompanied by a high false alarm rate and missed alarm rate. For example, a fragile watermarking algorithm for tamper detection was presented in Literature [8], in which the 4-bits watermark information was embedded in each sub-block of 8×8 pixels for tamper positioning. The algorithm could reduce the false alarm rate as per the status of adjacent sub-blocks, but fails to precisely locate the tampered areas. Although Kim [4] made use of non-fixed block division, but using the average values of the blocks as the authentication features would cause tampering attacks. Phadikar *et al.* [9] advocated using the average values of image blocks as authentication watermarks and using a modified technique of quantification index modulation to realize embedding. This algorithm had high computational efficiency, but tamper detection accuracy is low.

In this paper, a dual reversible watermarking algorithm with tamper detection based on based on the multi-scale decomposition is put forward. First, multi-scale decomposition is used to divide the original images into blocks, which can effectively overcome the shortcomings of the fixed division method; then according to their image feature, two unrelated feature values are extracted from the divided sub-blocks as dual authentication watermarks, thereby effectively improving the location accuracy of tamper detection and reducing the false alarm rate and missed alarm rate.

2. **Theoretical Knowledge.**

2.1. **Multi-scale decomposition[10].** An image F is divided into multiple scales from a whole to parts, thus obtaining sub-image blocks $F_{i,j}$ at different scales, where *i= 1, 2,,d* is denoted as the segmentation scale; $j = 1, 4^{i-1}$ is denoted as the number of sub-blocks at each scale. Due to the limited size of the image, the segmentation scale is also limited. The segmentation method is displayed in Figure 1. From left to right there is segmentation from the 1^{st} to the 3^{rd} scales, respectively. The whole image is the sub-blocks F1,1 obtained after being decomposed at the 1st scale, and then the whole image is divided into four sub-blocks $F_{2,1}, F_{2,2}, F_{2,3}$ and $F_{2,4}$; each sub-block is called a second scale sub-block, and then they are divided until they reach the maximum scale set.

(a) The 1st scale (b) The 2nd scale (c) The 3rd scale

FIGURE 1. Multi-scale segmentation of Lena image

FIGURE 2. Original image

As the traditional multi-scale decomposition also belongs to fixed-sized block decomposition method, this paper makes an improvement of the multi-scale decomposition. The improved image multi-scale decomposition is to divide a rectangular image into 4 equal-sized square blocks, and then determine whether or not these four square blocks meet the homogeneity criterion. If it is satisfied, the current block maintains unchanged; otherwise it continues to be decomposed into four square blocks, and determines whether or not they meet the criterion, until all the blocks meet the given criterion. The decomposition criterion can be expressed as:

$$|P_i - P_{ave}| > (g_l - 1) \times \gamma \tag{1}$$

In Formula (1), P_i and P_ave are the gray value of any pixel and the average gray value of all pixels in a square block, respectively; g_l is the gray level of a pixel; γ is a decimal in the range of [0,1]. The criterion is, when the guidelines when the absolute value of the difference between the gray value of either pixel and the average gray value of all pixels in the square block is greater than $(g_l-1)\times\gamma$, the block needs to be further divided, as shown in Figure 2 and Figure 3. As per the block division method, it divides images into unfixed sizes. Also from the perspective of the division results, the image blocks decomposed have pixels with high homogeneity, which are suitable for lossless watermark embedding. As specified in the algorithm, the minimum block size is 4×4. After multi-scale decomposition, the size of each image block is $2^{2+n} \times 2^{2+n}, n \in 0, 1, 2, 7$. The size information of each block can be converted into binary form. Each of the decomposed sub-blocks is coded by the sub-block size, as shown in Table 1: After multi-scale decomposition, the image sub-blocks obtained are sorted (from top to bottom, from left to right), and the scale information of each sub-block is recorded sequentially as per the ordering result, thereby constituting the decomposition information q of the original image. Given there are a small number of large-sized blocks decomposed, Huffman encoding [11] can be used

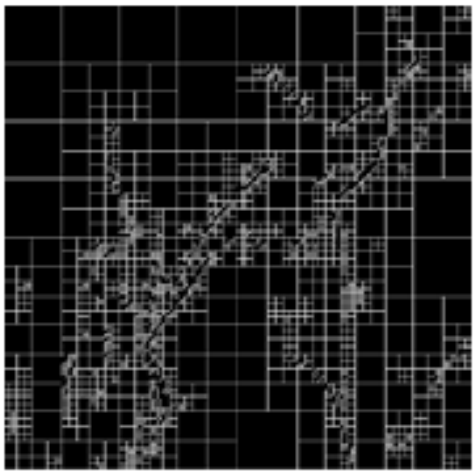

FIGURE 3. The generated block map after modified multi-scale decomposition

TABLE 1. Scale coding of image block after multi-scale decomposition

Size / pixels	**code**	**Size / pixels**	**code**
4× 4	000	64×64	100
8×8	001	128×128	101
16×16	010	256×256	110
32×32	011	512×512	111

to further reduce the length of the image decomposition information, denoted as Huf (q). For security of the algorithm, the length and encode table of the parameter Huf (q) are sent to the recipient in form of a secret key.

2.2. **Singular Value Decomposition [12].** The Singular value decomposition (SVD) transform is orthogonal transformation, and it can diagonalize a matrix. It can be found from the theory of image processing that an image is a real matrix composed of non-negative elements, then an image $F_{m\times n}$ can be decomposed into $F = USV^T$ based on the singular value decomposition theory, where U and V are orthogonal matrices of mm and nn, respectively. The superscript T denotes the matrix transpose. S is a diagonal matrix in which all are 0 except for the values in the diagonal. $S = diag(\lambda_1, \lambda_2, \lambda_3, , \lambda_r, 0, , 0)$. The diagonal values are the singular values of the matrix A and meet $\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \ \geq \lambda_r \geq \lambda_{r+1} = \ = \lambda_m = 0$, where r is the rank of S and equals the number of non-zero singular values. This paper selects the singular value feature of the image as one of authentication watermarks, because the singular values of the image have good stability. That is, when the image is subjected to less interference, its singular values do not change much. In addition, the singular value feature of the image embodies the intrinsic characteristics of the image itself rather than the visual characteristics.

2.3. **Reversible image watermarking scheme based on generalized difference expansion.** Tian[13] proposed that the expansion algorithm based on the adjacent pixels was to conduct integer transform of any one of the image pixels $P = (x, y)$ and get the mean value l and the difference value h. Accordingly, the mean value l and the difference value h can lossless restore the original image pixel values x and y after the inverse transform. Direct transform: $l = \frac{x+y}{2}$, $h = xy$

Inverse transform: $x = l + \frac{h+1}{2}$, $\mathrm{y} = l - \frac{h}{2}$

The resulting difference h is shifted left 1 bit, and the watermark is embedded into its least significant bit, and this is the difference expansion. Its mathematical expression is: $h' = 2h + b$. Meanwhile, the pixel values obtained by embedding the difference expansion into the watermark information may cause the pixel overflow [14], so *x, y* acquired by inverse transform should be limited to the range of [0,255], or it will no longer be reversible in watermark extraction and image restoration. Therefore, h' should be restricted: $\mid h' \mid \leq min(2(255 - l), 2l + 1)$.

Compared to the adjacent pixel expansion algorithm presented by Tian, generalized difference expansion algorithm [15] makes more fully use of the redundant information between adjacent pixels. It picks up a plurality of adjacent pixels for processing, and can be used to embed more watermark information. This paper uses this method for information embedding of the selected the original image pixel blocks. Suppose $X = (x_0, x_1, x_2, x_3, , x_{n-1})$ is a set of pixel values, the direct transform of the generalized integer transform is:

$$\bar{x} = \sum_{i=0}^{n-1} a_i x_i / \sum_{i=0}^{n-1} a_i \tag{2}$$

$$\begin{aligned} d_1 &= x_1 - x_0 \\ d_2 &= x_2 - x_0 \\ &\vdots \\ d_{n-1} &= x_{n-1} - x_0 \end{aligned}$$

For a group of pixel interpolations $d_1, d_2, , d_{n-1}$, Equation (3) can be used separately to hide 1 bit watermark information b:

$$d_i^{'} = 2 \times d_i + b \tag{3}$$

Where, d_i' represents the difference of the pixel pair after embedding watermark. It requires the watermark embedding process not to cause the overflow of image pixel values. The corresponding inverse transform is:

$$x_0^{'} = \bar{x} - \sum_{i=1}^{n-1} d_i^{'} / \sum_{i=0}^{n-1} a_i \tag{4}$$

$$\begin{aligned} x_1^{'} &= x_0^{'} + d_1^{'} \\ x_2^{'} &= x_0^{'} + d_2^{'} \\ &\vdots \\ x_{n-1}^{'} &= x_0^{'} + d_{n-1}^{'} \end{aligned}$$

A set of pixel values $\mathrm{X}^{'} = (x_0^{'},\ x_1^{'},\ x_2^{'},\ \ x3,\ \ \ldots,\ x_{n-1}^{'})$ is generated by the generalized difference expansion algorithm, in which the mean of the group pixels is:

$$\bar{x}^{'} = \sum_{i=0}^{n-1} a_i x_i^{'} / \sum_{i=0}^{n-1} a_i \tag{5}$$

After deduction and calculation, $\bar{x}^{'} - \bar{x} = 0$ Visibly a group of pixels have the same group mean value after the generalized difference expansion transform. After using the generalized difference expansion algorithm to embed information into the pixel blocks, the mean value of the block pixels should be unchanged, and that is a fairly strict requirement. Hence, since the approximate smoothness of each pixel block before and after embedding

watermarks is invariant, using this in variance property can identify the information embedding location and thus replace location marking figures that occupy a lot of space [16].

2.4. **Logistic mapping [17].** Logistic mapping is a simple chaotic mapping system and can be denoted by Equation (6).

$$x_{n+1} = \mu x_n (1 - x_n) \tag{6}$$

where $\mu \in (0, 4]$. Sequence pair initial value generated by logistic mapping is highly sensitive. That is, when x_0 takes different values, the value sequence of x shows different states. In addition, the sequence codomain generated by logistic mapping is [0, 1]. In this paper, the logistic chaotic mapping is used to construct a mapping function between image sub-blocks and sub-blocks after multi-scale decomposition. For instance, the authentication watermark sequence generated in the self-block is embedded into the corresponding mapping block, instead of embedding the authentication watermark into the self-block, so as to achieve tamper detection. Thus, different sub-blocks constitute a certain mapping relationship to effectively fight against collage attacks.

3. **Algorithm design.** In order to improve the accuracy of tamper detection, this paper adopts the dual watermarking detection method to detect whether or not the watermarked image has been tampered. Provided the original image size is $N_0 \times M_0$, before creating watermark, first edge enhancement is processed to the original image, so the image size is $N \times M$, where N and M are multiples of 4. After embedding the watermark, the watermarked image is output in the original size. Before conducting tamper detection of the image, the image size is enhanced first. After tamper detection of the image, output the image in the original size.

3.1. **Creation of authentication watermark.** In this algorithm, the double authentication watermarks needed to be embedded consists of two parts:
(1) Generation of authentication watermarking The singular value decomposition of each sub block I_p generated by the multi scale decomposition is carried out, namely: $I_p = U_p S_p V_p^T$
Its norm is: $Cou_p = \sqrt{\sum_{i=1}^{n} \left(\sigma_p^i\right)^2}$
Where, σ_p^i is the ith singular value of the sub-block I_{1p}. The ratio between the largest singular value σ_p^1 and the norm Cou_p in the sub-block I_{1p} is calculated as Equation (7):

$$k_{p1} = {}^{\sigma_p^1}/_{Cou_p} \tag{7}$$

The logistic chaotic mapping is created byk_{p1}. Since the value k_{p1} calculated by Equation (7) ranges from (-1, 1), the logistic chaotic mapping falls within (-1, 1). Therefore, in order to expand the key-space, we choose $k_{p2} = -k_{p1}$ as the second secret key. The final secret key for the logistic chaotic map is $k_p = k_{p2} + k_{p1}$. Let k_p be the initial value of the chaotic mapping, and the real value chaotic sequence of length 4 is $x_p^i, i \in \{1, 2, 3, 4\}$. Since the sequence mean produced after the logistic chaotic mapping is zero, 0 is used as the threshold for x_p^i binarization, namely: $w_p^i = \left(sgn(\mathrm{x}_p^i) + 1\right)/2$, $\mathrm{i} \in \{1, 2, 3, 4\}$, where, sgn(.) is the sign function. So far the first authentication watermark generation process has been completed. The first authentication watermark generated by each sub-block is denoted by four-bit binary number.
(2) In this paper, the generalized difference expansion is employed for embedding feature watermarks. The block pixels remain unchanged after embedding information into the pixel blocks using the generalized difference expansion method, which is a fairly strict

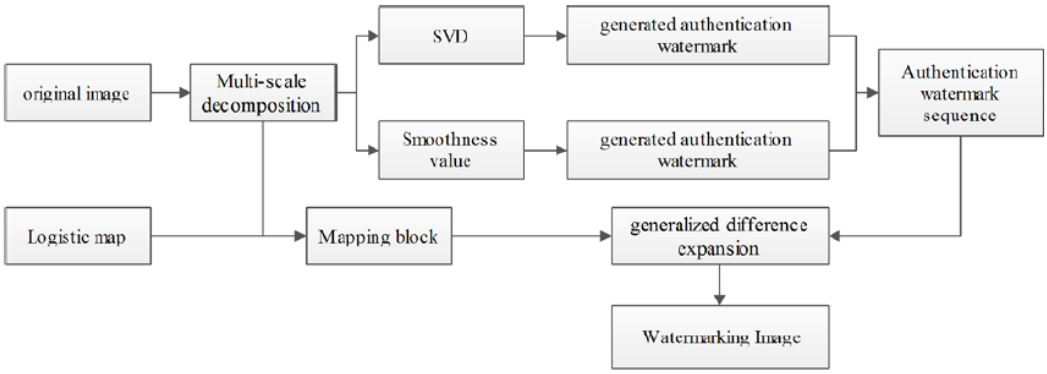

FIGURE 4. Watermark embedding process

requirement. By calculating the average pixel value of each sub-block after the original image is decomposed, we take the average pixel value of each sub-block as the second authentication watermark. The average pixel value of each sub-block is created as follows:

$$\bar{x}_i = \sum_{j=1}^{n} x_{i,j}/n \tag{8}$$

In Formula (8), $\bar{x}_i$ is the average pixel gray value of the sub-block i after multi-scale decomposition; $x_(i,j)$ is the gray value of the pixel j in the sub-block i; n is the number of pixels in the sub-block i. Since the average pixel value of sub-images is between [0,255], this paper denotes the dual authentication watermark using an 8-bit binary number.

3.2. **Watermark embedding.** To achieve the dual authentication of image watermarking, we need to set up the dual authentication watermarks. Since the singular values of an image have good stability, when the image is subjected to less interference, its singular values will not vary greatly, and so we take advantage of this feature to constitute the first authentication watermark of the image. In addition, after embedding the watermarked through the generalized difference expansion method, the average value of all pixels in image sub-block do not change. Therefore, we will take the average value of all pixels in each image sub-block as the second authentication watermark. This paper has set the minimum size of sub-blocks as created through multi-scale decomposition to be $4 \times S4$, so the generalized difference expansion can embed 15-bit watermark information. To decompose large sub-blocks, in order to unify and reduce the computational complexity, we also select the former 16 pixels in the sub-blocks for watermark embedding. In this algorithm, the watermark embedding process is shown in Figure 4, and the specific steps are as follows:

Step1 is to carry out multi-scale decomposition of the original image I, and to send the decomposed information produced (the length and encode table of Huf (q)) in form of secret key to the recipient.

Step2 is to sort each of the decomposed sub-blocks I_P, ($0 \leq p \leq n, n$ is the total number of sub-blocks obtained by decomposing the original image) from top to bottom, and from left to right, and to gain the feature value of each of the sorted sub-blocks I_P as the authentication watermark. By singular value decomposition of the sub-blocks I_P, calculate the ratio between the maximum singular value and the norm Cou_p as the first authentication watermark. Then calculate the average pixel of the sub-blocks I_P as the second authentication watermark.

Step3 is to build an overflow graph. After embedding information by difference expansion,

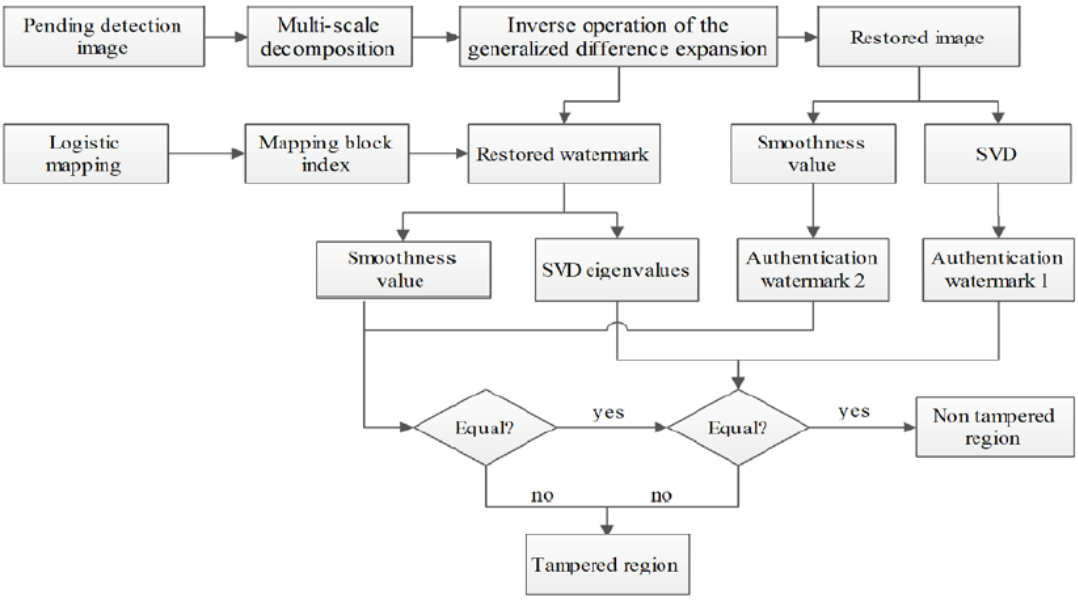

FIGURE 5. Watermark extraction and tamper detection process

mark the pixel points that fall out of the image gray value range in the overflow graph. The compressed overflow graph and authentication watermarks are embedded into the appropriate mapping blocks together by the generalized difference expansion technique. In this algorithm, there are 15 bits of watermark information embedded in each sub-image block, where the first watermark occupy 4 bits; the second watermark occupy 8 bits; and the remaining 3 bits are used for storing overflow graph information.
Step 4 is to use logistic chaotic maps to construct a mapping function between image sub-blocks and sub-blocks, and to embed the self-producing watermark authentication information into the corresponding mapping blocks. Save Logistic chaotic map keys so that it can be used to extract and detect the watermark information.
Step 5 is to regroup each sub-block I_P embedded with watermarks into watermarked images.

3.3. **Tamper detection of watermarks.** For image sub-blocks embedded with watermarks, it would be easy to extract watermark information since image pixels have the parity to the difference. Watermark extraction and tamper detection processes in this algorithm are shown in Figure 5, and the concrete steps are as follows:

Step1: the recipient receives from the sender the multi-scale decomposition information of the original image through the secret passage, in order to carry out multi-scale decomposition of the image I'.
Step2 is to sort the decomposed sub-blocks I_P, $(0 \leq p \leq n, n$ is the total number of sub-blocks obtained by decomposing the original image) from top to bottom, and from left to right. For each sub-block sorted, it is necessary to perform inverse operation of the generalized difference expansion, extract the authentication watermark information and the overflow marking information, while restoring each image sub-block.
Step3 is to build a one-to-one mapping between the sub-blocks by logistic chaotic function according to the key. Assume the corresponding mapping block for the restored sub-blockI'_P is $I'_i(0 \leq p \leq n, n$ is the total number of sub-blocks obtained by decomposing the original image). Generate a dual authentication watermark for the restored sub-block I'_P following Section 3.1, and extract the dual authentication watermark of the sub-block

FIGURE 6. Original image

TABLE 2. The performance effect of 3 original images after multi-scale decomposition

original image	γ	**The total number of blocks**	**Capacity/bit**	**PSNR/dB**
Plane	0.018	5548	83220	43.78
Lena	0.025	4008	60120	44.34
Baboon	0.042	7664	114960	44.62

I'_P from the corresponding mapping block I'_i by using the parity of image pixels to the difference.

Step4 is to compare the authentication watermark of the SVD feature value 'generated by the restored sub-block I'_P and the first four bits of binary numbers of the watermark information extracted from sub-blockI'_i. If they are unequal, the sub-block area has been tampered; if they are equal, further detection should be made to judge whether the area has been tampered.

Step5: After Step4, if they are equal, further detection should be made to judge whether the area has been tampered. Compare the average pixel of the restored sub-block I'_P with the middle eight bits of binary numbers of the watermark information extracted from sub-block I'_i (From Bit 4 to Bit 11). If they are unequal, the area has been tampered; if they are equal, the area has not been tampered. (In this paper, the second authentication watermark can be first used for tamper detection, following by using the first authentication watermark for further detection, the effect is the same).

Step 6: after Step4 and Step5, mark the tampered sub-block areas on the image to be detected, in order to complete tamper detection of the watermark images.

4. **Experimental Results and Analysis.** In this experiment, three images are selected as the original carriers: Plane, Lena and Baboon, which are all 512×512 standard images in 8-bit gray-scale (Figure 6). All the experimental results are achieved in the windows XP operating system under the MatlabR2012b experimental platform. The experiment places emphasis on the reversibility of the algorithm, the visual quality of watermark images, accuracy of tamper detection and accuracy of localization. The experimental design is as follows:

1) Use multiple scales to decompose the original image, and test the embeddable watermark capacity and decomposition adjustment factor;

2) Reversibility of the algorithm, which is the consistency between the restored test watermark image that has not been tampered and the original image;

3) The visual quality of image watermarking, which is the similarity between the image watermark generated and the original image after embedding the authentication watermark;

TABLE 3. Embedding capacity and PSNR comparison under different γ

original image	γ	**Capacity /bit**	**PSNR / dB**
Plane	0.018	83220	43.78
Plane	0.024	65220	45.22
Lena	0.025	60120	44.34
Lena	0.03	54600	45.67
Baboon	0.042	114960	44.62
Baboon	0.055	78360	46.29

(a) The original image (b) The watermarked image (c) The tampered image (d) The detection result

FIGURE 7. Authentication watermark embedding and tamper localization effect

4) Compare this algorithm with methods proposed in literature [5] and [6] regarding the accuracy of tamper detection and regional positioning. The criterion for multi-scale decomposition of the image is: $\|P_i - P_ave\| > (g_l - 1) \times \gamma$. Therefore, different values of will lead to different image decomposition effects. We call γ as the decomposition adjustment coefficient. For the specific relationship between the image decomposition coefficient and the watermark embedding capacity, see Table 2:

The embedding capacity listed in Table 2 is only the amount of embeddable watermark information by using generalized difference expansion. With different values of the decomposition adjustment coefficients and different texture structures of image carriers, there are different numbers of blocks that are subjected to multi-scale decomposition. Further, the resultant number of watermark information to be embedded would be diverse, as shown in Table 3.

When the watermark image has not been tampered, the recalculated feature information is exactly the same as the information extracted from the watermark image, and there is also no difference between the finally restored image and the original image, which verify that the algorithm is completely reversible.

Multi-scale decomposition is performed on the original image, and the sub-blocks are 4×4 regions of complex texture, while the larger sub-blocks are smooth. We embed feature information of the same size into sub-blocks of different sizes. Comparatively speaking, there are a large amount of watermark information embedded in these complex regions, and a small amount of watermark information embedded in the smooth regions. Hence, by this algorithm, there will be good visual quality when embedding watermark information of the same size. The watermarked image (Figure 7 (b)) is tampered, as shown in Figure 7 (c). After the tamper detection of the tampered image, the detection results are shown in Figure 7 (d), where the region has been identified as being tampered is marked in white. The tampered areas in the image are of complex texture, and therefore the positioned tamper areas are composed of a number of small-sized sub-blocks. In order to test the tamper detection accuracy of this algorithm, the experiment has also

(a) The original image (b) The watermarked image (c) The tampered image (d) The detection result

FIGURE 8. Authentication watermark embedding and tamper localization effect

tampered the Plane image which is embedded with watermarks, as shown in Figure 8 (c). The results of tamper location detection are exhibited in Figure 8 (d), showing that the tampered areas can be accurately located by this algorithm. The specific positioning accuracy is demonstrated in Table 4.

TABLE 4. The effect of the tamper image localization under different algorithms

Tampered image	Tampered area size	The number of Localization to the tampered block		
		This algorithm	Literature [5] algorithm	Literature [6] algorithm m
Fig.7(c)	32×32	42	64	52
Fig.8(c)	32×64	28	128	34

In Table 4, many tampered blocks have been localized by the algorithm advocated in Literature [5], because its algorithm uses a fixed-sized (4×4) sub-block approach. On the other hand, the algorithm proposed in this paper has localized a relatively small number of tampered blocks, because it resorts to multi-scale decomposition for blocking, and few decomposition blocks are of smooth texture. Using the proposed algorithm, Figure 7(c) has less tampered areas than Figure 8(c), but more tampered blocks have been detected since the tampered areas in Figure 7(c) are complicated and a large number of sub-blocks are obtained by multi-scale decomposition. The tampered areas in Figure 8(c) are smooth and relatively a small number of sub-blocks are decomposed. Moreover, the number of authorization blocks detected by the algorithm in Literature [6] is between the two aforementioned algorithms. As it employs the self-adaptive decomposition method to divide images into blocks, it detects less tampered blocks than Literature [5], but more tampered blocks than the proposed algorithm in this paper, since we adopt the dual authentication watermarking method which has lower misjudgment rate through dual authentication. The mean value of blocks as adopted by Literature [6] will be taken as the authentication feature and suffer from tampering attacks, which will have certain judgment errors. For this algorithm, fewer sub-blocks are used to locate the tampered areas, so it has higher position accuracy. In the meantime, using the dual authentication watermark to detect and locate the tampered areas will yield a lower misjudgment rate. The watermarking embedding method is an important step to determine the robustness and transparency of the whole digital watermarking system. A good algorithm can not only guarantee the robustness, but also improve the accuracy of image watermarking.

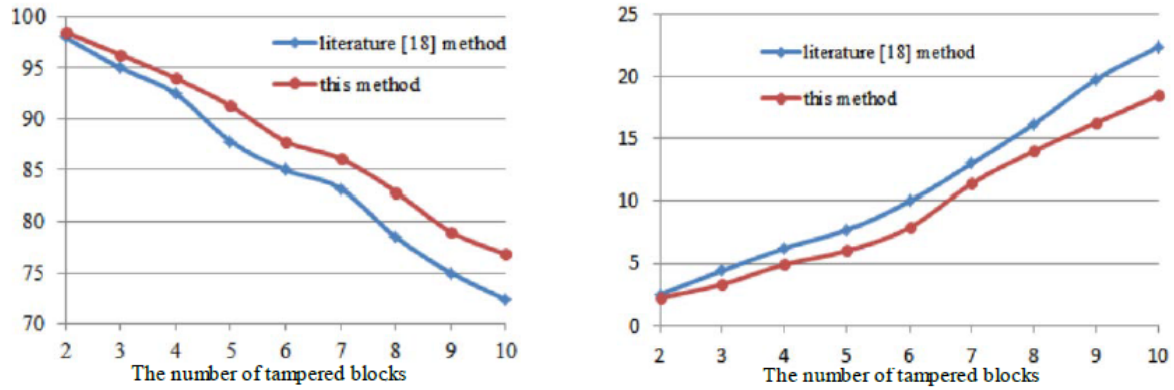

FIGURE 9. Comparison of the localization accuracy of the algorithm (40 experimental means)

The accuracy of tamper detection is calculated by the following two aspects:
(1) The positive detection rate (TPR), which is the ratio of the total number of all the tampering blocks correctly detected by the block;
(2) The negative detection rate (TNR), which is the ratio of the total number of blocks that have changed to the total number of the tampered blocks.
Image tamper localization accuracy can be explained by the positive detection rate and negative detection rate. The pixel value of one or more pixel blocks of 32 of the secret image is randomly selected. Figure 9 (a) shows the mean of the positive detection rate after the 40 experiments; Figure 9 (b) shows the mean value of the negative detection rate after the 40 experiments.

From Figure 9 (a), we can know, with the increase of tampered blocks, two methods of positive detection rate showed a downward trend, however this method is obviously better than the literature [18]; From Figure 9 (b) shows the tampered blocks increases, leading to a negative detection rate showed an upward trend, and this method rises slowly relative to the literature [18] method. Of course, if tampering leads to information error of decomposition blocks, the negative detection rate will rise sharply. Comprehensive analysis in Figure 9 curve data, compared with the method of literature [18], the tamper localization accuracy of this method can be increased by almost 4%.

5. **Conclusion.** The image tamper detection techniques have played an increasingly important role in digital image watermarking security. In this paper, a dual reversible watermarking algorithm with tamper detection based on the multi-scale decomposition is presented, which performs multi-scale decomposition on the original image, extracts the image block dual features as dual authentication watermarks and embeds them into corresponding sub-blocks by the generalized difference expansion. Since multi-scale decomposition is used, there are a small amount of watermark information embedded in the smooth regions, and a large amount of watermark information embedded in the regions of complex texture, so the images embedded with authentication watermarks can have superior visual quality. In addition, extracting different feature values from decomposed sub-blocks as the authentication watermarks can effectively enhance the accuracy of tamper localization and reduce the false alarm rate and missed alarm rate.

Acknowledgment. This work is supported by the Jiangsu province Natural Science Foundation of China (No.BK20131069).The authors do not have any possible conflicts of interest.

REFERENCES

[1] S. W. Weng, J. S. Pan, Reversible Watermarking Based on Eight Improved Prediction Modes, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 5, no. 3, pp. 527-533, 2014.

[2] S. W. Weng, J. S. Pan, Reversible watermarking based on multiple prediction modes and adaptive watermark embedding, *[J]. Multimedia Tools and Applications*, vol. 72, no. 3, pp. 3063-3083, 2014.

[3] K. H. Chiang, K. C. C. Chien, R. F. Chang et al, Tamper detection and restoring system for medical images using wavelet- based reversible data embedding, *[J]. Journal of Digital Imaging*, vol. 21, no. 1, pp. 77-90, 2008.

[4] X. T. Guo, T. G. Zhuang, Lossless watermarking for verifying the integrity of medical images with tamper localization, *[J]. Journal of Digital Imaging*, vol. 22, no. 6, pp. 620-628, 2009.

[5] C. L. Li, Y. H. Wand, B. Ma et al, Tamper detection and self-recovery of biometric images using salient region-based authentication watermarking scheme, *[J]. Computer Standards and Interfaces*, vol. 34, no. 4, pp. 367-379, 2012.

[6] K. S. Kim, M. J. Lee, J. W. Lee et al, Region-based tampering detection and recovery using homogeneity analysis in quality-sensitive imaging, *[J]. Computer Vision and Image Understanding*, vol. 115, no. 9, pp. 1308-1323, 2011.

[7] X. H. Deng, Z. G. Chen, F. Zeng et al, Authentication and recovery of medical diagnostic image using dual reversible digital watermarking, *Journal of Nanoscience and Nanotechnology*, vol. 13, no. 3, pp. 2099-107, 2013.

[8] C Li, Digital fragile watermarking scheme for authentication of JPEG images, *[J]. IEE Proc.-Vis. Image Signal Process*, vol. 151, no. 6, pp. 460-466, 2004.

[9] A. Phadikar, S. P. Maity, M. Mandal, Novel wavelet- based QIM data hiding technique for tamper detection and correction of digital images, *Journal of Visual Communication and Image Representation*, vol. 23, no. 3, pp. 454-466, 2012.

[10] Y. Y. Yan, Z. B. Guo, J. Y. Yang, Face recognition based on multi-scale singular value features, *[J]. J Tsinghua Univ (Sci & Tech)*,vol. 48, no. 10, pp. 1688-1692, 2008.

[11] Y. Q. Li, L.X. Li, Y. H. Liang, Image Watermarking Algorithm Based on Image Characteristics and Huffman Coding, *[J]. Computer Applications and Software*, vol. 30, no. 9, pp. 128-140, 2013.

[12] L. Lei, S. X. Gu, L. Wang, SVD Digital Image Watermarking Algorithm Based on Wavelet Transform, *[J]. Computer Simulation*, vol. 30, no. 9, pp. 169-172, 260, 2013.

[13] J. Tian, Reversible data embedding using a difference expansion, *[J]. IEEE Transactions Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890-896, 2003.

[14] W. Song, J. J. Hou, Z. H. Li, A novel block- classification and difference-expansion based reversible data hiding algorithm, *[J]. Journal of Central South University (Science and Technology)*, vol.42, no. 3, pp. 693-702, 2011.

[15] Z. Q. Chang, J. Xu, Reversible watermarking algorithm with general difference expansion, *[J]. Modern Electronics Technique*, vol. 35, no.20, pp. 84-86, 2013.

[16] C. F. Lee, C.-C. Chang, P. X. Pai et a1, An Adjustable and Reversible Data Hiding Method Based on Multiple-base Notational System without Location Map, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 6, no. 1, pp. 1-28, 2015.

[17] M. Liu , Z. Q. Chen, X. H. Deng, Image tamper detection scheme based on chaotic System and fragile watermarking, *Journal of Computer Applications*, vol. 33, no. 5, pp. 1371-1373, 2013.

[18] X. H. Deng, Z. G. Chen, F. Zeng et a1, Authentication and recovery of medical diagnostic image using dual reversible digital watermarking, *Journal of Nanoscience and Nanotechnology*, vol. 13, no. 3, pp. 2099-2107, 2013.