Multimedia Tools and Applications
https://doi.org/10.1007/s11042-020-09985-1

Reversible image visual transformation for privacy and content protection

Hao-Tian Wu[1] · Ruoyan Jia[1] · Jean-Luc Dugelay[2] · Junhui He[1]

Received: 20 March 2020 / Revised: 27 July 2020 / Accepted: 24 September 2020 /
Published online: 14 October 2020

Abstract

In this paper, a novel image transformation scheme is proposed to protect the visual information. By mimicking an arbitrarily chosen reference image, a secret image is visually changed and can be exactly recovered from the transformed image when needed. Unlike the blockwise visual encryption methods, the proposed transformation scheme modifies the secret image by bit plane replacement and reordering so that no block effect is introduced. In particular, one or more bit planes are hidden into the other bit planes so that the most significant one(s) can be vacated. Besides replacing the vacated bit plane(s) and reordering the others according to the reference image, histogram modification may be performed to conceal the secret content if needed. To exactly recover the secret image, the required information is recorded and reversibly hidden into the transformed image by adopting a reversible data hiding algorithm. The experimental results on three image sets show that their content can be semantically changed to prevent leakage of visual information. Moreover, the applicability and efficiency of the proposed scheme have been validated by comparing the existing visual encryption schemes.

Keywords Visual encryption · Histogram · Bit plane · Privacy protection · Reversible data hiding

✉ Hao-Tian Wu
wuht@scut.edu.cn

Ruoyan Jia
201820133058@mail.scut.edu.cn

Jean-Luc Dugelay
jld@eurecom.fr

Junhui He
hejh@scut.edu.cn

[1] School of Computer Science and Engineering, South China University of Technology, Guangzhou, GD 510006, China

[2] Digital Security Department, EURECOM, Biot, F-06410, France

1 Introduction

Nowadays, the well-developed social network services are widely available. As it is convenient to share pictures, voices and videos with these services, it is more and more challenging to protect the user privacy and digital content. Sometimes people want to share pictures with their friends but do not want others to see them due to the concerns of privacy and sensitive content. To protect image content, there are two categories of encryption methods, i.e., traditional and visual encryptions. Although traditional encryption schemes can be used to protect image content from being leaked, the file format is changed so that the encrypted file cannot be directly used. Furthermore, the scrambled cipher-text may cause attentions of attackers. Compared with traditional encryption, visual encryption schemes make the sensitive content invisible without changing the image format. To recover the original secret image, additional information should be reversibly embedded into the visual encrypted image with reversible data hiding (RDH). As a branch of data hiding, RDH can be performed in a lossless way so that the original signal can be recovered after retrieving the embedded data (e.g., [3–5, 11, 13–16, 18–21, 25, 27–30, 32, 33, 35]).

Reversible image visual transformation (RIVT), which is proposed based on RDH, is a type of the visual encryption methods. With the RIVT methods (e.g., [6, 7, 9, 10, 31]), secret images can be encrypted into the transformed ones, from which the original image can be correctly restored without resorting to other information. Therefore, RIVT can be used for privacy preservation (e.g., [34]) to protect the privacy information and content protection (e.g., [24]) to conceal the confidential data. By referring to a reference image, the visual content of a secret image is modified to prevent the leakage of information to be protected. Although the original image is changed, the authorized party can obtain it by extracting the hidden data while those who are not authorized can only see the transformed image. So the image owner can decide who can recover the original secret image to achieve privacy and content protections.

To our best knowledge, the first RIVT method was proposed in [9], where the secret image is divided into fragments called tile images. The tile images are rearranged and modified to create a mosaic image, in which the necessary information for recovery of the secret image is hidden by adopting the RDH method in [4]. Consequently, the secret image can be recovered without any distortion by extracting the data hidden in the mosaic image. But one drawback of the method in [9] is that the reference image must be selected from a large database to create a sufficiently similar mosaic image.

By dividing the secret and reference image into non-overlapping blocks of the same size, an improved method was developed in [10] to address the issue. Firstly, the blocks are sorted according to the standard deviation of pixel values. Then the color transfer in [17] is adopted to make the mean and standard deviation of a secret block close to the corresponding reference block. Hence, the secret image can be visually transformed to a randomly selected reference image. Nevertheless, real numbers are involved in the transformation and the truncation errors occur in converting them into integers (e.g., [8]). So the secret image can only be nearly restored with the method in [10] rather than being completely recovered with the method in [9].

Based on the method developed in [10], an efficient RIVT method was proposed in [6], where the transformation is simplified by shifting all pixel values in a block with a predefined value. The amplitudes of pixel value shifted in every block, the overflow/underflow information, rotation information and block indices, are embedded into camouflaged image based on RDH (e.g., [18]). Thus the original image can recovered by extracting the hidden data and then reversing the transformation. Similar to the methods in [6, 9, 10], the original image is divided into blocks to be paired with those obtained from a reference image for RIVT in [7].

The methods proposed in [6, 7, 9, 10] can be applied to a variety of images to achieve reversibility of visual transformation. However, block effects are more or less caused because all of these methods divide secret image into blocks and process them individually. Not only may some visual distortions be introduced into the transformed images, but the block-based transformations are easily detected by using forgery detection and image forensic algorithms (e.g., [1, 12, 36, 37]). So it is worth to study the RIVT methods other than those in [6, 7, 9, 10].

To change the visual content of a secret image without introducing the block effects, a tentative way is to replace the most significant bit (MSB) plane with that of a reference image, such as in [31]. However, the method proposed in [31] does not work well on the secret images with high texture because their MSB planes cannot be efficiently compressed. To fully exploit the redundancy in a secret image, the least significant bit (LSB) plane may be hidden into the rest bit planes to accommodate the extra data, such as in [33].

In this paper, a new way of vacating the MSB plane(s) is proposed by adopting the idea in [33] to reversibly hide the LSB plane into the other bit planes. Besides replacing the vacated bit plane(s), the other bit planes are reordered according to a reference image. If needed, the visual content may be further blurred by histogram modification. Similar to the method in [31], the vacated MSB plane is replaced by that of the reference image to conceal the visual information and avoid block effects. By hiding the recorded data with the RDH method in [29], a new RIVT scheme is proposed to reversibly change secret images to prevent leakage of the visual information. The experimental results have validated the applicability and efficiency of the proposed scheme by comparing the existing visual encryption schemes in [6, 31].

The rest of this paper is organized as follows. Section 2 presents the RIVT scheme to be proposed in detail. The experimental results of the proposed scheme are given and compared with the method in [6] and [31] in Section 3. Finally, Section 4 concludes this paper.

2 Proposed scheme

In this section, a new RIVT scheme based on bit plane replacement and bit plane reordering is proposed for privacy and content protection. As illustrated in Fig. 1, there are four phases in the proposed procedure for reversible visual transformation. In the first phase, the MSB

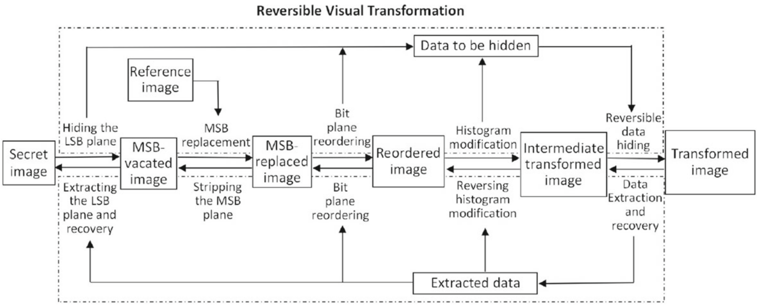


Fig. 1 Flowchart of the proposed image visual transformation scheme

plane of secret image is vacated and then replaced by that of the reference image. Then the other bit planes are reordered by referring to reference image to generate the reordered image. If needed, histogram modification is performed to generate the intermediate transformed image. Via RDH, the final phase is conducted to hide the information recorded in the first three phases to generate the transformed image. The details of four phases will be presented as follows.

2.1 Bit plane replacement

It is well known that the MSB plane can best affect the visual content of an image. For this reason, the MSB plane is chosen to be replaced by that of the reference image in [31]. In order to restore the original image, the MSB plane needs to be embedded into the other bit planes before it is replaced. However, it is hard to hide the whole MSB plane into the other bit planes for some high-textured images with the method in [31]. So in the proposed scheme, the MSB plane is not directly replaced but elaborately vacated. Thanks to the correlations between the neighboring pixels, the LSB plane can be hidden into the other bit planes by utilizing the prediction based RDH algorithms (e.g., [5, 11, 14, 15, 18, 25, 27]).

As shown in Fig. 2, RDH is utilized to hide the least significant bit (LSB) plane into the rest bit planes of secret image. Although the bitstream of the LSB plane is hard to be compressed, it can be totally hidden into the rest bit planes by exploiting the redundancy in them. For instance, the RDH algorithm proposed in [27] can be adopted to achieve high embedding capacity by using the interpolation technique for prediction. In the implementation, the bitstream of LSB plane is hidden into the 7-bit gray-level image consisting of the rest bit planes. Then the first seven bit planes are moved down as a whole. Consequently, the MSB plane can be vacated and thus can be replaced by the MSB plane of the reference image to generate the MSB-replaced image.

The experimental results show that the MSB plane can be vacated for all test images in three image sets including the high-textured ones. For some test images, the two LSB planes may be hidden into the rest planes so that two bit planes can be vacated. Even if the LSB plane cannot be completely hidden, the unused part can be recorded and hidden in the final phase of image transformation. Thus an MSB-replaced image can always be generated in the first phase.

2.2 Bit plane reordering

In this phase, the MSB-replaced image is further modified to change its visual content. Given that only the MSB plane is vacated and replaced in the first phase. Each bit plane except the MSB is compared with the second MSB plane of the reference image. After comparisons, the bit plane most similar to the second MSB plane of the reference image is found out and then moved to the second MSB plane. For the rest six bit planes, every one is

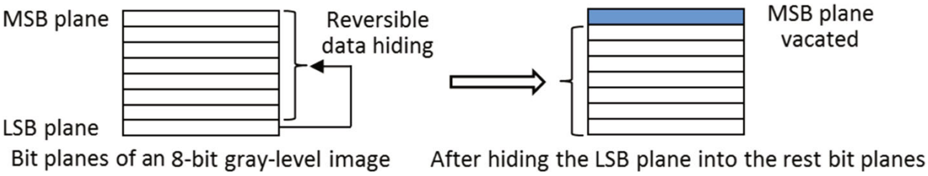

MSB plane
LSB plane
Reversible data hiding
MSB plane vacated
Bit planes of an 8-bit gray-level image
After hiding the LSB plane into the rest bit planes

Fig. 2 Vacating the MSB plane for bit plane replacement

compared with the next bit plane of the reference image to find out the most similar one. The process goes on until all bit planes are ordered, therefore the reordered image is generated. To memorize the original position in the MSB-replaced image, 3 bits are needed for each bit plane and totally 3 bytes of position information are recorded for an 8-bit image in total.

2.3 Histogram modification

Besides bit plane replacement and reordering, an operation called histogram modification may be performed to blur the visual content. To maintain the MSB plane, only the remaining seven bit plane are modified. Due to the pixel values for the seven bit plane range from 0 to 127, image histogram is divided into two intervals with the same length (i.e., [0, 127] and [128, 255]) and a histogram bin is mapped within the interval that it belongs to. In particular, the histogram bins in each interval are sorted according to their heights. For an 8-bit pixel value p, which bin ranks the i-th in its interval, the following operation is conducted:

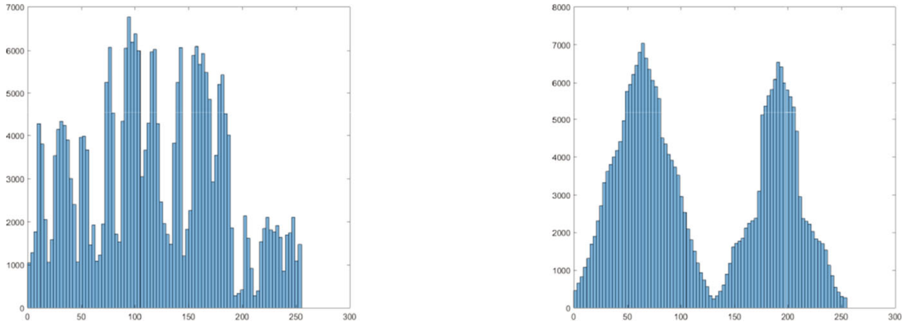
$$p' = \lfloor \frac{p}{128} \rfloor \times 128 + 63 + sign(i\%2 - 1) \times \lfloor \frac{i}{2} \rfloor, \qquad (1)$$

where p' is the modified pixel value, $\lfloor \cdot \rfloor$ represents the floor function. The sign function $sign(i\%2 - 1)$ equals to 1 if $i\%2 = 1$, and equals to -1 if $i\%2 = 0$. After applying (1) to every pixel in the image, the intermediate transformed image is generated while the highest bins are mapped around the center of each interval, as shown in Fig. 3.

Since the difference between p and p' is within the range of $[-127, 127]$, it can be exactly represented with 8 bits (i.e., 1 byte). In total, at most 256 bytes are required to record the histogram bin mapping information for there is no need to record the value of i. The recorded bit mapping information is put together with bit plane reordering information and the unused part of the LSB plane (if any). The concatenated information is to be hidden into the intermediate transformed image in the final phase. Since the image histogram has been centralized by conducting the bin mapping specified in (1), the embedding capacity in the next phase can be increased to accommodate more data for image recovery.

2.4 Reversible data hiding for exact recovery

In the final phase, the recorded data need to be reversibly hidden into the intermediate transformed image. After the first three phases, the correlations between the neighboring pixels are largely destroyed. So the prediction-based RDH methods (e.g., [4, 5, 11, 14, 15, 18, 25,



(a) Histogram before bin mapping

(b) Histogram after bin mapping

Fig. 3 An image histogram before and after bin mapping

27]) are no more suitable to hide the recorded data. To cope with this issue, a histogram-based RDH method proposed in [29] is adopted, in which the correlations between the neighboring pixels are not required. Interested readers may refer to [29] for the detailed implementation of the RDH algorithm. To further improve security, the recorded information can be encrypted and the corresponding key is generated before applying the RDH algorithm.

The data to be hidden consist of two parts. One is the information recorded in the second and three phases, and the other is the LSB bits which are not embedded in the first phase. Since the data recorded in the second and three phase are no more than 3+256=259 bytes, the RDH method in [29] is directly applied on the intermediate transformed image in the **first round of data hiding**. If the LSB plane(s) has not been completely embedded in the first phase, then the **second round of data hiding** needs to be conducted. In that case, the amount of information embedded in the second round varies with image size and may be much more than the first round. To keep the MSB plane unchanged, image histogram is calculated excluding the MSB of each pixel value to apply the RDH algorithm in [29]. Consequently, the value of a histogram bin varies from 0 to 127. That means that a pixel value $i \in [0, 127]$ and another pixel value $i + 128$ are counted in the same histogram bin. It should be noted that at most 32 pairs of histogram bins can be used for data hiding instead of 64 pairs in [29]. The transformed image is generated after all of the recorded data have been hidden in it. Finally, the receiver can directly recover the original image without needing additional information.

2.5 Recovery of Original Secret Image

According to the flowchart as show in Fig. 1, there are four phases to recover original secret image from the transformed image. In the first phase, one or two rounds of data extraction need to be conducted. At first, the transformed image histogram is calculated excluding the MSB plane to extract the hidden data. Meanwhile, the image before the second round of data embedding can be recovered. Then the image histogram is calculated from all bit planes so that the recorded information of bit plane reordering and histogram modification can be extracted. After that, the intermediate transformed image is obtained. With the extracted information, the original value of every histogram bin is known so that every bin can be mapped back. The MSB-replaced image is obtained by putting every bit plane to the original position.

To recover the original secret image, the LSB plane needs to be extracted from the MSB-replaced image. Firstly, the replaced MSB plane(s) is stripped before performing data extraction from the rest bit planes. Then the extracted bitstream and data extracted in the first phase of recovery (if any) make up the LSB plane(s). Since the rest bit planes can be restored after data extraction, the original secret image can be recovered by combining the extracted LSB plane(s) with them.

3 Experimental results

In the experiments, 8 test images denoted by the USC image set [22] and 50 test images downloaded from the BOWS2 web site [2] were used, which are all with the size of 512 × 512. In addition, 8 test images used in [10] and [6] were employed, which are with the size of 1024 × 768 and denoted by Large image set. Note that all test images were obtained by converting the color images to the gray-level ones. The programmes of image transformation, data embedding and extraction, and image recovery were implemented with the Microsoft Visual C++ and executed on a 64-bit PC with Intel Core CPU @4.2 GHz and 16G RAM.

3.1 Reversibility of visual transformation

To verify the reversibility of the proposed transformation scheme, the amount of data recorded and the embedding capacity obtained with the proposed scheme on the Larger and USC image sets were listed in Tables 1 and 2, respectively. The numerical results in Tables 1 and 2 represent the amount of data recorded in bit plane replacement, bit plane reordering and histogram modification, which need to be hidden into the transformed image during the last phase of visual transformation. The information recorded in the first phase represents the bit values in the LSB plane(s) that cannot be hidden into the other bit planes. The information recorded in the second and third phases represents the data used to record the bit plane reordering and histogram modification. The embedding capacity in the first round and the second round (which is optional) represents the amount of data reversibly embedded by the two rounds of RDH in the last phase of visual transformation, respectively. Furthermore, the pure capacity is calculated by subtracting the amount of data recorded in the first three phases from the sum of embedding capacity.

The pure capacity of every test image was high than 0, indicating that all of the recorded information was hidden into the transformed image. That means the reversibility was achieved for all test images with the proposed scheme by arbitrarily choosing a reference image. In contrast, the scheme in [31] was not successfully applied on the high-textured image “Baboon” in the USC set and 2 out of the 50 test images in the BOWS2 set. As shown in Table 2, the amount of side information recorded in the second and third phase was less than 259 bytes for the test image “Baboon” because some gray levels were absent in the MSB-replaced image. For some images, no side information was recorded in the first phase of visual transformation so that the second round of data hiding in the final phase was not performed. As shown in Tables 1 and 2, additional data were hidden into the transformed images because the embedding capacity was more than the information required to recover

Table 1 Visual transformation of 8 images in Large image set (size: 1024×768)

Test	Hiding the LSB plane(s) with [27]			Information recorded		Embedding capacity		Pure
image	Bit plane replaced	Hiding rate	Surplus (bytes)	First phase (bytes)	Second and third phases (bytes)	First round (bytes)	Second round (bytes)	capacity (bytes)
Bus	2	1.772	-22395	22395	259	1225	28249	6820
Bridge	2	2.213	20966	0	259	2683	0	23390
Flowers	1	1.036	3543	0	243	55276	0	58576
Girls	2	1.838	-15962	15962	259	2582	19551	5912
Man	2	2.194	19054	0	259	2606	0	21401
Sunflower	2	2.106	10385	0	259	1371	0	11497
Twoman	2	1.787	-20962	20962	259	1425	28373	8577
Woman	2	1.532	-45965	45965	259	3143	47487	4406

Table 2 Visual transformationof 8 images in USC image set (size: 512×512)

Test	Hiding the LSB plane(s) with [27]			Information recorded		Embedding capacity		Pure capacity
image	Bit plane replaced	Hiding rate	Surplus (bytes)	First phase (bytes)	Second and third phases (bytes)	First round (bytes)	Second round (bytes)	(bytes)
Baboon	1	1.098	3211	0	255	455	0	3411
Boat	2	1.986	-459	459	259	509	605	396
Barbara	1	1.464	15204	0	259	328	0	15273
Goldhill	2	1.895	-3441	3441	259	477	3926	783
F-16	2	1.966	-1115	1115	259	769	1510	905
Lena	2	2.159	5210	0	259	616	0	5567
Peppers	2	2.120	3932	0	259	470	0	4143
Sailboat	1	1.352	11534	0	259	517	0	11792

the original secret image. To preserve image visual quality, data hiding in the second round of RDH was stopped when all of the recorded information had been hidden.

3.2 Visual effect

Among the USC images, “Barbara” was chosen as the reference image of the others, as shown in Fig. 4, where the seven transformed images are labelled with their original names,

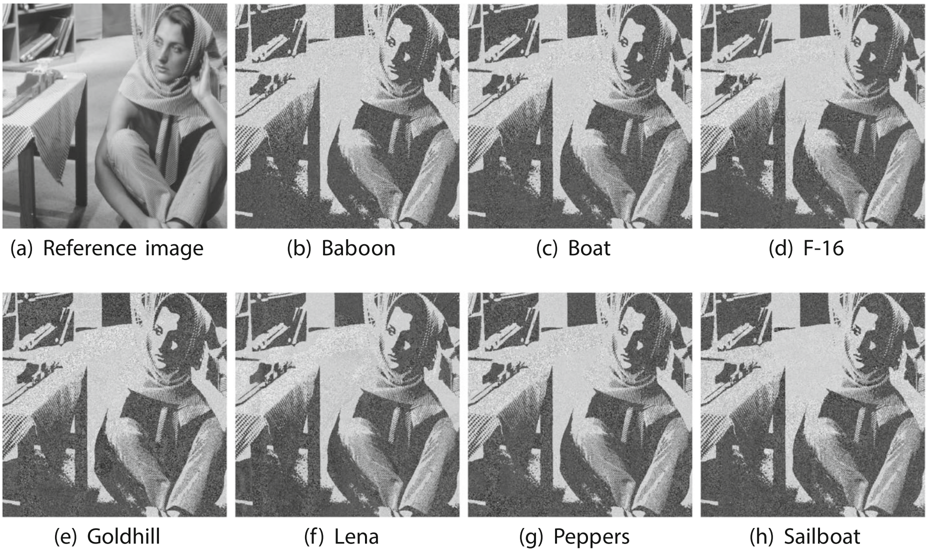
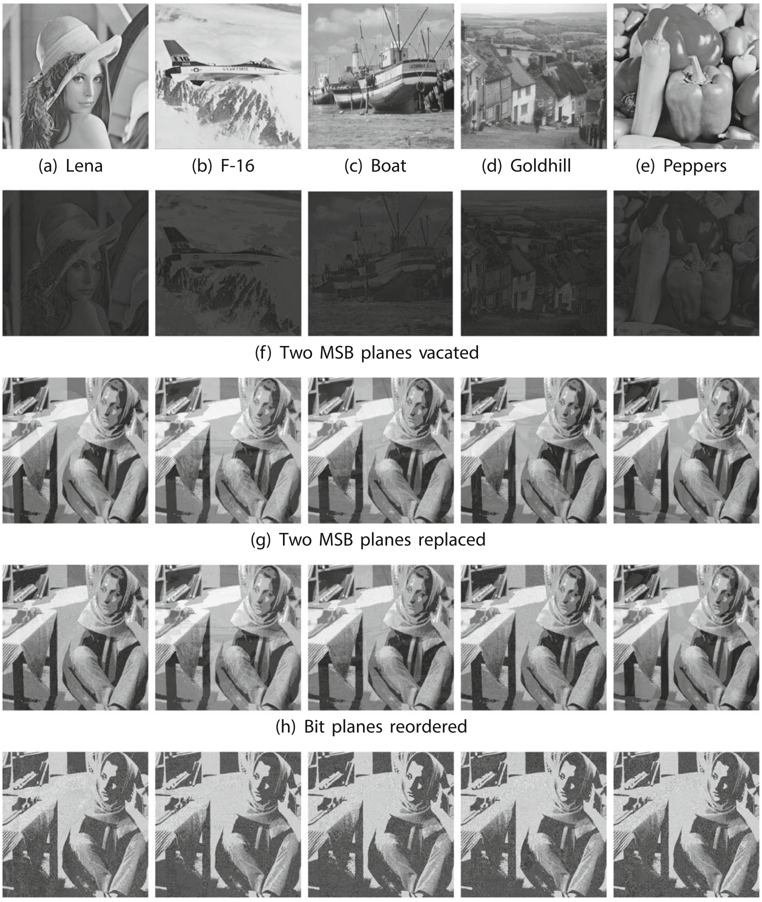

(a) Reference image
(b) Baboon
(c) Boat
(d) F-16
(e) Goldhill
(f) Lena
(g) Peppers
(h) Sailboat

Fig. 4 The reference image “Barbara”, and seven images transformed from the other test images with the proposed scheme

respectively. Despite that the secret images have different content, the transformed images look similar to each other by using the same reference image, indicating that the visual information of secret images was concealed by applying the proposed RIVT scheme.

To further illustrate the visual transformation process, five test images to be protected, the images after vacating the most significant two bit planes, bit plane replacement, bit plane reordering and histogram modification are shown in Fig. 5, respectively. It can be seen in the third row of Fig. 5 that the contour of secret images can still be noticed though the most significant two bit planes were replaced by those of the reference image, respectively. After the bit plane reordering and histogram modification, the intermediate transformed images were generated while the visual content was largely blurred, as shown in the fifth row of Fig. 5. From the transformed images are shown in Fig. 4 by choosing "Barbara" as the reference image, it can be seen that the visual content of every secret image was semantically changed.


(a) Lena (b) F-16 (c) Boat (d) Goldhill (e) Peppers

(f) Two MSB planes vacated

(g) Two MSB planes replaced

(h) Bit planes reordered

(i) After Histogram Modification

Fig. 5 Five secret images and their transformed images by vacating two bit planes, bit plane replacement, bit plane reordering and histogram modification

3.3 Avoiding block effects

To examine the block effects, the resultant images obtained with the proposed scheme were compared with those obtained with the scheme in [6]. As shown in Fig. 6, two block sizes were set to generate the transformed images by choosing "Barbara" as the target in applying [6], respectively. It can be seen that block effects were caused with the block size of 8×8 for all test images. When the block size was reduced to 4×4, the block effects were also noticeable, especially in the high-textured regions. As shown in Fig. 4, there was no such block effect after applying the proposed scheme to the test images.

3.4 Similarity evaluation of the transformed images

To measure the similarity between the transformed and reference images, the root mean square error (RMSE) and Structural SIMilarity (SSIM) index [23] between them were calculated, respectively. Meanwhile, the RMSE and SSIM index between the transformed and original secret images were also calculated to measure the information that may be leaked. The range of a SSIM index is from 0 to 1. And it equals to 1 when the two images are identical to each other. For the transformed images as shown in Fig. 4, the RMSE and SSIM index values calculated with their original secret images are listed in Table 3, while the RMSE and SSIM index values calculated between the transformed and reference images are shown in Table 4. For comparison, the RMSE and SSIM values obtained by applying the scheme in [31] are also listed in Tables 3 and 4. Most of test images can be reversibly transformed with the scheme in [31] except "Baboon" so that the corresponding results are absent. In Tables 3 and 4, the numerical results obtained by applying the scheme in [6] with two block sizes (i.e., 4×4 and 8×8) are also included. Since the scheme in [6] processes a color image, the luminance component was set to each of the RGB channel to obtain the gray-level transformed image.

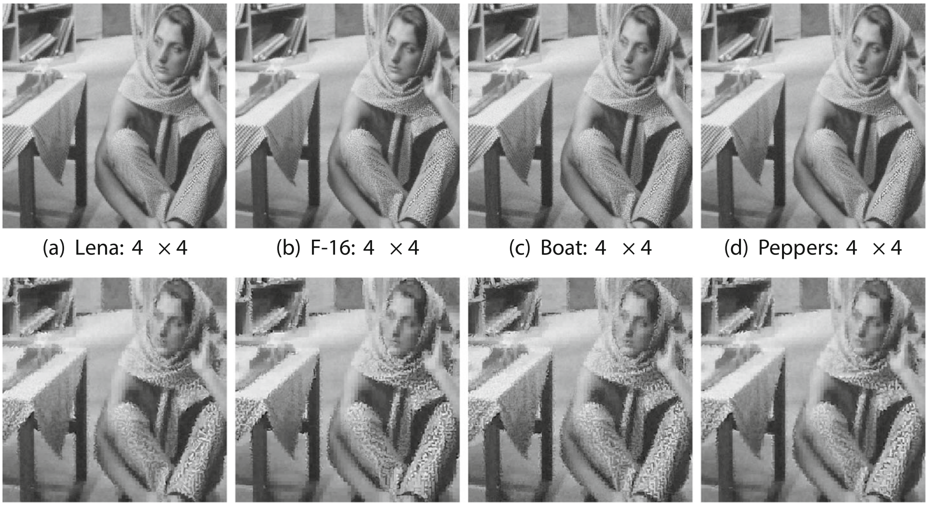

(a) Lena: 4 ×4
(b) F-16: 4 ×4
(c) Boat: 4 ×4
(d) Peppers: 4 ×4
(e) Lena: 8 ×8
(f) F-16: 8 ×8
(g) Boat: 8 ×8
(h) Peppers: 8 ×8

Fig. 6 Four test images transformed by applying the scheme in [6] with two different block sizes

Table 3 Similarity Evaluation of the Transformed Images (with Secret Images)

Secret	Proposed		Scheme [31]		Scheme[6]:4×4		Scheme[6]:8×8	
image	RMSE	SSIM	RMSE	SSIM	RMSE	SSIM	RMSE	SSIM
Baboon	82.99	0.020	–	–	74.33	0.050	71.88	0.066
Boat	69.51	0.243	81.06	0.068	67.63	0.137	66.97	0.168
F-16	95.99	0.143	102.30	0.131	94.20	0.231	94.15	0.252
Goldhill	79.52	0.064	85.59	0.042	73.14	0.151	72.35	0.179
Lena	70.84	0.072	80.14	0.057	63.47	0.216	63.06	0.248
Peppers	77.71	0.215	93.46	0.044	77.68	0.180	77.42	0.228
Sailboat	85.20	0.072	86.85	0.047	75.78	0.135	75.78	0.170

From the evaluation results listed in Table 3, it can be seen that the transformed images obtained with the proposed scheme were less like the secret images because the RMSE values were higher than those obtained scheme [6]. Meanwhile, the SSIM values obtained with the proposed scheme were lower than those obtained with scheme [6]. The larger RMSE values and lower SSIM values indicate that less visual information of a secret image is leaked from the transformed image. As for the difference between the transformed and reference images as shown in Table 4, the RMSE values obtained with the proposed scheme were lower than those obtained with scheme [31] for most test images, but higher than those obtained with scheme [6]. Meanwhile, the SSIM values obtained with the proposed scheme were close to those obtained with scheme [31], but lower than those obtained with scheme [6]. Compared with the scheme in [6], the images transformed by the proposed scheme are less like both of the arbitrarily chosen reference images and the original secret images, respectively.

To demonstrate the efficacy of the first three phases in the proposed RIVT scheme, the ablation study was conducted by removing each of the three phases (i.e., bit plane replacement, bit plane reordering, and histogram modification) at one time. Then the RMSE and SSIM index between the reference and transformed images, were calculated and compared with those obtained with the complete scheme, as shown in Table 5. From the numerical results, it can be seen that the average similarity between the reference and transformed images was increased by replacing the MSB plane(s). The second phase (i.e., bit

Table 4 Similarity Evaluation of the Transformed Images (with Reference Images)

Secret	Proposed		Scheme [31]		Scheme[6]:4×4		Scheme[6]:8×8	
image	RMSE	SSIM	RMSE	SSIM	RMSE	SSIM	RMSE	SSIM
Baboon	44.06	0.238	–	–	29.62	0.326	31.11	0.283
Boat	25.17	0.424	42.90	0.277	20.26	0.526	25.18	0.432
F-16	23.11	0.467	42.69	0.322	19.02	0.641	25.14	0.497
Goldhill	26.01	0.396	47.36	0.256	18.96	0.547	22.89	0.448
Lena	25.06	0.412	49.31	0.214	19.28	0.549	23.67	0.471
Peppers	23.12	0.485	49.64	0.222	21.13	0.514	26.76	0.428
Sailboat	44.12	0.254	45.70	0.257	22.41	0.464	26.79	0.421

Table 5 Ablation Study of the Proposed Scheme (similarity with reference image)

Trans-	Without conducting the						Applying the	
formed	first phase		second phase		third phase		whole scheme	
image	RMSE	SSIM	RMSE	SSIM	RMSE	SSIM	RMSE	SSIM
Baboon	91.46	0.016	44.05	0.238	48.71	0.198	44.06	0.238
Barbara	87.24	0.254	39.12	0.222	38.34	0.269	39.13	0.222
Boat	84.68	0.022	43.54	0.245	25.17	0.424	43.55	0.245
F-16	90.94	0.129	41.28	0.283	23.11	0.467	41.91	0.270
Goldhill	87.57	0.071	44.99	0.230	26.01	0.396	46.62	0.224
Lena	82.88	0.060	42.81	0.260	25.06	0.412	42.82	0.261
Peppers	89.83	0.049	44.50	0.247	23.12	0.485	44.51	0.247
Sailboat	82.16	0.163	46.15	0.223	50.54	0.184	44.12	0.254
Average	87.10	0.072	43.31	0.244	**32.51**	**0.354**	43.34	0.245

The lowest RMSE and the highest SSIM both indicate the highest similarity with reference image

plane reordering) has much less effects than the other two phases because the replaced planes are more significant. The similarity between the reference and transformed images was increased by not performing the third phase (i.e., histogram modification), while the reversibility of visual transformation was maintained for all test images. So the transformed images were more similar to the reference ones without performing the third phase in applying the proposed scheme.

Besides the USC image set, the similarity evaluations were also conducted on the BOWS2 and the Larger image sets, respectively. The mean of the RMSE and SSIM values obtained by applying the proposed RIVT scheme, the proposed scheme without histogram modification (HM), the schemes in [6, 31] were listed in Table 6, respectively. Note that the scheme in [31] could not be applied on several test images (e.g., “Baboon” in USC image set and 2 out of 50 test images in the BOWS2 set), which were excluded in calculating the mean of the RMSE and SSIM values. From the statistical results, it can be seen that the transformed images obtained with the proposed scheme were less like the secret images and more like the reference images than those obtained with the scheme in [31]. Besides, the similarity between the reference and transformed images can be increased by not performing histogram modification in applying the proposed scheme. Compared with the scheme in

Table 6 Statistical (Mean) Evaluation of the Transformed Images

Compared	Image	Proposed		Without HM		Scheme[6]:4×4		Scheme[6]:8×8		Scheme [31]	
with	set	RMSE	SSIM	RMSE	SSIM	RMSE	SSIM	RMSE	SSIM	RMSE	SSIM
the secret image	USC	85.64	0.067	77.95	0.171	75.49	0.170	74.99	0.201	78.22	0.166
	Larger	86.94	0.068	74.49	0.163	74.94	0.201	74.32	0.216	90.85	0.077
	BOWS2	88.24	0.090	81.81	0.147	81.03	0.253	78.84	0.279	90.41	0.130
the reference image	USC	43.24	0.246	30.19	0.377	19.67	0.561	24.76	0.459	45.90	0.247
	Larger	43.31	0.227	27.67	0.316	20.06	0.544	25.38	0.473	50.42	0.196
	BOWS2	38.28	0.335	25.83	0.480	19.56	0.687	28.93	0.515	42.34	0.357

[6], our scheme is more applicable because the reversibility was achieved on all test images.

3.5 Security discussion

Security is an important aspect of data embedding with keys (e.g., [26]). The security of the proposed RIVT scheme relies on the order of traversing the pixels. In the final phase of visual transformation, the RDH algorithm in [29] is adopted to embed the data recorded in the previous phases. According to the bit values to be hidden, the pixels with the same value may be modified to different values, respectively. Since the order of traversing the pixels can be controlled with a secret key, extracting the hidden data and recovering the intermediate transformed image also rely on the secret key. Without knowing it, the computations for correctly recovering the secret image will exponentially increase with the pixel number.

Since the reference image is arbitrarily chosen with the proposed scheme, the collusion attack can be avoided by using a different reference image for each secret image. As the main usage of the proposed scheme is to conceal the visual information, how to resist the detection of the forgery detection and image forensic algorithms (e.g., [1, 12, 36, 37]) needs further investigation.

4 Concluding remarks

In this paper, we have proposed a new reversible image visual transformation scheme to protect the visual information. The proposed scheme consists of hiding one or two bit planes of secret image to the other planes, replacing the most significant bit plane(s), reordering the rest bit planes and modifying the histogram before data embedding. Furthermore, the data recorded to recover the original secret image can be kept in the transformed image in a lossless manner. Consequently, the original secret image can be recovered when needed and the proposed scheme is useful in protecting the sensitive information.

Different from the methods that divide both of the secret and reference images into blocks with the same size, there is no block artifact introduced by applying the proposed scheme. The experimental results have shown that the visual information can be well concealed after changing the visual content while the similarity between the reference and transformed images can be increased by not performing the histogram modification. Meanwhile, the reversibility of the proposed scheme has been validated on three sets of test images. Besides the security issues, how to improve the visual quality of the transformed images will be further studied in our future work.

Acknowledgements This work was supported by the National Natural Science Foundation of China (No. 61772208), the Key-Area Research and Development Program of Guangdong Province (No. 2019B010137004) of China and Fundamental Research Funds for the Central Universities of China (x2js-D2190700).

Compliance with Ethical Standards

Conflict of interests The authors declare that they have no conflict of interest.

References

1. Bianchi T, Piva A (2012) Image forgery localization via block-grained analysis of JPEG artifacts. IEEE

Trans. Inf. Foren. Sec 7(3):1003–1017

2. Break Our Watermarking System, 2nd Edition. http://http://bows2.ec-lille.fr/
3. Cheung YM, Wu HT (2007) A sequential quantization strategy for data embedding and integrity verification. IEEE Trans. Circuits Syst. Video Technol 17(8):1007–1016
4. Coltuc D, Chassery J-M (2007) Very fast watermarking by reversible contrast mapping. IEEE Signal Processing Letters 14(4):255–258
5. Dragoi I-C, Coltuc D (2015) On local prediction based reversible watermarking. IEEE Trans. Image Process 24(4):1244–1246
6. Hou D, Zhang W, Yu N (2016) Image camouflage by reversible image transformation. J. Vis. Commun. Image R 40(A):225–236
7. Hou D, Zhang W, Zhan Z, Jiang R, Yang Y, Yu N (2016) Reversible image processing via reversible data hiding. Proc. IEEE International Workshop on Digital Signal Processing, pp 427–431
8. Kang Y, Liu F, Yang C, Luo X, Zhang T (2019) Color image steganalysis based on residuals of channel differences. Computers, Materials & Continua 59(1):315–329
9. Lai IJ, Tsai WH (2011) Secret-fragment-visible mosaic image - a new computer art and its application to information hiding. IEEE Trans. Inf. Forens. Secur 6(3):936–945
10. Lee YL, Tsai WH (2014) A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible color transformations. IEEE Trans. Circuits Syst. Video Technol 24(4):695–703
11. Li X et al (2015) Efficient reversible data hiding based on multiple histograms modification. IEEE Trans. Inf. Foren. Sec 10(9):2016–2027
12. Liao X et al (2020) Robust detection of image operator chain with two-stream convolutional neural network. IEEE J Selected Topics Signal Process 14(5):955–968
13. Ma B, Shi YQ (2016) A reversible data hiding scheme based on code division multiplexing. IEEE Trans. Inf. Foren. Sec 11(9):1914–1927
14. Ou B, Li X, Zhao Y, Ni R, Shi YQ (2013) Pairwise prediction-error expansion for efficient reversible data hiding. IEEE Trans. Image Process 22(12):5010–5021
15. Peng F, Lin Z, Zhang X, Long M (2019) Reversible data hiding in encrypted 2D vector graphics based on reversible mapping model for real numbers. IEEE Trans. Inf. Foren. Sec 14(9):2400–2411
16. Qin C, Chang C-C, Hsu T-J (2015) Reversible data hiding scheme based on exploiting modification direction with two steganographic images. Multimedia Tools and Applications 74:5861–5872
17. Reinhard E, Ashikhmin M, Gooch B, Shirley P (2001) Color transfer between images. IEEE Comput. Graph. Appl 21(5):34–41
18. Sachnev V, Kim HJ, Nam J, Suresh S, Shi YQ (2009) Reversible watermarking algorithm using sorting and prediction. IEEE Trans. Circuits Syst. Video Technol 19(7):989–999
19. Shi YQ, Li X, Zhang X, Wu HT, Ma B (2016) Reversible data hiding: Advances in the past two decades. IEEE Access 4:3210–3237
20. Su W, Wang X, Li F, Shen Y, Pei Q (2019) Reversible data hiding using the dynamic block-partition strategy and pixel-value-ordering. Multimedia Tools and Applications 78:7927–7945
21. Subburam S, Selvakumar S, Geetha S (2018) High performance reversible data hiding scheme through multilevel histogram modification in lifting integer wavelet transform. Multimedia Tools and Applications 77:7071–7095
22. The USC Image Database. http://sipi.usc.edu/database/
23. Wang Z, Bovik AC, Sheikh HR, Simoncelli EP (2004) Image quality assessment: from error visibility to structural similarity. IEEE Trans. Image Process 13(4):600–612
24. Wang B, Kong W, Li W, Xiong NN (2019) A dual-chaining watermark scheme for data integrity protection in internet of things, computers. Materials & Continua 58(3):679–695
25. Wang J, Ni J, Zhang X, Shi YQ (2017) Rate and distortion optimization for reversible data hiding using multiple histogram shifting. IEEE Trans. Cybernetics 47(2):315–326
26. Wang Y, Zhu G, Kwong S, Shi YQ (2018) A study on the security levels of spread-spectrum embedding schemes in the WOA framework. IEEE Trans. Cybernetics 48(8):2307–2320
27. Wu HT, Huang J (2012) Reversible image watermarking on prediction error by efficient histogram modification. Signal Process 92(12):3000–3009
28. Wu HT, Dugelay JL, Cheung YM (2008) A data mapping method for steganography and its application to images. In: Proc. Information Hiding. IH 2008. Lecture Notes in Computer Science, vol 5284. Springer, Berlin, Heidelberg, pp 236–250
29. Wu HT, Dugelay JL, Shi YQ (2015) Reversible image data hiding with contrast enhancement. IEEE Signal Process. Lett 22(1):81–85
30. Wu HT, Cheung YM, Huang J (2016) Reversible data hiding in Paillier cryptosystem. J Vis Commun Image R 40:765–771

31. Wu HT, Tang S, Dugelay JL (2018) Image reversible visual transformation based on MSB replacement and histogram bin mapping. Proc. the 10th International Conference on Advanced Computational Intelligence, pp 813–818
32. Wu H-T, Tang S, Huang J, Shi Y-Q (2018) A novel reversible data hiding method with image contrast enhancement. Signal Process: Image Communication 62:64–73
33. Wu HT, Yang Z, Cheung YM, Xu L, Yang S (2019) High-capacity reversible data hiding in encrypted images by bit plane partiton and MSB prediction. IEEE Access 7:62361–62371
34. Xia Z, Lu L, Qiu T, Shim HJ, Chen X, Jeon B (2019) A privacy-preserving image retrieval based on ac-coefficients and color histograms in cloud environment, computers. Materials & Continua 58(1):27–43
35. Xiao D, Liang J, Ma Q, Xiang Y, Zhang Y (2019) High capacity data hiding in encrypted image based on compressive sensing for nonequivalent resources. Computers, Materials & Continua 58(1):1–13
36. Yang J, Xie J, Zhu G, Kwong S, Shi YQ (2014) An effective method for detecting double JPEG compression with the same quantization matrix. IEEE Trans. Inf. Foren. Sec 9(11):1933–1942
37. Yang J, Zhang Y, Zhu G, Kwong S (2020) A Clustering-based framework for improving the performance of jpeg quantization step estimation. IEEE Trans. Circuits Syst. Video Technol. https://doi.org/10.1109/TCSVT.2020.3003653
38. Zhang W, Wang H, Hou D, Yu N (2016) Reversible data hiding in encrypted images by reversible image transformation. IEEE Trans. Multimedia 18(8):1469–1479

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.