International Journal of Digital Crime and Forensics
Volume 11 • Issue 1 • January-March 2019

A Reversible Watermarking Algorithm Resistant to Image Geometric Transformation

Jian Li, Nanjing University of Information Science & Technology, Nanjing, China

Jinwei Wang, Nanjing University of Information Science & Technology, Nanjing, China

Shuang Yu, Nanjing University of Information Science & Technology, Nanjing, China

Xiangyang Luo, Zhengzhou Science and Technology Institute, Zhengzhou, China

ABSTRACT

This article proposes a novel robust reversible watermarking algorithm. The proposed watermarking scheme is reversible because the original image can be recovered after extracting watermarks from the watermarked image, as long as it is not processed by an attacker. The scheme is robust because watermarks can still be extracted from watermarked images, even if it is undergone some malicious or normal operations like rotation and JPEG compression. It first selects two circles, which are centred at the centroid and the centre of image. Then, statistic quantities of these two circles are employed for robust watermark embedding by altering the pixels' value. The side information generated by above embedding process will be embedded as fragile watermarks at another stage to ensure the recovery of original image. Experimental results verify the high performance of the proposed algorithm in resisting various attacks, including JPEG compression and geometric transformation.

KEYWORDS

Centre, Centroid, Histogram Shifting, Reversible Watermarking, Robust Watermarking

INTRODUCTION

Reversible watermarking has been one of the hottest research topics in information hiding domain over the past two decades. Unlike the traditional one (Wang and Zhu, 2015), this technique can extract the hidden data and recover host image to be its original condition losslessly. This reversibility feature is widely used in military, medical and other sensitive fields. Creating a new space by losslessly compressing one bit-plane of image to embed data was first proposed by (Fridrich, Goljan & Du, 2001). Tian (2003) proposed a difference expansion (DE) algorithm by calculating pixel difference to afford more capacity. In addition, prediction-error expansion (PEE) was proposed by Thodi and Rordriguez (2004). The existing reversible watermarking algorithms (Wang, Li, Yang & Guo, 2010; Li, Yang & Zeng, 2011; Chen, Sun, Sun, Zhou & Zhang, 2013; Li, Zhang, Gui & Yang, 2013; Ou, Li, Zhao, Ni & Shi, 2013; Wang & Zhu, 2015)) are mostly based on the aforementioned DE, PEE

DOI: 10.4018/IJDCF.2019010108

and histogram shift (HS) techniques. However, they are designed for lossless environment. That is the host image must be transmitted without any attacks such as image compression, geometric attacks, noise etc. Otherwise, the embedded information will no longer be extracted exactly.

Aiming at the problem above, Vleeschouwer et al. (Vleeschouwer, Delaigle & Macq, 2003) proposed a robust reversible method against JPEG compression. By a special circular interpretation of bijective transformation, this method embeds secret data losslessly. At the receiving end, if the host does no experience any attacks, the embedded data can be extracted correctly and the host can be restored to be the same as the initial state. Besides, the hidden data can be still extracted accurately after JPEG compression to some extent. Henceforth, we call such technology as robust lossless data hiding. The drawback of Vleeschouwe et al.'s algorithm is that it may generate salt-pepper noise and spoil the visual quality of host image. In 2008, Ni et al. (Ni, Shi, Ansari, Su, Sun & Lin, 2008) presented a robust lossless algorithm based on statistic histogram modification. The performance of Ni et al.'s method regarding PSNR and robustness is much better than the aforementioned one. Then, a similar scheme was presented by Li (2012). Besides these two schemes carried out in spatial domain, a framework for distortion-free robust image authentication was proposed by Coltuc (2007). This general framework embeds robust data in frequency domain and fragile ones in spatial domain with two stages, which provides inspiration to our work in this paper. Liu et al. (Liu, Ju, Hu, Ma & Zhao, 2015) adopted an intra-prediction model to embed data into integer DCT coefficients in frequency domain. Gao et al. (An, Gao, Li, Tao, Deng & Li, 2012) provided a robust reversible framework based on clustering and wavelet transformation. However, in these above robust lossless schemes, the most focus of robustness is resisting to image compression. Little attention is payed to geometric attacks such as rotation, scale and translation (RST).

To get robustness for RST attacks, we provide a novel robust reversible watermarking algorithm based on Coltuc's framework. The watermark is embedded into the circle areas, which centred at the centroid and the centre of host image. As a result, we can achieve robustness against rotation and other image geometric transformations. Furthermore, because the side information used for recovering host image is also embedded, the proposed watermarking algorithm owns reversibility in lossless environment.

The rest of this paper is organized as follows. Section 2 gives a preliminary about the related work of a robust statistic, relation of centroid and centre. In Section 3, our proposed watermarking algorithm is introduced in detail. The experimental results are given in Section 4, followed by the conclusion in Section 5.

PRELIMINARY

In the literature, watermarking robustness is usually guaranteed by generating some statistical quantities of the image. This paper adopts a special statistic of circle in the image to embed robust information. For resisting more types of attacks, position of the circle for watermarking is also discussed in this Section.

Robust Statistic in a Circle

For a given image, we choose a circle from image like Figure 1. The robust watermark will be embedded in this circle by changing the pixels in it.

In the circle, there is an even number of pixels and the numbers varies from different radius. In addition, the circle will be split into a pair of subsets as shown in Figure 2(a) and Figure 2(b). Subset A consists of pixels marked by "+" while subset B consists of pixels marked by "-". Then a statistical quantity, i.e. the arithmetic average of difference between A and B, denoted by α is calculated by

Figure 1. A selected circle in gray image ‘Lena’

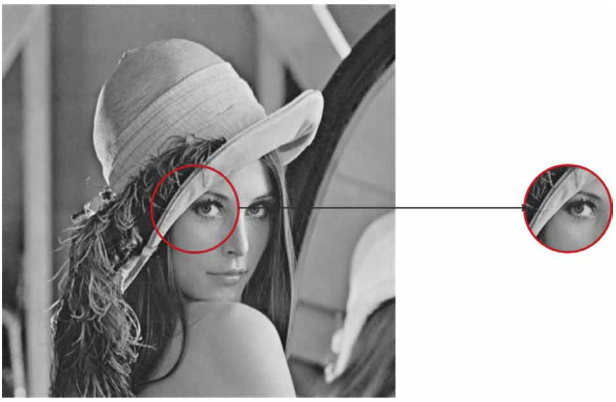
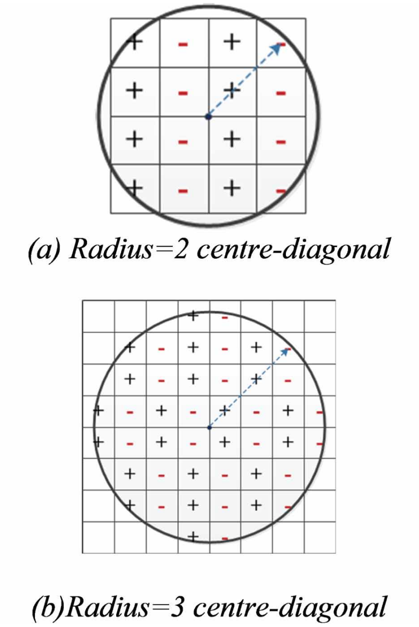


Figure 2. Selected circle with different radius. When radius of circle is rotated to 45º, the number of pixels on the segment is the length of radius. 2 centre-diagonal means that there is 2 pixels on the diagonal radius (a) Radius=2 centre-diagonal (b) Radius=3 centre-diagonal



(a) Radius=2 centre-diagonal

(b)Radius=3 centre-diagonal

$$\alpha = \frac{1}{\mathrm{n}} \sum_{i=1}^{n} \left(\mathrm{a}_{\mathrm{i}} - \mathrm{b}_{\mathrm{i}}\right), \tag{1}$$

where $\mathrm{a}_{\mathrm{i}} \in \mathrm{A}, \mathrm{b}_{\mathrm{i}} \in \mathrm{B}$, n is the number of elements of subset A/B, which is equal to half of pixels’ number in specified circle.

Note that neighboring pixels usually have strong correlation from each other. So the difference α is a random variable with zero mean. Even the host image has been under some attacks, α is still tending to zero. If we change α to make it far away from zero, a robust watermark can be embedded.

For instance, we alter gray value of the pixels marked by "+" as shown in Figure 2. Each pixel adds a variable β to its gray value, and α will be turned into α+β. With large enough β, the absolute value of difference of circle according to formula (1) will be larger than a threshold even under some attacks.

Relation Between Centroid and Centre

As mentioned above, most existing schemes like (Vleeschouwer, Delaigle & Macq, 2003; Ni, Shi, Ansari, Su, Sun & Lin, 2008; Li, 2012; Coltuc, 2007) focused on robustness for image compression. Even though the host has been compressed, the difference between pixels is maintained to some extent. But these statistics are unstable for geometric changes for an image. For instance, if the host image is rotated, the gray values of the pixels in the circles will be changed because of interpolation. I.e., the value will be modified to neighboring pixels. Hence, even if a robust data has been embedded, the alteration of some pixles' value may be erased. The farther away from centre of rotation is, the more likely to be erased. And the difference statistic will not reflect whether the watermark embedded or not.

Circle with appropriate radius is used in this paper, which consists of pixels nearer to the centre to make sure the difference α small. For image compression, rotation and scale attacks, the relative position of the centre in an image is not changed, which means pixels around the centre are quite similar to the original ones. But for translation, the pixels around centre are changed and cannot be used to calculate the statistic any more. In this case, the centroid, namely centre of mass of the host image is employed. The relative position of centriod in an image will not shifted greatly, which means the circle of centroid is retained in some degree after attacks. Hence, the hidden data can be extracted by centroid's circle after translation. This paper adapts two centre points to embedded robust data. It firstly gains two values α_1, α_2 of circles of centre and centroid according to the formula (1) separately. Then if it needs embedding a data, the quantity β is going to be employed to change α_1 and α_2 according Section 2.1, otherwise.

In an image, the position of image centre and centroid may be different or be similar. Refer to Figure 3(a)-Figure 3(d), there are four scenarios: (a) two circles have overlapping portions and the centroid is in the left of centre (b)two circles have overlapping portions and the centroid is in the right of centre (c)two circles has no overlapping portions (d)two circles are overlapped completely. Once we embed a robust watermark, the pixels in the circle of centre are first altered. Then, in case (a) and case (b), the rest non-overlapping area will be changed differently according to the position of last or first overlapping pixel in each row. In case (c), the circle of centroid will be operated the same as the circle of centre again. Case (d) without any alteration.

THE PROPOSED SCHEME

Robust Watermark Embedding

To embed robust watermark into an image, circle of centre, denoted by C_1, is divided into two subsets A_1 and B_1. Refer to Figure 2, A_1 consists pixels marked "+", B_1 otherwise.

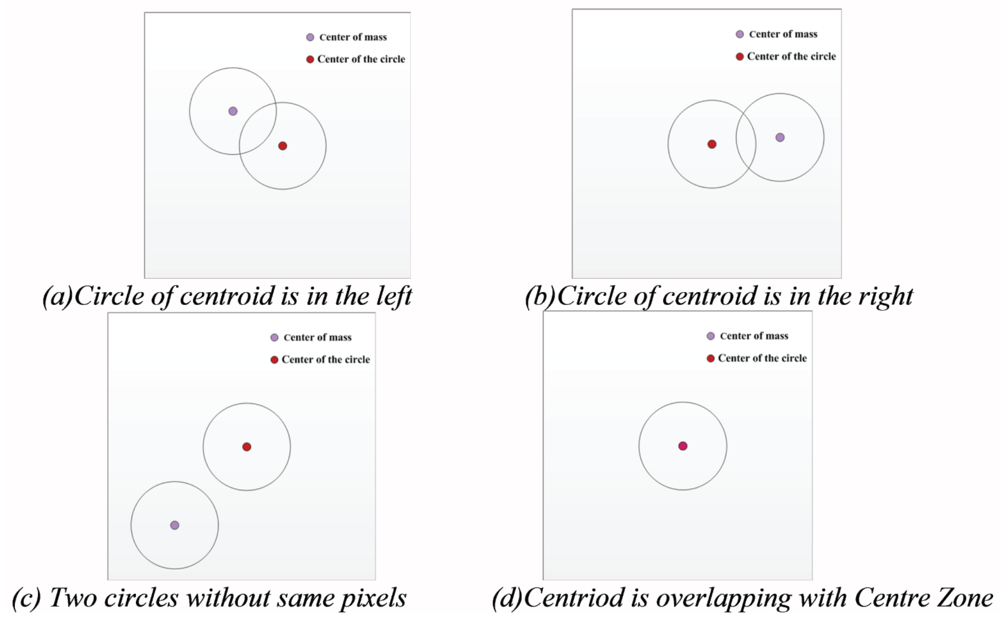
First, the alteration of pixels in the circle of image's centre is given by

$$c_i = \begin{cases} c_i + \alpha, & if \ c_i \in A_1 \\ c_i, & if \ c_i \in B_1 \end{cases} \tag{2}$$

where $c_i \in C_1$, $i \in [1,m]$, m is number elements of C_1.

For circle of centroid, denoted by C_2, the relationship of above two circles will be discussed by Figure 4. Case (c) and case (d) have given the scheme in Section 2.2, so only case (a) and case (b) will state below in detail.

Figure 3. The relative position of centre of mass and the centre of the circle. Circles centred at centroid and centre of host image are partially overlapping in case (a) and (b). The non-overlapping pixels will be altered according the first or last overlapping pixel. In case (c), two circles are non-overlapped absolutely. They will both be changed according to Section 2.2 at the same time. In case (d), two circles are overlapped completely and only need changing one (a) Circle of centroid is in the left (b) Circle of centroid is in the right (c) Two circles without same pixels (d) Centriod is overlapping with Centre Zone



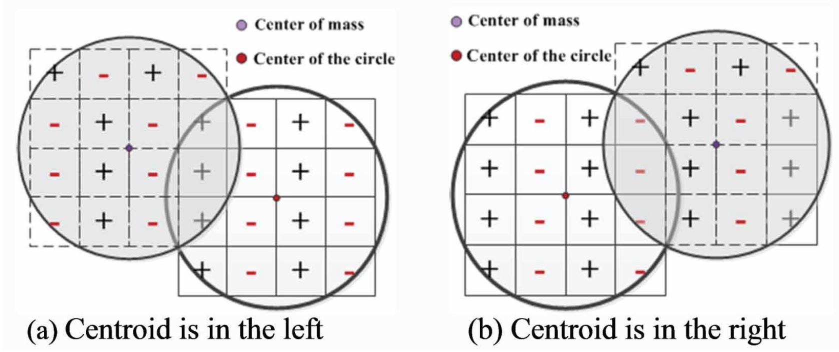
(a)Circle of centroid is in the left

(b)Circle of centroid is in the right

(c) Two circles without same pixels

(d)Centriod is overlapping with Centre Zone

Figure 4. Subsets marked by "+" and "-" with different position of centre and centroid (a) Centroid is in the left (b) Centroid is in the right



(a) Centroid is in the left

(b) Centroid is in the right

In case (a), we find the first overlapping pixel from each row and mark it by "+". Then, we mark the other pixels in the non-overlapping portion of centroid's circle on backward inference method as shown in Figure 4 (a). In case (b), the last overlapping pixel from each row is marked by "-", and other non-overlapping pixels are marked as shown in Figure 4 (b). Finally, the gray values of the marked "+" pixels in the non-overlapping portion of centroid's area are added with β as centre's area.

After changing all the pixels marked by "+", a robust data has been embedded into the host image. And the differences α_1, α_2 of circles of centre and centroid are both larger than a threshold.

Side Information Embedding

Along with embedding robust watermark, side information for recovering host image has been generated. In many existing schemes, there must be another channel to share the side information between sender and the receiver, which adds security risks.

In our proposed algorithm, the original coordinate of centroid, shifting quantity β and overflow/underflow information are side information.

Coltuc (2007) proposed embedding robust data and side information in two stages, this special framework is also suitable for our scheme. We will losslessly compress the side information and adopt histogram expanding and shifting technology to hide these data as fragile watermarks. In other words, these data can be extracted lossless without any attacks and used to recover host image.

The peak point of image histogram provides enough capacity for hiding side information. Refer to Figure 5, assuming the peak point is located at p. For example, p equals to 128. It means all the pixels equal to p could be employed to embed fragile data. Side information is losslessly compressed to be a binary bit sequence firstly. And this sequence will be embedded one by one. From the first pixel (top-left of the image), we check its value. If the pixel is smaller than p, we make no change on it. If it is equal to p, we change its value to p+b, where b is the current bit to be embedded. And if it is larger than p, we change its value to p+1 as shown in Figure 5. If one point p is not enough, the more such points should be employed. For a given image, denote by Ir, which has embedded robust watermark, the fragile watermarking embedding process is given by

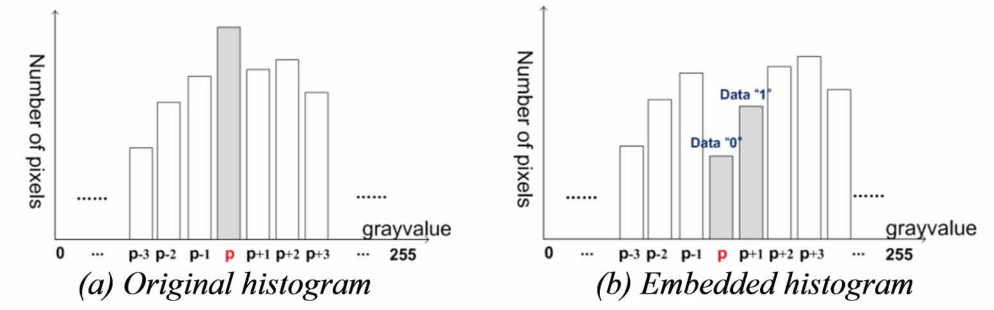
$$I_r^{'}(i,j) = \begin{cases} I_r(i,j)+1, & if\ \ I_r(i,j) = p\,\&\, hidden\ \ data\ \ b = 1 \\ I_r(i,j), & if\ \ I_r(i,j) = p\,\&\, hidden\ \ data\ \ b\ \ = 0 \\ I_r(i,j)+1, & if\ \ p < I_r(i,j) \le 254 \\ I_r(i,j), & if\ \ 0 \le I_r(i,j) < p \end{cases} \tag{3}$$

where i∈[1,m_1], i∈[1,n_1], $m_1 \times n_1$ is the size of matrix Ir.

Solving the Overflow/Underflow Problem

As we know, after series of action to the image in embedding, some pixels' gray value may be out of the gray range. Truncation is introduced after robust watermarking embedding in this paper by

Figure 5. Histogram of fragile watermarking embedding process (a) Original histogram (b) Embedded histogram



(a) Original histogram

(b) Embedded histogram

$$I_r(i,j) = \begin{cases} 0, & if\ I_r(i,j) < 0 \\ 255, & if\ I_r(i,j) > 255 \\ I_r(i,j), & otherwise \end{cases} \tag{4}$$

The difference between the original and truncated Ir and location of pixels that gray value equal to 255 will be added into side information. From equation (3), pixels in gray value 255 are not changed. It is highly confused with original ones in 254 in the recovery. By extracted side information of location in original 255, we keep these located pixels intact, and shift others' value from 255 to 254 during the recovery.

Watermark Extraction and Host Image Recovery

Extraction is the reverse process of embedding. If the host image has been experienced attacks, we cannot recover the original one. So we just extracted the robust watermark. Two circles centred at image centre and centroid are got by the way given in Section 2. Besides, two new difference statistics α3, α4 are calculated according formula (1). The α3 represents difference of centre's area, and the α4 represents difference of centroid's area. If the attack is compression, rotation or scale, we extracted data from α3 by judging if it is larger than a threshold T or not. If the attack is translation, robust watermark can be extracted from α4.

When the host is not under any attacks, we can recover the image to be its original condition. By the inverse of equation (3), the side information is attained. Side information consists of original coordinate of centroid, the shift quantity β, overflow/underflow information and so on. First, the image can be recovered to robust watermarked image according to overflow/underflow information. Then we calculated the difference α3, which represents difference of centre's area, to judge whether the robust watermark embedded or not. If not, the host image has been recovered and has no robust watermark. If robust watermark has been embedded, by the coordinate of centroid from the side information, the relationship between original centroid and centre will be established. There four relationships as shown in Figure 3. In either case, the gray values of pixels marked by "+" minus β and the values of pixels marked by "-" keep intact. Finally, the original host image has been recovered.

EXPERIMENTAL RESULTS

Experiment Setup and Evaluation Criteria

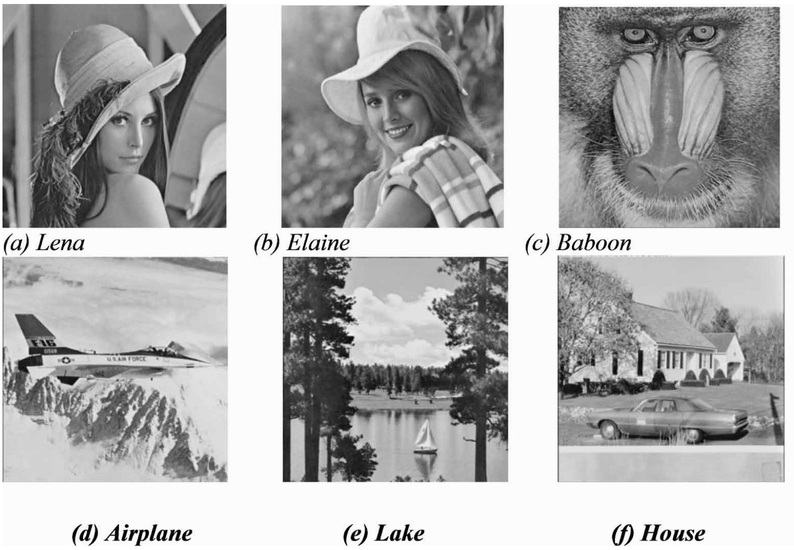
As shown in Figure 6, six grayscale images sized 512×512 are employed to test performance in our experiments. The visibility of host image will be affected by alteration of pixels' gray value. The greater the modification is, the more distortion leaving in the image. Peak Signal-Noise Ratio (PSNR) shows the objective distortion between marked image and original one. We will adopt this parameter to measure imperceptibility of image.

For robustness of this algorithm, we will compare the statistic α calculated by formula (1) of watermarked image with the initial one's. If the absolute values of α of watermarked image are generally larger than the initial one's, it shows that we have extracted the embedded robust watermark successfully.

Robustness and Imperceptibility Testing

Since we adopt Coltuc's framework in this paper, the side information will be embedded as fragile watermarks at the second stage after robust watermarking embedding. If the capacity of side information is very enormous, the information may not be embedded in the host image completely. In addition, the image visual quality and robustness will also sharply decrease.

Figure 6. Test images: six standard grayscale images sized 512×512 (a) Lena (b) Elaine (c) Baboon (d) Airplane (e) Lake (f) House



The second row in Table 1 gives the volume of side information in six images. The largest volume is 630 bits in image 'Baboon'. As each host image sized 512×512 has 262144 pixels, we just need change less than 0.3% pixels' gray value by one grey level according above side information embedding process. This slight alteration has limited influence on imperceptibility and robustness of the host image.

The third row in Table 1 reflects the imperceptibility of hosts by the parameter PSNR. PSNRs of six gray images as shown in Table 1 are greater than 50dB and the radius of circle is two centre-diagonal, which often suggest that image visual quality is quite good. And we choose three host images to make a comparison between initial image and marked image in Figure 7. Texture features of these three ones are representative. The distortion is much minor because the less number of altered pixels in the whole host image.

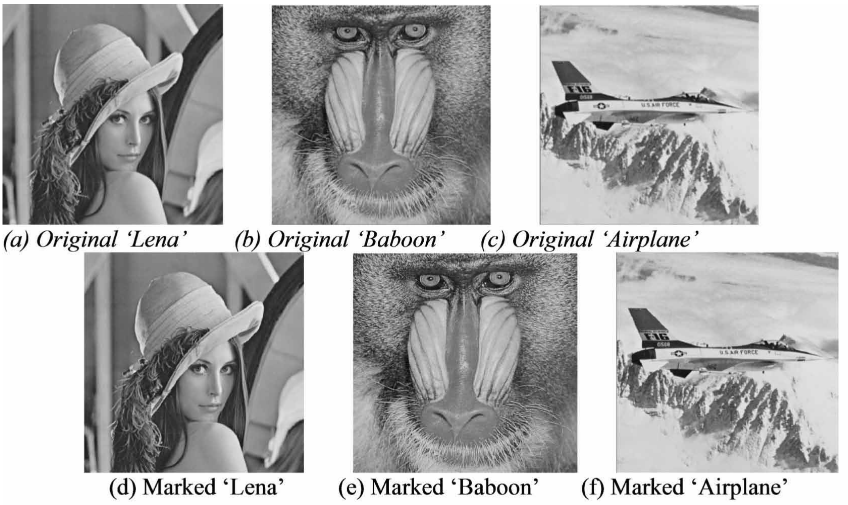
Since the host image can be recovered and watermarks can be extracted without any errors in lossless environment, we mostly focus on robustness test of watermark under different attacks. Under JPEG compression, rotation and scale attacks, the difference statics α_1 and α_3 of circles centred at the centre of image calculated by formula (1) are different, which original image's quantity α_1 is close to zero but marked image's α_3 is much greater than it.

Tables 2-5 show the robustness of this scheme under different attacks. In Table 2, the absolute value of difference can be kept greater than initial one even under compression quality factor 50. And this feature is also maintained under rotation with 30º and scale attack with factor from 1.1 to 1.2 as Table 3 and Table 4 shown. For example, in Table 2, the initial difference of image

Table 1. Volume of side information and PSNRs of six grayscale images with shifting quantity β=30, radius=2 centre-diagonal

Image	Lena	Elaine	Baboon	Airplane	Lake	House
Volume of side information (bits)	118	150	630	118	118	118
PSNR (dB)	50.78	51.27	50.89	54.32	50.66	53.95

Figure 7. Original (up) and robust-reversible (down) watermarked images (a) Original 'Lena' (b) Original 'Baboon' (c) Original 'Airplane' (d) Marked 'Lena' (e) Marked 'Baboon' (f) Marked 'Airplane'



(a) Original 'Lena' (b) Original 'Baboon' (c) Original 'Airplane'

(d) Marked 'Lena' (e) Marked 'Baboon' (f) Marked 'Airplane'

Table 2. The difference statics of circle centred at centre of host image under JPEG compression with different factors from 50 to 100, radius=2 centre-diagonal, the last column in the initial arithmetic difference before embedding

JPEG factor	100	90	80	70	60	50	Initial difference
Lena	29.50	27.88	18.25	16.88	11	2.75	**-1.125**
Elaine	30.50	31.13	26.13	23.63	27.13	11	**-0.875**
Baboon	31.38	29.13	25	27.38	26.13	15.13	**1.375**
Airplane	31.50	29.88	22.38	17	10.38	6.25	**0.5**
Lake	39	37	43.88	29.63	21.88	21.13	**8.875**
House	32.13	31.25	24.13	15.63	18.76	10.5	**2.125**

Table 3. The difference statics of circle centred at centre of host image under rotation with different degrees from 5^o to 30^o, radius=2 centre-diagonal

Rotation Angle	5^o	10^o	15^o	20^o	25^o	30^o	Initial difference
Lena	29.50	29.50	29.50	18.38	14	15.75	**-1.125**
Elaine	30	30	30	13.38	2.75	1.63	**-0.875**
Baboon	31.38	31.38	31.38	13.88	6.63	4.25	**1.375**
Airplane	31.38	31.38	31.38	19.50	12.38	13.38	**0.5**
Lake	38.88	38.88	38.88	23.75	17.88	18.75	**8.875**
House	32.13	32.13	32.13	16.63	8.63	10.50	**2.125**

Table 4. The difference statics of circle centred at centre of host image under scale attack with different scaling times, radius=2 centre-diagonal

Scale factor	0.8	0.9	1.1	1.2	1.3	Initial difference
Lena	-13.86	-5.82	14.35	10.63	0.126	**-1.125**
Elaine	-18.14	-5.57	13.55	9.76	0.14	**-0.875**
Baboon	-10.81	-4.79	14.94	10.68	1.02	**1.375**
Airplane	-12.77	-6.57	15.41	10.89	-0.04	**0.5**
Lake	5.73	4.48	23.61	18.61	7.99	**8.875**
House	-9.98	-3.90	19.12	16.65	2.52	**2.125**

Table 5. The difference statics of circle centred at centroid of host image under translation with different shifted coordinates, radius=2 centre-diagonal

Translated coordinate	(-1,0)	(0,1)	(1,2)	(2,0)	Initial centroid's difference
Lena	24.38	-34.63	16.75	13.63	**0.75**
Elaine	-7.3	24.63	-14.75	6.25	**6.25**
Baboon	13.50	23.25	26.50	16.75	**4**
Airplane	22	19.88	24.25	17.63	**-0.5**
Lake	31.38	14.75	28.75	14.25	**10.625**
House	13	-8.63	18.88	9.75	**-2.875**

'Lake' is 8.875, and the difference turns to be 21.13 to 39 under different JPEG compression with factors from 50 to 100. We find that 21.13 is larger than 8.875. It means that the robustness is still retained under JPEG compression with factor 50. In Table3, difference of image 'Lake' is 18.75 under rotation with 30º, which is still larger than 8.875. So we still can extract the embedded robust watermark.

However, we also find that, the higher attacking degree, the faster decline of the difference. In Table 4, the difference of image 'Lake' is 23.61 when the size of the image is added by 20 percent of original one. The value shows that, the robust watermark can be extracted. But when the scaling ratio expands to 1.3 times of the original image's size, the difference is 7.99, which is less than 8.875. At this time, the existence of robust watermark cannot be judged.

For translation attack, the coordinates of pixels in the host image has been changed. So the circle of centre in the attacked image is much different and pixels in these areas cannot be used to test robust watermark. Hence, the centroid of image is applied at this moment. And the static is α4 calculated by equation (1), which is the difference of centroid. Table 5 shows the robustness under translation. The less shifting of image is, the higher possibility to extract robust watermark.

From Table 2 to Table 5, it shows the high robustness especially under rotation attack. This is because the statistical pixels are surrounding the centre of image and much less likely changed with different rotation angle. And side information is much less and cannot influence robustness.

Comparative Experiment

We compare some state-of-the-art schemes (Ni, Shi, Ansari, Su, Sun & Lin, 2008; Li, 2012; Coltuc, 2007) with our proposed one in the accuracy of extracted robust watermark under rotation and using image 'Lena', and the payload of robust watermark is one bit, as shown in Table 6 and Table 7.

Table 6. Comparison between the proposed scheme with Ni's(2008), Li's(2012) and Coltuc's(2007) under attack of rotation with different degrees, radius=2 centre-diagonal, the symbol of tick shows that robust watermark can be extracted correctly

Rotation Angle	0.1°	0.5°	1°	5°	10°	20°	PSNR(dB)
Ni's (2008)	√	×	×	×	×	×	**45.12**
Li's (2012)	√	×	×	×	×	×	**42.11**
Coltuc's (2007)	√	√	×	×	×	×	**19.11**
Proposed	√	√	√	√	√	√	**50.78**

Table 7. Comparison between the proposed scheme with Ni's(2008), Li's(2012) and Coltuc's(2007) under attack of scale with different scaling times, radius=2 centre-diagonal, the symbol of tick shows that robust watermark can be extracted correctly

Scale factor	0.8	0.9	1.1	1.2	1.3	PSNR(dB)
Ni's (2008)	×	×	×	×	×	**45.12**
Li's (2012)	×	×	×	×	×	**42.11**
Coltuc's (2007)	√	√	√	√	×	**19.11**
Proposed	√	√	√	√	×	**50.78**

We compare Ni's (2008), Li's (2012) and Coltuc's (2007) with proposed scheme by embedding only one bit robust watermark in image 'Lena'. But these three schemes can embed multiple robust bits by divided image into many non-overlapping blocks. If the error rates of robust watermark are much low enough, error correction code such as BCH code can be used to ensure embedding several effective robust watermarks. Table 8 shows the error rates of Ni's (2008), Li's (2012) and Coltuc's(2007) under attack of rotation after embedding 4096 bits robust watermarks. When the degree of rotation is greater than 1°, the error rate is larger than 36.96% which is much higher than minimum bit error rate. For instance, BCH code can only correct error rate at most 24.71% by BCH(255,9,63). It means that these three schemes cannot embed one effective robust watermark under attack of rotation with degrees greater than 1°.

The results show that our proposed algorithm has better robustness under geometric attacks such as rotation and scale with higher PSNR. This is a easily neglected point but a ubiquitous phenomenon during the image transmission in reality. It affords a new way to deal with that problem in this paper.

CONCLUSION

In this article, we proposed a new robust reversible watermarking algorithm. Robust watermark and side information are embedded in two stages separately. Two circle areas with different centres are

Table 8. Error rates of Ni's(2008), Li's(2012) and Coltuc's(2007) under attack of rotation with different degrees after embedding 4096 bits robust watermarks

Scale factor	0.1°	0.5°	1°	5°	10°	20°
Ni's (2008)	6.88%	22.07%	36.96%	50.54%	49.46%	49.02%
Li's (2012)	0%	34.30%	43.60%	49.76%	49.93%	50.24%
Coltuc's (2007)	1.71%	50.51%	50.66%	49.41%	48.61%	48.24%

employed to ensure robustness under different attacks. Experimental results have shown good visual quality of image after embedding data. And robustness of the proposed scheme is better than others especially under rotation and scale attacks. Finally, the less capacity of side information can help the host image to be restored without any distortion in lossless environment.

In our future work, we will further enhance the robustness under scale and translation attacks with higher degree to ensure highly robust performance in an integrated RST attacking system.

REFERENCES

An, L., Gao, X., Li, X., Tao, D., Deng, C., & Li, J. (2012). Robust reversible watermarking via clustering and enhanced pixel-wise masking. *IEEE Transactions on Image Processing*, *21*(8), 3598–3611. doi:10.1109/TIP.2012.2191564 PMID:22453636

Chen, X., Sun, X., Sun, H., Zhou, Z., & Zhang, J. (2013). Reversible watermarking method based on asymmetric-histogram shifting of prediction errors. *Journal of Systems and Software*, *86*(10), 2620–2626. doi:10.1016/j.jss.2013.04.086

Coltuc, D. (2007). Towards distortion-free robust image authentication. *Journal of Physics: Conference Series*, *77*(1), 1–7.

De Vleeschouwer, C., Delaigle, J. F., & Macq, B. (2003). Circular interpretation of bijective transformations in lossless watermarking for media asset management. *IEEE Transactions on Multimedia*, *5*(1), 97–105. doi:10.1109/TMM.2003.809729

Fridrich, J., Goljan, M., & Du, R. (2001). Invertible authentication. *Security and Watermarking of Multimedia Content.*, *397*, 197–208. doi:10.1117/12.435400

Li, X. (2012). Robust lossless image data hiding with statistical quantity shifting. *Journal of Image & Graphics*, *17*(11), 1359–1366.

Li, X., Yang, B., & Zeng, T. (2011). Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection. *IEEE Transactions on Image Processing*, *20*(12), 3524–3533. doi:10.1109/TIP.2011.2150233 PMID:21550888

Li, X., Zhang, W., Gui, X., & Yang, B. (2013). A novel reversible data hiding scheme based on two-dimensional difference-histogram modification. *IEEE Transactions on Information Forensics and Security*, *8*(7), 1091–1100. doi:10.1109/TIFS.2013.2261062

Liu, Y., Ju, L., Hu, M., Ma, X., & Zhao, H. (2015). A robust reversible data hiding scheme for h.264 without distortion drift. *Neurocomputing*, *151*(1), 1053–1062. doi:10.1016/j.neucom.2014.03.088

Ni, Z., Shi, Y. Q., Ansari, N., Su, W., Sun, Q., & Lin, X. (2008). Robust lossless image data hiding designed for semi-fragile image authentication. *IEEE Transactions on Circuits and Systems for Video Technology*, *18*(4), 497–509. doi:10.1109/TCSVT.2008.918761

Ou, B., Li, X., Zhao, Y., Ni, R., & Shi, Y. Q. (2013). Pairwise prediction-error expansion for efficient reversible data hiding. *IEEE Transactions on Image Processing*, *22*(12), 5010–5021. doi:10.1109/TIP.2013.2281422 PMID:24043388

Thodi, D. M., & Rodriguez, J. J. (2004). Prediction-error based reversible watermarking. In *International Conference on Image Processing*, Singapore (Vol. 3, pp. 1549-1552).

Tian, J. (2003). Reversible data embedding using a difference expansion. *IEEE Transactions on Circuits and Systems for Video Technology*, *13*(8), 890–896. doi:10.1109/TCSVT.2003.815962

Wang, X., Li, X., Yang, B., & Guo, Z. (2010). Efficient generalized integer transform for reversible watermarking. *IEEE Signal Processing Letters*, *17*(6), 567–570. doi:10.1109/LSP.2010.2046930

Wang, Y., & Zhu, G. (2015). An improved AQIM watermarking method with minimum-distortion angle quantization and amplitude projection strategy. *Information Sciences*, *316*, 40–53. doi:10.1016/j.ins.2015.04.029

Wang, Y.-G., & Zhu, G. (2015). An improved AQIM watermarking method with minimum-distortion angle quantization and amplitude projection strategy. *Information Science*, *316*, 40–53. doi:10.1016/j.ins.2015.04.029

Jian Li is with Nanjing University of Information Science and Technology. His research interest includes data hiding and forensics.

Jinwei Wang is a professor and PhD supervisor at NUIST. His research interests include multimedia forensics, multimedia encryption, multimedia watermarking, and the application of AI for forensics.

Yu Shuang, is a master's degree candidate, research direction is in information hiding.

Xiangyang Luo received the M.S. degree and the Ph.D. degree from Zhengzhou Information Science and Technology Institute, Zhengzhou, China, in 2004 and 2010, respectively. From 2006 to 2007, he was a visiting scholar of the Department of Computer Science and Technology of Tsinghua University. He is the author or coauthor of more than 100 refereed international journal and conference papers. He is currently a professor Zhengzhou Science and Technology Institute. His research interest includes multimedia security, image steganography/steganalysis.