Cogn Comput (2016) 8:890–899
DOI 10.1007/s12559-016-9408-6

Improved Reversible Image Authentication Scheme

Zhaoxia Yin[1,2] · Xuejing Niu[2] · Zhili Zhou[1] · Jin Tang[2] · Bin Luo[2]

Received: 19 October 2015 / Accepted: 7 April 2016 / Published online: 22 April 2016

Abstract Image integrity authentication has aroused concerns because of the frequent modification on images. However, most of the image authentication schemes proposed so far employed the irreversible data hiding approach and the results of the published few reversible authentication methods are not satisfactory. To improve the detection accuracy as well as marked image quality, this paper proposes an improved reversible image authentication method based on Hilbert Curve mapping. In the proposed method, pixels are first mapped to a one-dimensional vector by using Hilbert Curve and divided into non-overlapping sets. Then, authentication codes can be embedded into each set by reversible data hiding approach. After comparing the extracted bits with the original authentication codes, the image set could be taken as modified one or unmodified one. Because image redundancy can be explored more fully and more flexibly by adopting Hilbert Curve mapping, more authentication codes can be embedded into the host image while leaving less distortion. Thus, both the detection accuracy and the marked image quality can be improved. The experimental results demonstrate the improvement compared with the latest development of reversible image authentication.

Keywords Image authentication · Random number generator · Digital signature · Fragile watermarking

✉ Bin Luo
luobin_ahu@163.com

[1] School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing, People's Republic of China

[2] School of Computer Science and Technology, Anhui University, Hefei 230601, People's Republic of China

Introduction

For one thing, the image processing software has been upgraded with time going by, and it is becoming more and more powerful, humanized and popular. For another image integrity authentication resulting from more frequent modifications on images has aroused concerns since 2000. Maliciously modified images would lead to serious consequences. For example, misdiagnose will happen if the medical images are modified. Many pioneers have explored the methods of dealing with the problem of image modification.

The existing authentication methods can be classified into two groups: digital signature-based methods [1–3] and fragile watermarking-based methods [4–7]. In the digital signature-based methods, signature is kept by third party. The signature extracted from image will be compared with the signature kept by third party to detect the integrity of image. The fragile watermarking can be divided into semi-fragile watermarking and complete fragile watermarking. The semi-fragile watermarking is robust to some processes and can distinguish usual signal processing and malicious tampering. Nevertheless, semi-fragile watermarking is insensitive to tampering. By contrast, complete fragile watermarking is sensitive to tampering. Any image modification can be detected by complete fragile watermarking. So complete fragile watermarking is suitable for precise authentication.

Information hiding methods in image spatial domain [8, 9] are different form robust watermarking methods. They are not able to resist any modification, thus belong to complete fragile watermarking. Correct data cannot be extracted from a marked image if pixels' value of the marked image has been changed. The data hiding methods could be used in image authentication can be divided into

irreversible methods, such as [10, 11], and reversible methods, such as [12–20]. Most of the current image integrity authentication methods adopt irreversible data hiding to embed authentication codes. Two evaluation criteria are applied to assess image integrity authentication methods: detection accuracy and image quality. Irreversible methods modify pixels' values of a host image to embed data, and the image quality and detection accuracy are high. However, irreversible methods bring damages to the host image in itself and the host image cannot be recovered after data embedding. On the contrary, reversible methods can reconstruct the host image error-free. The common techniques of reversible data hiding methods can be divided into two categories: histogram shifting [12–17] and difference expansion [18, 19]. The main idea of shifting-based reversible data hiding is modifying the pixels between peak point and zero point of histogram produced by image to embed data into peak point. The image quality and embedding capacity of shifting-based reversible method are acceptable. In 2013, pixel value ordering (PVO) [14] was proposed by Li et al. [14]. In PVO, host image is divided into non-overlapping blocks. Histograms are produced by the difference between the largest value and the second-largest value, and between the smallest value and the second-smallest value of each block. The largest value and the smallest value of each block are modified to embed data. PVO achieves high embedding capacity with high image quality, but it does not take advantage of image's redundancy space fully. In 2014, Peng et al. [15] improved PVO by utilizing more peak points. Higher embedding capacity and better image quality are achieved. In 2015, Wang et al. [16] made a further improvement with dynamic block partition.

Since it can detect whether image is modified, locate the tampered areas, and recover the host image accurately, reversible data hiding-based authentication methods are desired in our time. Unlike irreversible authentication methods, reversible authentication methods can recover the host image after extracting authentication codes, which is not only applicable to medical images and some other images requiring image integrity, but also suitable for any case where host images need to be recovered after integrity detecting.

However, most of the image authentication schemes proposed so far employed the irreversible data hiding approach and the detection accuracy and image quality of the published few reversible authentication methods are not satisfactory. Last year, Lo and Hu [7] proposed a histogram sifting-based reversible image authentication scheme for digital images, which makes full use of the poor robustness of spatial domain data hiding, and embeds authentication codes into host image to get a marked image. Then integrity of marked image can be detected according to the integrity of extracted data. To improve the detection accuracy as well as marked image quality based on [7], an improved reversible image authentication method based on Hilbert Curve mapping is proposed in this paper. In the first place, pixels are mapped to a one-dimensional vector by using Hilbert Curve, and divided into non-overlapping sets. Then, authentication codes can be embedded into each set by reversible data hiding approach. After comparing the extracted bits with the original authentication codes, the image set could be taken as modified one or unmodified one. Because image redundancy can be explored more fully and more flexibly by adopting Hilbert Curve mapping, more authentication codes can be embedded into the host image while leaving less distortion. Thus, both the detection accuracy and the marked image quality can be improved. Compared with the latest development of reversible image authentication [7], the experimental results demonstrate significant improvement in terms of detection accuracy and image quality. The following section is the details of the proposed method. The third section is experimental results and conclusion is made in the fourth section.

Proposed Method

In this part, the details of the proposed method are depicted. The proposed method includes three parts: authentication codes embedding, tamper detection and image recovery, and refinement process. Pre-arranged authentication codes are embedded into a host image to obtain the corresponding marked image. Receiver can detect integrity of the marked image by comparing extracted bits with predefined authentication codes. Actually, it is important that how to embed the location map for solving overflow and underflow problem. This is also a common issue for all of the reversible data hiding methods and has been addressed in the original reversible image authentication scheme proposed in Ref. [7]. Because it has nothing to do with the improvement of detection accuracy and image quality, no modification of this part is made in this paper.

Authentication Codes Embedding

In the proposed method, several bits authentication codes need to be embedded into each set. We make an improvement reversible data hiding method based on [16] and adopt it to embed authentication codes. In the first place, a host image is visited with Hilbert Curve (as shown in Fig. 1) and divided into non-overlapping sets. After that, each set are dynamically partitioned according to two predefined thresholds $T_1, T_2(-1 \leq T_1 \leq T_2 \leq 255)$. Then authentication codes will be embedded with two difference histograms. The detailed embedding procedure is presented step by step in the following.

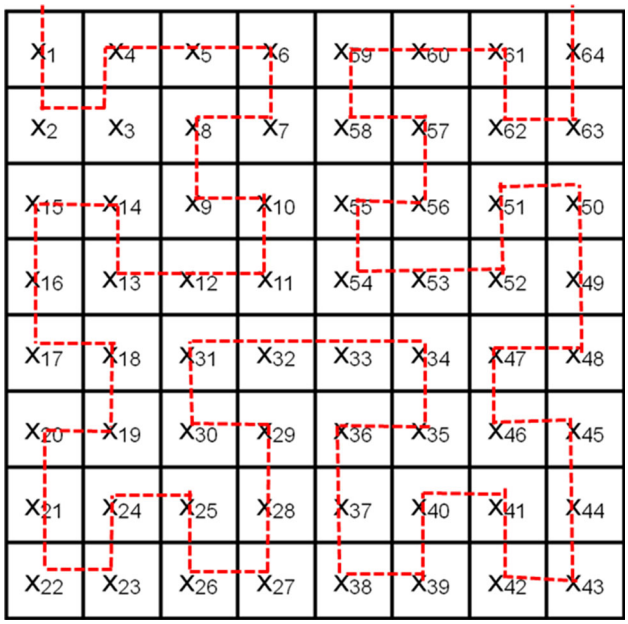


Fig. 1 Visit image with Hilbert Curve

Step 1: (Image partition)

Visit the host image sized $H \times W$ with Hilbert Curve and divide all the pixels into non-overlapping sets with L pixels.

Step 2: (Authentication codes generating)

Pseudorandom binary bits $B = \{b_i | b_i = 0 \text{ or } 1, \quad i = 1, 2, 3, \ldots\}$ produced by secret key are used for authentication codes. The length of B is $\lfloor H \times W / L \rfloor$ so that one bit authentication code corresponds to one set.

Step 3: (Authentication codes embedding)

According to pre-defined two thresholds T_1, T_2, embed the copies of i-th authentication code b_i into the i-th set as following. Please note that, the copies of b_i would be embedded in the i-th set. It must be admitted that the embedding capacity of reversible method is far lower than irreversible method. $\exists i$, the i-th set is not embeddable, then b_i will be skipped, and b_{i+1} will be embedded into the $(i+1)$-th set.

Given the i-th set $X_i = \{x_1, \ldots, x_L\}$ containing L pixels, in order to evaluate the complexity NL of it, X_i is divided into four subsets $X_i^n = \left\{x_1^n, \ldots, x_{L/4}^n\right\}, \quad n = 1, 2, 3, 4$. Sort these subsets in ascending order:

$$X_i^1 = \left\{x_{\sigma(1)}^1, \; x_{\sigma(2)}^1, \ldots, x_{\sigma(L/4)}^1\right\}$$

$$X_i^2 = \left\{x_{\sigma(1)}^2, \; x_{\sigma(2)}^2, \ldots, x_{\sigma(L/4)}^2\right\}$$

$$X_i^3 = \left\{x_{\sigma(1)}^3, \; x_{\sigma(2)}^3, \ldots, x_{\sigma(L/4)}^3\right\}$$

$$X_i^4 = \left\{x_{\sigma(1)}^4, \; x_{\sigma(2)}^4, \ldots, x_{\sigma(L/4)}^4\right\}$$

Here σ is a function mapping $\{1, \ldots, k\}$ to $\{1, \ldots, k\}$ and $x_{\sigma(i)} \leq x_{\sigma(j)}$ if $i < j$. NL is obtained according to the following equation:

$$\begin{aligned} \mathrm{NL} = & \max\left\{x_{\sigma(L/4-1)}^1, x_{\sigma(L/4-1)}^2, x_{\sigma(L/4-1)}^3, x_{\sigma(L/4-1)}^4\right\} \\ & - \min\left\{x_{\sigma(2)}^1, x_{\sigma(2)}^2, x_{\sigma(2)}^3, x_{\sigma(2)}^4\right\} \end{aligned} \tag{1}$$

Case 1 If $\mathrm{NL} \leq T_1$, X_i would be considered as a flat set and subdivided into four subsets with $L/4$ pixels to embed codes;
Case 2 If $T_1 < \mathrm{NL} \leq T_2$, X_i would be taken as normal block with no partition to embed code;
Case 3 If $T_2 < \mathrm{NL}$, X_i would be omitted in embedding procedure as a rough set

After dynamic partition, X_i will remain unchanged or be subdivided into 4 sets, namely the length of the set is L or $L/4$. The flat set and normal set are possible to embed data, we define those dynamically partitioned sets as X_i'. Then sort X_i' in ascending order and calculate $d_{\max}$, the difference between the largest value and the second-largest value of X_i', as Eq. (2).

$$d_{\max} = x_u - x_v \quad \text{where} \begin{cases} u = \min(\sigma(\xi), \sigma(\xi - 1)) \\ v = \max(\sigma(\xi), \sigma(\xi - 1)) \end{cases} \text{ and } \xi \text{ is the length of } X_i' \tag{2}$$

All $d_{\max}$ in the whole image constitute a difference histogram. On account of most $d_{\max}$ are 0 and 1 in images [16], take bin 1 and bin 0 acquiescently as the peak points of difference histogram to embed data. Histograms are shifted and the i-th authentication code b_i can be embedded in the set by the following equation:

$$\tilde{x}_{\sigma(\xi)} = \begin{cases} x_{\sigma(\xi)} + b_i, & \text{if } d_{\max} = 1 \text{ or } d_{\max} = 0 \\ x_{\sigma(\xi)} + 1, & \text{if } d_{\max} > 1 \text{ or } d_{\max} < 0 \end{cases} \tag{3}$$

where ξ is the length of X_i'

Similarly, $d_{\min}$, the difference between the smallest value and the second-smallest value of X_i', can constitute another histogram. And the i-th authentication code b_i can be embedded once more.

$$d_{\min} = x_s - x_t \quad \text{where} \begin{cases} s = \min(\sigma(1), \sigma(2) \\ t = \max(\sigma(1), \sigma(2)) \end{cases} \tag{4}$$

$$\tilde{x}_{\sigma(1)} = \begin{cases} x_{\sigma(1)} - b_i, & \text{if } d_{\min} = 1 \text{ or } d_{\min} = 0 \\ x_{\sigma(1)} - 1, & \text{if } d_{\min} > 1 \text{ or } d_{\min} < 0 \end{cases} \quad (5)$$

Until now, the authentication codes are embedded.

Step 4: (Marked image generating)

Hereto, the marked image $\tilde{I}$ with authentication codes can be obtained by utilizing an inverse process of Hilbert Curve visiting.

Tamper Detection and Image Recovery

In tamper detection procedure, authentication codes $B = \{b_i | b_i = 0 \text{ or } 1,\ i \in N\}$ are generated by the same secret key used in Sect. 2.1 and are consistent with the authentication codes embedded in the embedding procedure. If the bits extracted from the marked image are the same as B, this image is regarded as an integral one; otherwise, this image is regarded as a tampered one. The specific tamper detection and image recovery procedure is presented in the following.

Step 1 Evaluate the complexity NL of the i-th set $\tilde{X}_i = \{x_1, \ldots, x_L\}$ based on Eq. (1).

Step 2 Partition $\tilde{X}_i$ dynamically according to the thresholds T_1, T_2 used in the embedding procedure to obtain $\tilde{X}_i'$ and Sort $\tilde{X}_i'$ in ascending order.

Step 3 Generating difference histogram constituted by all $d_{\max}$ in $\tilde{I}$.

Step 4 The code $\tilde{b}_i$ is extracted from the set according to the following equation:

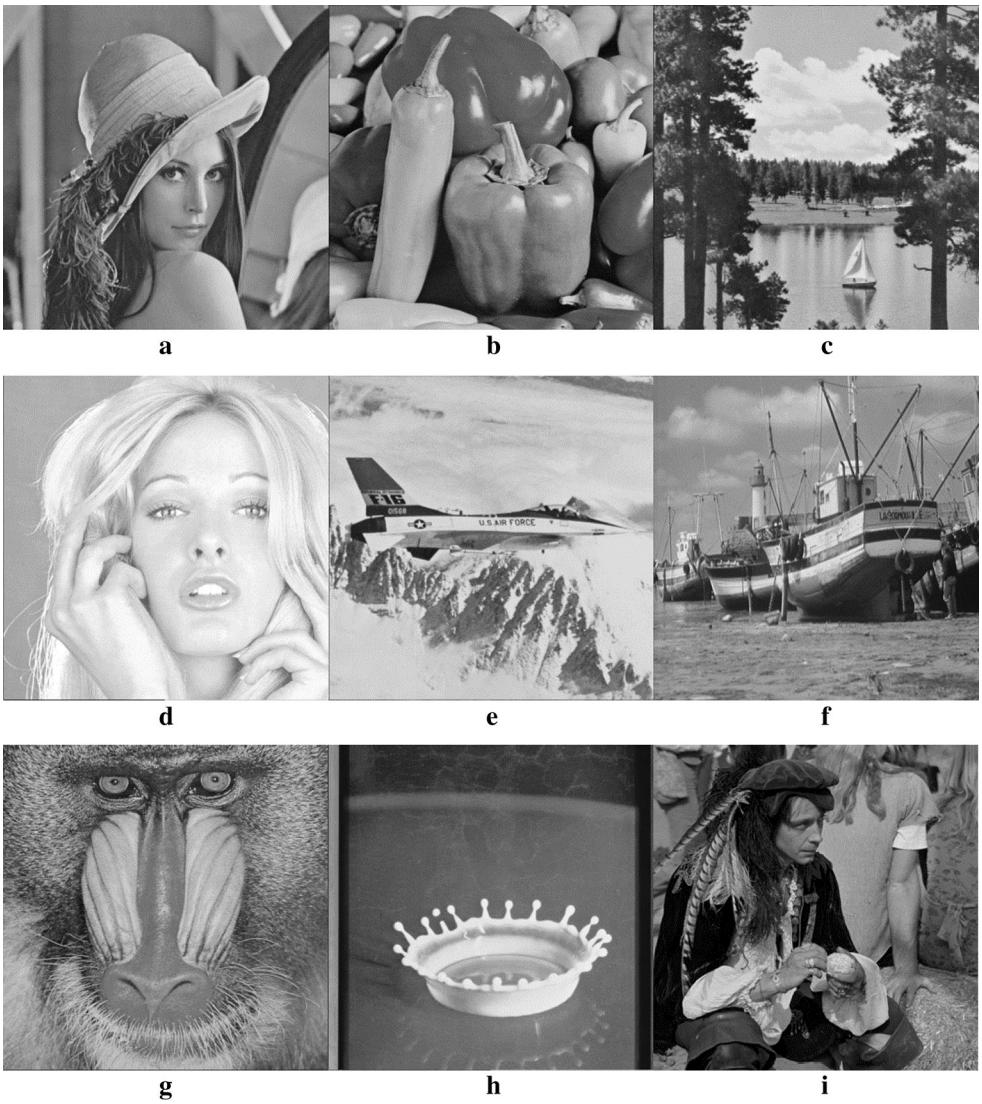


Fig. 2 Nine test grayscale images. **a** Lena, **b** Peppers, **c** Sailboat, **d** Tiffany, **e** Plane, **f** Boat, **g** Baboon, **h** Splash, **i** Man

Fig. 3 The embeddable areas of Lena in the proposed method. **a** $T_1 = 40$, $T_2 = 80$, PSNR = 52.36 dB, **b** $T_1 = 60$, $T_2 = 100$, PSNR = 52.09 dB, **c** $T_1 = 255$, $T_2 = 255$, PSNR = 51.84 dB

$$\tilde{b}_i = \begin{cases} 0, & \text{if } d_{\max} = 1 \text{ or } d_{\max} = 0 \\ 1, & \text{if } d_{\max} = 2 \text{ or } d_{\max} = -1 \end{cases} \tag{6}$$

Step 5 Image recovery according to the following equations:

$$x_{\sigma(\xi)} = \begin{cases} \tilde{x}_{\sigma(\xi)}, & \text{if } d_{\max} = 1 \text{ or } d_{\max} = 0 \\ \tilde{x}_{\sigma(\xi)} - 1, & \text{if } d_{\max} > 1 \text{ or } d_{\max} < 0 \end{cases}, \tag{7}$$

ξ is the length of $\tilde{X}_i'$

Step 6 Authentication codes extraction and image recovery from difference histogram constituted by all $d_{\min}$:

$$\tilde{b}_i = \begin{cases} 0, & \text{if } d_{\min} = 1 \text{ or } d_{\min} = 0 \\ 1, & \text{if } d_{\min} = 2 \text{ or } d_{\min} = -1 \end{cases} \tag{8}$$

$$x_{\sigma(1)} = \begin{cases} \tilde{x}_{\sigma(1)}, & \text{if } d_{\min} = 1 \text{ or } d_{\min} = 0 \\ \tilde{x}_{\sigma(1)} + 1, & \text{if } d_{\min} > 1 \text{ or } d_{\min} < 0 \end{cases} \tag{9}$$

Authentication codes $\tilde{B} = \{\tilde{b}_i, i = 1, \ldots, \lfloor H \times W/L \rfloor\}$ can be completely extracted with data extraction method mentioned above one by one. It is easy to make out that 8 bit codes $\tilde{B}_i = \{\tilde{b}_i^n, n \leq 8, n \in N_+\}$ at most can be extracted from $\tilde{X}_i$, and no data can be extracted at worst. *Step 7* Tamper detection. The i-th set will be regarded as an unmodified set if $\tilde{b}_i^1 = \cdots = \tilde{b}_i^n = b_i, \quad n \leq 8$; otherwise, it will be regarded as a tampered set if $\exists \tilde{b}_i^n \neq b_i, n \leq 8$. If $\tilde{B}_i = \emptyset$, which is possible to happen, the i-th set will be treated as an unmodified one for the time being and handled in the refinement process later. Host image can be recovered without any error with location map if the image is integral.

Refinement Process

L pixels in marked image are segmented into one set. Some sets cannot be detected because no code is embedded in them. In addition, it is true that the codes extracted from tampered areas are precisely the same as authentication codes in some cases. On account of two special cases above, refinement process is adopted to deal with the initial detection results in Sect. 2.2.

The shape of the set is likely to be irregular after dividing using Hilbert curve. We use square block to count the modified block or unmodified block. In one square block, if unmodified pixels are more than modified pixels, that block is taken as unmodified block, or else that block is taken as a modified block.

To refine preliminary detection in Sect. 2.2, an unmodified block is regarded as a modified one if above adjacent set and below adjacent set are tampered sets. In a similar way, an unmodified set will be treated as a modified one if the adjacent right and left sets, upper right and bottom left sets, or upper left and bottom right sets are tampered sets. Conduct repeatedly the above refinement processing until no unmodified set becomes modified set after a round, then tampered areas is located. Experimental results show that, with above procedure, tampered area can be located accurately.

Experimental Results

In this part, all experiments are performed with MATLAB. Nine commonly used grayscale images sized 512×512 are adopted here. They are: Lena, Peppers, Sailboat, Tiffany, Plane, Boat, Baboon, Splash and Man, as show in Fig. 2.

Two commonly used evaluation criteria for authentication methods are detection accuracy and marked image quality. In this paper, peak signal-to-noise ratio (PSNR) defined as Eqs. (10)–(11) is used to evaluate the marked image quality:

$$\text{MSE} = \frac{1}{H \times W} \sum_{i=1}^{H \times W} (I_i - \tilde{I}_i)^2 \tag{10}$$

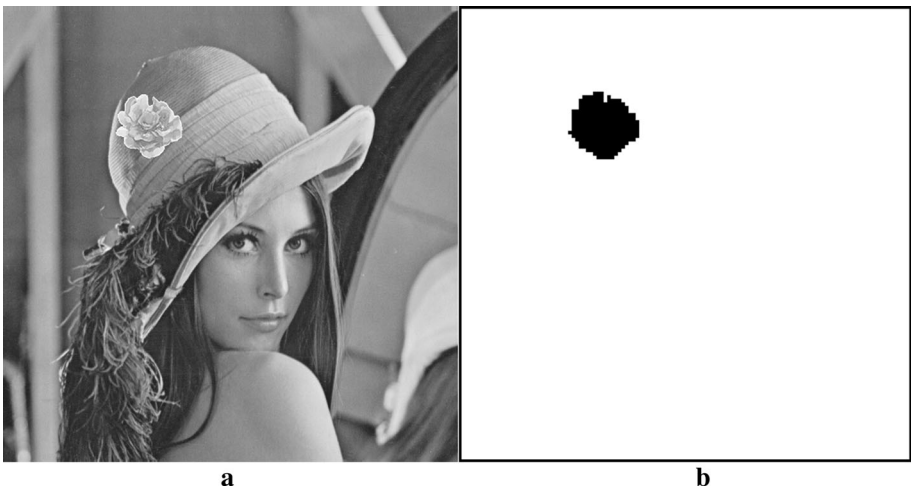


Fig. 4 Tampered Lena. **a** A flower added to Lena's hat, **b** Tampered area of (**a**)

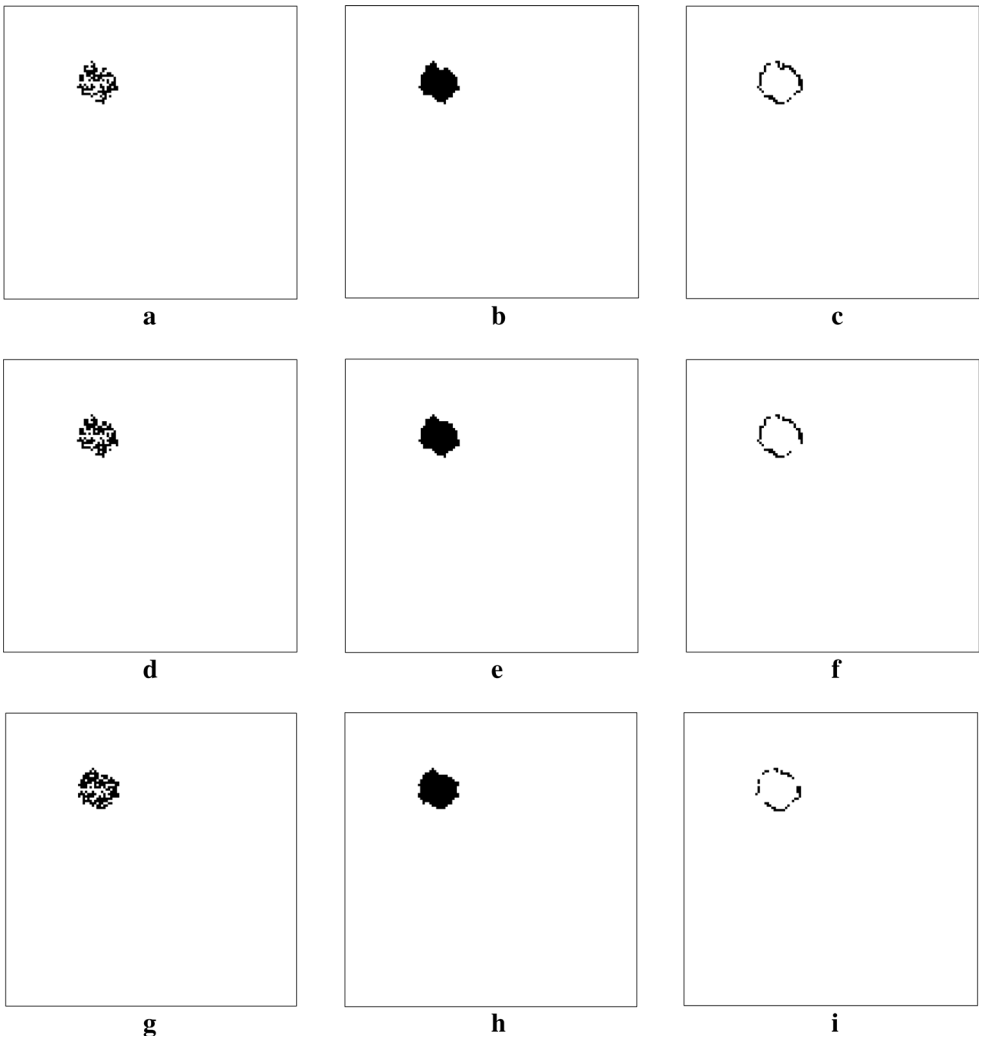


Fig. 5 Tamper detection results. **a**, **d**, **g** are the preliminary detection results, **b**, **e**, **h** are the final detection results of **a**, **d**, **g**, and **d**, **f**, i are the detection error of **b**, **e**, **h**

Table 1 Amount of non-embeddable block of the proposed method and Lo and Hu's method in nine test images

Images	Lena	Peppers	Sailboat	Tiffany	Plane	Boat	Baboon	Splash	Man
Proposed	2162	2548	4276	1600	1831	3539	7742	713	3185
[7]	3686	3776	5651	2954	3344	5331	8851	1938	5017
Gain	1524	1228	1375	1354	1513	1792	1109	1225	1832

Table 2 Total number of the image blocks with different embeddable bits t and the theoretical average error rate of the proposed method with $T_1 = T_2 = 256$, and average PSNR = 51.82 dB

Images	Lena	Peppers	Sailboat	Tiffany	Plane	Boat	Baboon	Splash	Man
$t = 0$	2162	2548	4276	1600	1831	3539	7742	713	3185
$t = 1$	3500	4548	4937	2996	2441	5083	5070	2108	3981
$t = 2$	3639	4381	3347	3520	2637	3997	2378	3265	3341
$t = 3$	3123	2850	1980	3255	2484	2256	870	3653	2349
$t = 4$	2077	1387	946	2491	2221	959	266	2840	1533
$t = 5$	1137	515	525	1400	1922	373	51	1656	917
$t = 6$	467	141	247	656	1406	131	7	999	530
$t = 7$	130	13	99	313	980	43	0	742	334
$t = 8$	149	1	27	153	462	3	0	408	214
Error rate	0.3288	0.3893	0.4827	0.2806	0.2595	0.4538	0.6713	0.2009	0.3931

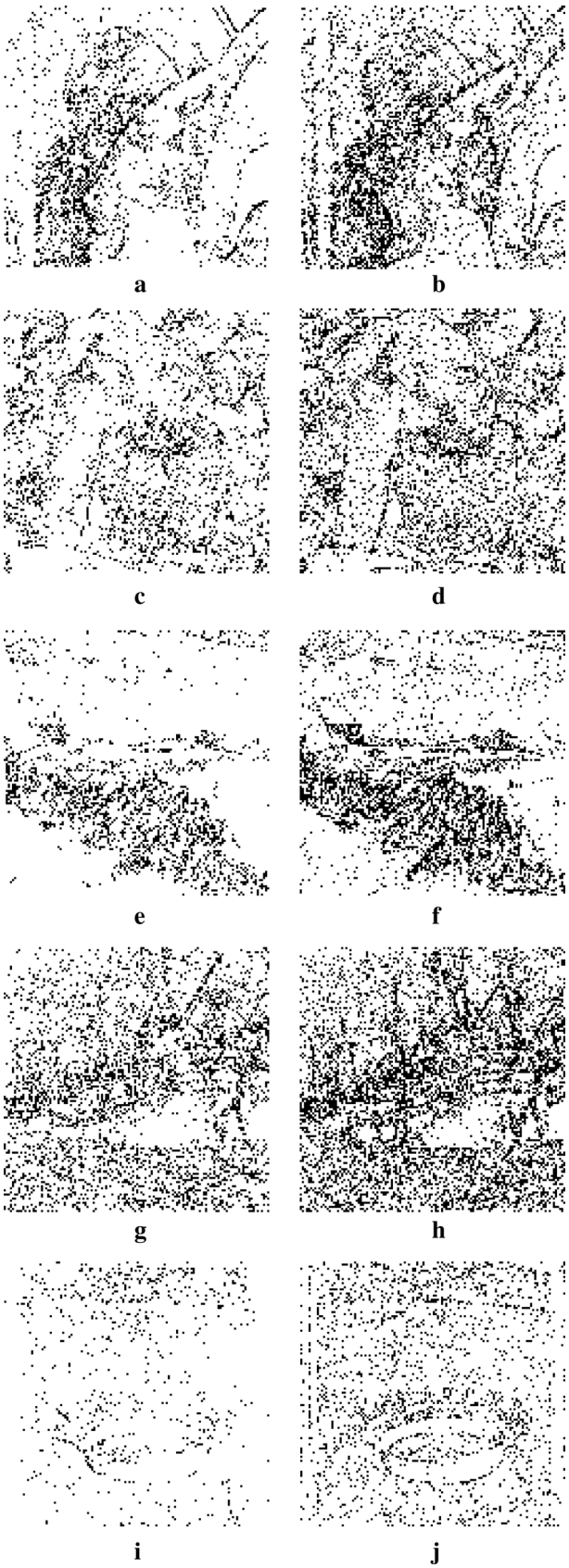
Table 3 Total number of the image blocks with different embeddable bits t and the theoretical average error rate of the [7], average PSNR = 48.75 dB

Images	Lena	Peppers	Sailboat	Tiffany	Plane	Boat	Baboon	Splash	Man
$t = 0$	3686	3776	5651	2954	3344	5331	8851	1938	5017
$t = 1$	3646	4083	4190	3146	2767	4493	4520	2794	4091
$t = 2$	2875	3333	2656	2881	2135	2948	1842	2846	2545
$t = 3$	2168	2304	1601	2237	1705	1682	753	2606	1559
$t = 4$	1573	1420	919	1772	1460	917	272	2039	1000
$t = 5$	975	807	550	1286	1195	481	102	1524	626
$t = 6$	651	392	329	818	962	292	35	940	427
$t = 7$	434	177	193	458	708	112	5	565	291
$t = 8$	188	63	109	300	600	71	2	288	209
$t = 9$	96	21	79	172	422	31	1	205	137
$t = 10$	54	3	56	81	344	12	1	125	113
$t = 11$	28	2	26	57	246	11	0	146	103
$t = 12$	4	2	19	40	166	3	0	105	73
$t = 13$	2	0	5	47	126	0	0	91	59
$t = 14$	2	1	1	53	105	0	0	103	66
$t = 15$	2	0	0	82	99	0	0	69	68
Error rate	0.4054	0.4309	0.5305	0.3476	0.3435	0.5251	0.7133	0.2788	0.4874

$$\mathrm{PSNR} = 10\log_{10}\frac{255^2}{\mathrm{MSE}}(\mathrm{dB}) \tag{11}$$

where $H \times W$ is the image size, I_i and $\tilde{I}_i$ is the i-th pixel of the host image and the marked image, respectively. The unit of PSNR is dB. The higher PSNR is, the better the marked image quality is. The average PSNR of the marked image generated by the proposed method is above 50 dB in general, which is higher than that of 48.75 dB in method [7].

Except for image quality, detection accuracy is another and more important evaluation criterion for authentication methods. The mechanism of the two image authentication methods proposed by [7] and this paper are the same: authentication codes are embedded into host images so that the codes can be extracted from the marked images and compared with the original bits to detect image integrity. So the detection accuracy depends much on authentication codes embedding. If we intend to detect the integrity of some areas, authentication codes must have been embedded into those areas. However, the capacity of reversible authentication methods is limited. Some areas of image are



◀**Fig. 6** Comparison of embeddable area between the proposed method and [7]. **a**, **b** Lena, **c**, **d** Peppers, **e**, **f** Plane, **g**, **h** Boat, **i**, **j** Splash. **a**, **c**, **e**, **g**, i are generated by the proposed method with average PSNR = 51.82 dB, **b**, **d**, **f**, **h**, **j** are generated by Lo and Hu's method with average PSNR = 48.75 dB

not embeddable, so the embedding blind area exists. It can confirm that detection accuracy of reversible authentication would enhance if the embedding blind areas decrease.

In Fig. 3, the embeddable areas of Lena in the proposed method are given with $L = 16$. Sixteen pixels in two-dimensional image are located in a 4×4 block, similarly hereinafter. If a block is embeddable, in other words, at least 1 bit data can be embedded in this block, it is colored with white, or else black. In Fig. 3 (a) is the embeddable areas when $T_1 = 40$, $T_2 = 48$, PSNR = 52.36 dB, (b) is the embeddable areas when $T_1 = 60$, $T_2 = 100$, PSNR = 52.09 dB, and (c) $T_1 = 255$, $T_2 = 255$, PSNR = 51.84 dB. It is obvious that as threshold T_1, T_2 increase, image quality decreases, but embeddable areas increase, and blind areas decrease.

To test the detection accuracy of the proposed method, a flower is added to Lena's hat, as show in Fig. 4a. The corresponding tampered area of Fig. 4a is shown in Fig. 4b, and the black area in Fig. 4b is the modified area. Figure 3a–c are modified as Fig. 4a, and corresponding preliminary detection results are shown in Fig. 5a, d, g. The black blocks in Fig. 5a, d, g are the tampered blocks whose extracted codes are distinct from authentication codes. The white blocks in Fig. 5a, d, g are not tampered blocks or blocks without data extraction.

According to Fig. 5a, d, g, it is not hard to know that, with the increasing of threshold, the embeddable areas increase and the blind areas decrease so that the accuracy of preliminary detection is enhanced. Preliminary detection is a rough reflection of tampered areas, but not accurate enough. Figure 5a, d, g is processed further with method in Sect. 2.3, and the corresponding results are shown in Fig. 5b, e, h. It is clear that the detection results of Fig. 5b, e, h are more accurate than Fig. 5a, d, g. As a result, Sect. 2.3 is estimation of tampered area on the basis of preliminary detection. The difference between estimated tampered areas and genuine tampered areas exists. In Fig. 5c, f, i, the difference between the final authentication results in Fig. 5b, e, h and genuine tampered areas is given. The black blocks in Fig. 5c, f, i are the authentication error of the proposed method. Likewise, it can be concluded that authentication accuracy increase with the augment of embeddable areas.

Furthermore, to make comparison of detection accuracy with Lo and Hu's method [7], the statistic of block that is not embeddable is shown as Table 1. In Table 1, the first

row is the amount of block that is not embeddable in the proposed method, and the second row is that of Lo and Hu's method [7]. The proposed method produces fewer blind areas than Lo and Hu's method in nine test images, as shown in the third row. Tables 2 and 3 are the number of image blocks with different embeddable bits and theoretical average error rate of proposed method and [7]. If one block is modified, the error rate of block without extracted codes is 1, the error rate of block with n authentication codes is $(1/2)^n$. It is obvious that the average error rate of proposed method is lower than [7].

The embeddable area of the proposed method and Lo and Hu's method in Lena, Peppers, Plane, Boat, and Splash are shown in Fig. 6. Respectively, the embeddable area of the proposed method are shown in Fig. 6a, c, e, g, i, and the embeddable area of Lo and Hu's method are shown in Fig. 6b, d, f, h, j. It can be observed with naked eye that the black blocks in Fig. 6a, c, e, g, i are fewer than b, d, f, h, j. The increase in embeddable areas and decrease in blind areas ensure the enhancement of detection accuracy.

Conclusion

In this paper, an improved reversible image authentication method is proposed. With the purpose of improving the detection accuracy as well as marked image quality, Hilbert Curve is adopted to visit the image and map all pixels to a one-dimensional vector. By embedding authentication codes into each non-overlapping set and comparing the extracted bits with the original authentication codes, the image set could be taken as modified one or unmodified one. Because image redundancy can be explored more fully and more flexibly by adopting Hilbert Curve mapping, more authentication codes can be embedded into the host image while leaving less distortion. As the experimental results suggest, compared with Lo and Hu's reversible authentication method, the proposed method achieves better image quality, fewer blind areas, and higher detection accuracy.

Funding This study was funded by National Natural Science Foundation of China (Grant Number 61502009 and 61472002), Anhui Provincial Natural Science Foundation (Grant Number 1508085SQF216), Key Program for Excellent Young Talents in Colleges and Universities of Anhui Province (Grant Number gxyqZD2016011), Large-scale Application Demonstration of the Education Cloud (Grant Number 2013BAH72B03) and funds of PADA & CICAEET.

Compliance with Ethical Standards

Conflict of interest Zhaoxia Yin, Xuejing Niu, Zhili Zhou, Jin Tang, and Bin Luo declare that they have no conflict of interest.

Informed Consent All procedures followed were in accordance with the ethical standards of the responsible committee on human experimentation (institutional and national) and with the Helsinki Declaration of 1975, as revised in 2008 (5). Additional informed consent was obtained from all patients for which identifying information is included in this article.

Human and Animal Rights This article does not contain any studies with human or animal subjects performed by the any of the authors.

References

1. Lou DC, Liu JL. Fault resilient and compression tolerant digital signature for image authentication. IEEE Trans Consum Electron. 2000;46(1):31–9.
2. Tsai PY, Hu YC, Chang CC. A novel image authentication scheme based on quadtree segmentation. Imaging Sci J. 2005;53(3):149–62.
3. Ababneh S, Ansari R, Khokhar A. Iterative compensation schemes for multimedia content authentication. J Vis Commun Image Represent. 2009;20(5):303–11.
4. Lin CY, Chang SF. A robust image authentication method distinguish JPEG compression from malicious manipulation. IEEE Trans Circuits Syst Video Technol. 2001;11(2):153–68.
5. Zhang XP, Qian ZX, Ren YL, Feng GR. Watermarking with flexible self-recovery quality based on compressive sensing and compositive reconstruction. IEEE Trans Inf Forens Secur. 2011;6(4):1223–32.
6. Qin C, Chang CC, Chen PY. Self-embedding fragile watermarking with restoration capability based on adaptive bit allocation mechanism. Signal Process. 2012;92(4):1137–50.
7. Lo CC, Hu YC. A novel reversible image authentication scheme for digital images. Signal Process. 2014;98:174–85.
8. Xia Z, Wang X, Sun X, Wang B. Steganalysis of least significant bit matching using multi-order differences. Secur Commun Netw. 2014;7(8):1283–91.
9. Xia Z, Wang X, Sun X, Liu Q, Xiong N. Steganalysis of LSB matching using differences between nonadjacent pixels. Multimed Tools Appl. 2016;75(4):1947–62.
10. Yin ZX, Tang J, Liu YJ, Luo B. Data hiding algorithm with high payload based on pixel pair matching. Syst Eng Theory Pract. 2013;33(11):2972–9.
11. Hong W, Chen TS. A novel data embedding method using adaptive pixel pair matching. IEEE Trans Image Process. 2012;7(1):176–84.
12. Ni Z, Shi YQ, Ansari N, Su W. Reversible data hiding. IEEE Trans Circuits Syst Video Technol. 2006;16(3):354–62.
13. Tsai PY, Hu YC, Yeh HL. Reversible image hiding scheme using predictive coding and histogram shifting. Signal Process. 2009;89(6):1129–43.
14. Li X, Li J, Li B, Yang B. High-fidelity reversible data hiding scheme based on pixel-value-ordering and prediction-error expansion. Signal Process. 2013;93:198–205.
15. Peng F, Li X, Yang B. Improved PVO-based reversible data hiding. Digit Signal Process. 2014;25:255–65.
16. Wang X, Ding J, Pei QQ. A novel reversible image data hiding scheme based on pixel value ordering and dynamic pixel block partition. Inf Sci. 2015;310:16–35.
17. Qu XC, Kim HJ. Pixel-based pixel value ordering predictor for high-fidelity reversible data hiding. Signal Process. 2015;111:249–60.
18. Tian J. Reversible data embedding using a difference expansion. IEEE Trans Circuits Syst Video Technol. 2003;13(8):890–6.

19. Li X, Zhang W, Gui X, Yang B. A novel reversible data hiding scheme based on two-dimensional difference-histogram modification. IEEE Trans Inf Forens Secur. 2013;8(7):1091–100.

20. Qian Z, Zhang X. Reversible data hiding in encrypted image with distributed source encoding. IEEE Trans Circuits Syst Video. 2015. doi:10.1109/TCSVT.2015.2418611.