Copyright © 2019 Tech Science Press CMC, vol.59, no.1, pp.239-255, 2019

A GLCM-Feature-Based Approach for Reversible Image Transformation

Xianyi Chen[1, 2, *], Haidong Zhong[1, 2] and Zhifeng Bao[3]

Abstract: Recently, a reversible image transformation (RIT) technology that transforms a secret image to a freely-selected target image is proposed. It not only can generate a stego-image that looks similar to the target image, but also can recover the secret image without any loss. It also has been proved to be very useful in image content protection and reversible data hiding in encrypted images. However, the standard deviation (SD) is selected as the only feature during the matching of the secret and target image blocks in RIT methods, the matching result is not so good and needs to be further improved since the distributions of SDs of the two images may be not very similar. Therefore, this paper proposes a Gray level co-occurrence matrix (GLCM) based approach for reversible image transformation, in which, an effective feature extraction algorithm is utilized to increase the accuracy of blocks matching for improving the visual quality of transformed image, while the auxiliary information, which is utilized to record the transformation parameters, is not increased. Thus, the visual quality of the stego-image should be improved. Experimental results also show that the root mean square of stego-image can be reduced by 4.24% compared with the previous method.

Keywords: Image encryption, feature extraction, reversible image transformation, GLCM.

1 Introduction

With the development of cloud service, more and more images are outsourced to cloud for storage or processing. However, some private information may be leaked out, such as design drawings and travel photos, and the eavesdropper is easy to steal these contents.

There are two common ways to protect information from leakages: encryption [Bhatnagar, Wu and Raman (2013); Shan, Chang, Zhong et al. (2012); Shen, Shen, Chen et al. (2017)] and data hiding [Chen, Chen and Wu (2017); Zhou, Wu, Yang et al. (2017); Chan and Cheng (2004); Wu and Wang (2015)], while the former is easy to cause the eavesdropper's suspicious because of the messy codes of cipher text with the special form, thus the latter-data hiding attracts more and more researchers recent years, and then

[1] School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, 210044, China.

[2] Jiangsu Engineering Centre of Network Monitoring, Nanjing, 210044, China.

[3] School of Computer Science and Information Technology, RMIT University, Melbourne, Australia.

[*] Corresponding Author: Xianyi Chen. Email: 0204622@163.com.

CMC. doi:10.32604/cmc.2019.03572 www.techscience.com/cmc

many algorithms have been proposed. For example, Chan et al. [Chan and Cheng (2004)] applied an optimal pixel adjustment process to the stego-image obtained by the simple LSB substitution method, and the image quality of the stego-image can be greatly improved with low extra computational complexity. Wu et al. [Wu and Wang (2015)] designed a novel steganography approach using a reversible texture synthesis and weave the texture synthesis process to conceal secret messages. However, although these methods have high concealment, most of them are hardly to achieve a large payload (more than 1 bit per pixel).

In order to improve hiding capacity, Lee et al. [Lee and Tsai (2014)] proposed a new secure image transmission technique, which transforms automatically a given large-volume secret image into a so-called secret-fragment-visible mosaic image with the same size. It has a great hidden capacity and high concealment. Based on Lee et al.'s method, Hou et al. [Hou, Zhang, and Yu (2016)] designed a reversible image transformation (RIT) method, in which the secret image and target image are divided into N blocks with the same manner firstly, and then the block features of the two group blocks are extracted. Therefore, the selection of the block feature is very important for improving the performance of the image transformation.

In Lee et al.'s method and Hou et al.'s method, the standard deviation (SD) is selected as the only feature during the block matching and the visual quality of transformed image is not so good. Thus, the accuracy of blocks matching should be increased by choosing more image feature descriptors for improving the visual quality of transformed image, such as the GLCM descriptors [Haralick, Shanmugam and Dinstein (1973); Ulaby, Kouyate, Brisco et al. (1986)].

In our proposed method, we choose GLCM descriptor as the image block feature because it can concentrate in a small range close to zero and the frequency fast drops with the increasing of the feature value. Moreover, it can enhance the accuracy of block matching and improve the visual quality of transformed image, while the amount of the auxiliary information is unchanged. So, the visual quality of stego-image can be improved. Thus, the main contribution of the proposed method is that we have proved that the existing feature such as GLCM descriptor can improve the visual quality of transformed image and stego-image.

The rest of this paper is arranged as follows. In section 2, the related work is described. In section 3, the framework of the proposed method is introduced and detailed steps about feature extraction for block matching, reversible shift and rotate transformation and secret image extraction are expressed. Section 4 displays the performance of the proposed method through the experimental results and Section 5 concludes.

2 Related work

In order to protect the outsourced image and secret information, many reversible data hiding in encrypted images (RDH-EI) methods have been proposed to encrypt the outsourced image and embed secret information into the encrypted image. The existing RDH-EI methods can be grouped into three categories: vacate room after encryption (VRAE) methods [Zhang (2011); Hong, Chen, and Wu (2012)], reserving room before encryption (RRBE) methods [Ma, Zhang, Zhao et al. (2013); Cao, Du, Wei et al. (2016)]

and RIT methods [Zhang, Wang, Hou et al. (2016)].

Zhang [Zhang (2011)] proposed the framework of "VRAE", in which, the data hider divides the encrypted image blocks into two sets firstly, then embed secret bits by flipping three LSBs of a set. To decrease the extracted-bits error rate, Hong et al. [Hong, Chen, and Wu (2012)] evaluated the complexity of image block respectively. However, the "VRAE" methods used by the cloud server should be specified together with the receiver.

Ma et al. [Ma, Zhang, Zhao et al. (2013)] designed the framework of "RRBE", in which the image owner can reverse the room of LSBs by using an RDH method and encrypt the self-embedded image, then the cloud sever embeds secret data into the reversed LSBs of encrypted image. Cao et al. [Cao, Du, Wei et al. (2016)] compressed pixels in the local patch by sparse representation and achieve a higher reversed room than other previous methods. The complexity of this framework is determined by the sender who should reserve room for RDH by exploiting the redundancy within the image, and thus the RDH method used by the cloud sever should be specified with the sender.

Therefore, the framework of "VRAE" cannot ensure that the encrypted image after data extraction can decrypt and obtain the original image in the receiver, and the framework of "RRBE" need the sender undertake the algorithm complexity since the original image in the sender should be compressed and reversed room for data hiding. In other words, the RDH method used by cloud sever in the two frameworks is receiver-related or sender-related. However, the cloud sever may be semi honest and should not know the encryption or decryption methods which is concerned with the sender and receiver in the public cloud environment. Therefore, data embedding in the cloud sever should be not have effect on the encryption and decryption method. In other words, the cloud sever can utilize arbitrary classic RDH methods to embed secret information into encrypted image which is similar to other image, and the framework is independence of the receiver-related or sender-related frameworks. How to transform reversibly the original image to the encrypted image which is similar to other image is a more challenging problem, which is called "reversible image transform" (RIT).

The RIT method was designed for image privacy protection because the secret information is just the image itself. Although the method of Yang et al. [Yang, Ouyang, and Harn (2012)] can be used for "secret sharing" by embedding an image into several other images, the transmission and storage of multiple images cause the practicability to be low. Therefore, it is very challenging and important to hide one image into other one with the same size, which is called "image transformation". The first image transformation technology is proposed by Lai et al. [Lai, and Tsai (2011)], they chosed a target image similar to the secret image in an image database, and transformed each secret block to generate the final stego-image by the map between secret blocks and target blocks, then embedded the map. Lai et al.'s method is reversible, but the visual quality of stego-image is not good because the auxiliary information is very large, and it needs more time to choose a target image in a database. Lee et al. [Lee and Tsai (2014)] improve Lai et al.'s method by transforming a secret image to a freely-selected target image and reduce the auxiliary information. However, the method only reconstructs a good estimation of secret image because traditional color transformation method is not reversible.

In order to overcome the shortcomings of Lai et al.'s and Lee et al.'s methods, Hou et al. [Hou, Zhang, and Yu (2016)] presented a novel RIT method, in which, they transform a secret image to a freely-selected target image and obtain a stego-image similar to the target image by designing a reversible shift transformation. Before shifting image blocks, an effective clustering algorithm is used to match secret and target blocks, which not only can improve the visual quality of transformed image, but also can reduce the auxiliary information for recording block indexes. In this method, image block is paired by similar means and standard deviations (SDs) between the original and target images. Let a block B be a set of pixels such that $B = \{p_1, p_2, \dots, p_n\}$, and then the mean value and SD can be calculated as follows:

$$u = \frac{1}{n}\sum_{i=1}^{n} p_i \tag{1}$$

$$\sigma = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(p_i - u)^2} \tag{2}$$

As shown in Fig. 1, by RIT, the secret image can be transformed to an image similar to the target image. In previous methods, the transformed image is utilized to embed the auxiliary information with reversibility and RDH realizes that the stego-image can be returned into the transformed image completely. In addition, RIT achieves the transformed image that can be restored to the secret image without error, and secret image can not be recovered only by target image.

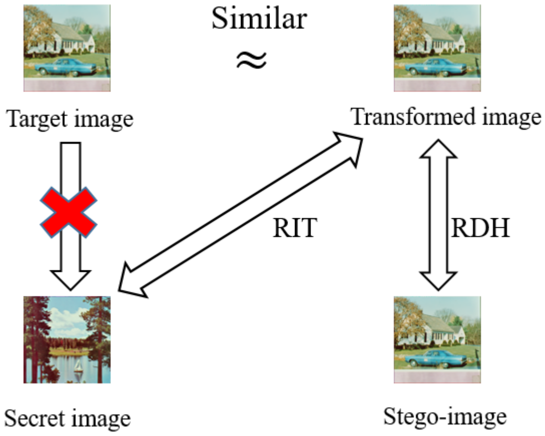


Figure 1: Reversible image transformation

Inspired by the RIT method, Zhang et al. [Zhang, Wang, Hou et al. (2016)] transform the original image into the encrypted image which looks like the target image and propose the RDH-EI framework based on RIT. Since the correlation of transformed image are not destructed, the cloud sever can embed secret bits by a traditional RDH method. The RDH method used by the cloud sever is not affected by the encryption and decryption algorithm, and thus it is irrelevant with neither the sender nor receiver. Therefore, it is a very meaningful work to improve the visual quality of transformed image and stego-image in RIT method which is used to encrypt the original image.

3 Proposed method

In this section, the proposed method will be described with three steps: (1) Feature extraction for block matching; (2) Reversible shift and rotate transformation; (3) Secret image extraction. The detail is introduced in Fig. 2.

To hide the secret image, a data hider firstly calculates each image block feature and utilizes K-means clustering algorithm to divide image blocks into K classes, then moves each secret block to match the corresponding target block. After that, each pixel in secret blocks are added to the quantified difference, which is between the secret and matched target blocks, for having a similar mean with the matched target blocks. Then the overflow/underflow pixels are truncated and each block is rotated to the optimal angle for minimizing the root of mean square error (RMSE) between the rotated and the matched target blocks.

In RIT method, the auxiliary information contains class index, quantified difference, small overflow/underflow information and rotation angle, which also need to be recorded and embedded into the transformed image by RDH method. On the receiver side, after obtaining the auxiliary information, the receiver can use the auxiliary information to rotate each block to anti-angle, restore overflow/underflow pixels, remove quantified difference and recover positions of each secret image block. Finally, the secret image can be recovered completely.

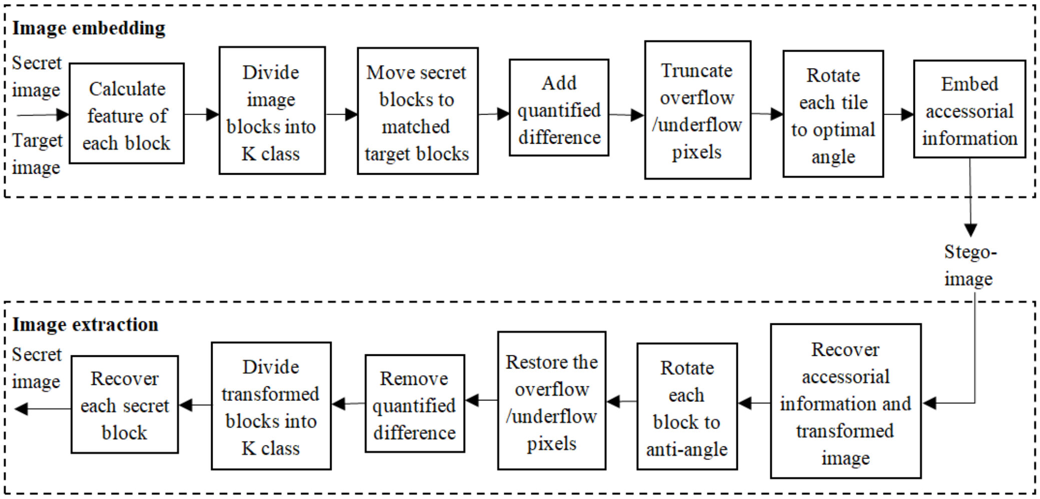


Image embedding
Secret image
Target image
Calculate feature of each block
Divide image blocks into K class
Move secret blocks to matched target blocks
Add quantified difference
Truncate overflow /underflow pixels
Rotate each tile to optimal angle
Embed accessorial information
Stego-image
Image extraction
Secret image
Recover each secret block
Divide transformed blocks into K class
Remove quantified difference
Restore the overflow /underflow pixels
Rotate each block to anti-angle
Recover accessorial information and transformed image

Figure 2: System framework of the proposed method

3.1 Feature extraction

In Haralick et al.’s method [Haralick, Shanmugam, and Dinstein (1973)], 13 textural features can be derived from the normalized GLCM. These features measure different aspects of the GLCM, but many are correlated. Thus, Ulaby et al. [Ulaby, Kouyate, Brisco et al. (1986)] prove that energy, entropy, contrast and relevance are not correlated, which not only have a high precision of texture complexity, but also can reduce the computational burden.

To improve the visual quality of transformed image, the proposed method chooses these GLCM descriptors as image blocks features because it can concentrate in a small range close to zero and the frequency fast drops with the increasing of the feature value.

Suppose the distance of image pixels is $d = \{dx, dy\}$, the direction is $\theta = \{0^{\circ}, 45^{\circ}, 90^{\circ}, 135^{\circ}\}$, and thus d belongs to the rectangle region $\{(0, d), (d, d), (d, 0), (-d, d)\}$, GLCM also can be denoted as $g(i, j, d, \theta)$. The main characteristic parameters are described as follow.

(1) Energy. Energy E_1 is used to describe the distribution of image blocks uniformity and the coarse grain size of the texture, and E_1 can be calculated by

$$E_1 = \sum_{i=1}^{L} \sum_{j=1}^{L} g(i, j, d, \theta)^2 \tag{3}$$

where L is the number of rows or columns of GLCM, (i, j) is pixel coordinate, and d (d>0) is a distance in the corresponding direction.

(2) Entropy. Entropy H_1 is utilized to measure the amount of information contained in an image. If the image texture is complex, the entropy value is correspondingly large. H_1 can be represented by

$$H_1 = -\sum_{i=1}^{L} \sum_{j=1}^{L} g(i, j, d, \theta) log_2 g(i, j, d, \theta) \tag{4}$$

(3) Contrast. Contrast C_1 is used to describe the clarity and texture depth of an image. When an image has a clear and deep texture, the contrast of the image will be correspondingly large, and C_1 can be calculated by

$$C_1 = -\sum_{i=1}^{L} \sum_{j=1}^{L} (i - j)^2 g(i, j, d, \theta) \tag{5}$$

(4) Relevance. Relevance R_1 is an index to measure the degree of similarity in the row (column) of GLCM. The high or low R_1 is positively related to the local gray correlation of the image. R_1 can be calculated by

$$R_1 = \left[\sum_{i=1}^{L} \sum_{j=1}^{L} (i * j) * g(i, j, d, \theta) - \mu_1 \mu_2 \right] - \sigma_1 \sigma_2 \tag{6}$$

where μ_1 and μ_2 are mean values in the row(column) of GLCM, σ_1 and σ_2 are SD values. Note that E_1, H_1, C_1 and R_1 are texture feature parameters in one direction.

However, the texture feature parameters in four directions are not different. The mean square error (MSE) can be assigned weights of texture feature parameters in four directions, and it can restrain the orientation vector and make the obtained texture features independent of direction. Thus, the complexity of sub block texture can be more accurately calculated. Taking energy feature parameter as an example, the energy values in four directions are E_1, E_2, E_3 and E_4, then denote

$$\bar{E} = (E_1 + E_2 + E_3 + E_4)/4 \tag{7}$$

$$MSE_i = (E_i - \bar{E})^2 \tag{8}$$

$$w_i = \frac{MSE_i}{\sum_{i=1}^{4} MSE_i} \tag{9}$$

$$E = w_1E_1 + w_2E_2 + w_3E_3 + w_4E_4 \tag{10}$$

where $\mathrm{MSE_i}$ is the mean square error of four directions, w_1, w_2, w_3 and w_4 are the weights of the characteristic parameter assigned to four directions, respectively. And the assigned weights of entropy H, contrast C and relevance R also can be calculated as the formal (7-10). Finally, the complexity of each image block can be represented by

$$f = \varphi_1E + \varphi_2H + \varphi_3C + \varphi_4R \tag{11}$$

where f is the complexity of image blocks, φ_1, φ_2, φ_3 and φ_4 are the weight assigned to four main feature parameters, which can be calculated as the formulas (7-9).

3.2 Block matching

After replacing the SD with f, a suitable block pairing should be selected. In Lee et al.'s method, the secret and target blocks are sorted in ascending order according to their SDs, respectively, and then each secret tile is paired up with a corresponding target block in turn according to the order. To restore the secret image from the transformed image, the positions of the secret tiles must be recorded and embedded into the transformed image with a reversible method, thus $\lceil NlogN \rceil$ bits are needed for recording the block indexes. However, it will decrease the visual quality of stego-image when the number of image blocks is large or block size is small.

In the proposed method, the blocks with close fs are deemed as one class since most of fs are similar. The secret block should be transformed to the target block in the same class.

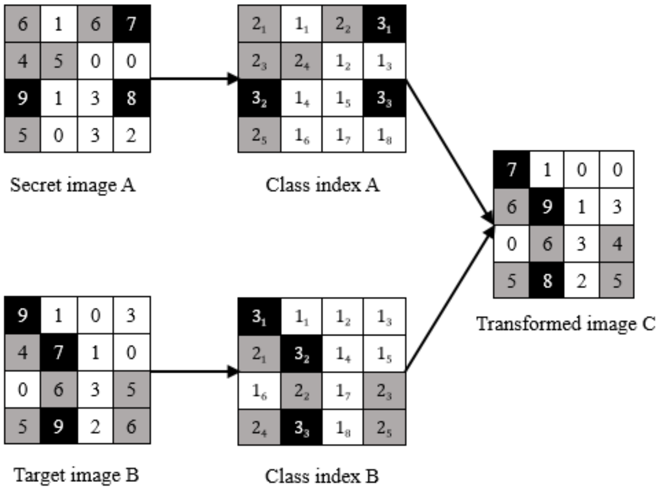
(1) Cluster all fs of secret blocks into K classes by a traditional clustering method such as K-means, and sort the K classes to ensure that the fs in the ith class is smaller than in the jth class when $1 < i < j \leq K$.

(2) Classify the target blocks by the classes' volumes of secret image, the scanning order, and each target class has the same volume with the corresponding class of the secret image. Let the αth secret image class contains $\mathrm{n_\alpha}$ blocks, where $1 \leq \alpha \leq K$. The first n_1 target blocks, with the smallest fs, are divided into the first class, the second n_2 target blocks, with second-smallest fs, are divided into the second class, and so on, until all of target blocks are divided.

(3) Distribute a compound index α_β to each block, where α_β is the βth block of the αth class and $1 \leq \beta \leq n_\alpha$. Then the $\alpha_\beta th$ secret blocks should be replaced to $\alpha_\beta th$ target blocks, and the transformed image is generated.

A simple example of block matching is shown in Fig. 3. The secret tiles are divided into three classes here: (1) $fs\{0,1,2,3\}$ belongs to the class 1, it is labeled as "white"; (2) $fs\{4,5,6\}$ belongs to the class 2, labeled as "gray"; (3) $fs\{7,8,9\}$ belongs to class 3, labeled as "black". The compound index for each block can be defined by scanning fs

classes in the raster order. For instance, the second secret block is the first one of SD class 1 that is assigned as 1_1, and the seven block is the second one of SD class 1 that is assigned as 1_2. After that, the target blocks can be classified according to the class of secret blocks, and the one-to-one map between secret blocks and target blocks will be created. Then the $\alpha_\beta th$ secret blocks should be transformed to $\alpha_\beta th$ target blocks and replace them. Finally, the transformed image is generated and the class index A is recorded as auxiliary information for recover the position of secret image blocks.



Tile index A	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Tile index B/C	5	2	10	1	12	13	3	4	6	7	8	14	16	9	11	15

Figure 3: An example of block matching

3.3 Reversible shift and rotate transformation

After block matching, the transformed image blocks should be shifted and rotated for being similar as the target image. Let the matched block C is a set of pixels $C = \{p_1, p_2, \dots, p_n\}$ with mean value u_C, and the target block B is a set of pixels $B = \{p_1{}', p_2{}', \dots, p_n{}'\}$ with mean u_B, then the matched block $C = \{p_1'', p_2{}'', \dots, p_n{}''\}$ can be generated.

$$p_i'' = p_i + u_B - u_C. \tag{12}$$

To keep the transformation reversible, the amplitude $u_B - u_C$ should be rounded to be an integer.

$$\Delta u = round(u_B - u_C). \tag{13}$$

To solve the overflow/underflow problem, Δu should be modified as follow. Denote the maximum overflow pixel value as OV_{max} for $u \geq 0$ and the minimum underflow value is UN_{min} for $u < 0$, T is a parameter to control a balance between the number of overflow and underflow and the distance from the mean value of target image. When $\Delta u \geq 0$:

$$\Delta u = \begin{cases} \Delta u + 255 - OV_{max}, & if\ 255 - OV_{max} < 0 \\ \Delta u - T, & if\ 255 - OV_{max} \geq 0 \end{cases} \quad (14)$$

and when $\Delta u < 0$:

$$\Delta u = \begin{cases} \Delta u - UN_{min}, & if\ UN_{min} < 0 \\ \Delta u + T, & if\ UN_{min} \geq 0 \end{cases} \quad (15)$$

To reduce the amount of auxiliary information, Δu should be quantized to a little integer.

$$\Delta u = \begin{cases} \lambda \times round\left(\frac{\Delta u}{\lambda}\right), & if\ u \geq 0 \\ \lambda \times floor\left(\frac{\Delta u}{\lambda}\right) + \frac{\lambda}{2}, & if\ u < 0 \end{cases} \quad (16)$$

where the quantization step λ must be an even parameter and $floor(\cdot)$ is ceiling function. Then $\Delta u' = 2|\Delta u|/\lambda$ should be recorded as the final auxiliary information, which is embedded into the transformed image, and λ is a parameter to make a trade-off between the amount of auxiliary information and the distance from the mean value of target image. Thus, the matched block $C = \{p_1'', p_2'', \ldots, p_n''\}$ can be shifted as follows.

$$\mathrm{p}_\mathrm{i}'' = \mathrm{p}_\mathrm{i} + \Delta \mathrm{u}. \quad (17)$$

Although modifying the amplitude $u_B - u_C$ to Δu, the overflow/underflow problem may still occur. To deal with the problem, the pixels less than 0 are truncated to be 0, and the pixels more than 255 are truncated to be 255, then a location map $LM = (lm_1, lm_2, \ldots, lm_n)$ can be generated to record the position of overflow/underflow pixels.

$$lm_i = \begin{cases} -p_i'', & if\ p_i'' < 0 \\ p_i'' - 255, & if\ p_i'' > 255 \end{cases} \quad (18)$$

The LM can be compressed well because, it is very small. To further maintain the similarity between the transformed image and target image as much as possible, the shifted block C can be rotated into one of the four angles 0°, 90°, 180° or 270°. The best angle $\vartheta \epsilon \{0^\circ, 90^\circ, 180^\circ, 270^\circ\}$ is selected for minimizing the root of mean square error (MSE) between the rotated block and the target block.

Now, the transformed image is generated, and the auxiliary information containing the class index of secret image, quantified difference $\Delta u'$, small overflow/underflow information LM and rotation angle ϑ, which also can be embedded into transformed image by the arbitrary traditional RDH methods. Before embedding, the auxiliary information should be compressed by the classic method such as Huffman code for reducing the amount and should be encrypted by the traditional way such as AES encryption for security.

3.4 Secret image extraction

Image recovery is the opposite process of the image hiding. The transformed image and embedded auxiliary information firstly can be recovered by the RDH method, and the information can be decrypted and decompressed. The transformed image is divided into non-overlapping N blocks, and each block is rotated in the anti-direction of ϑ.

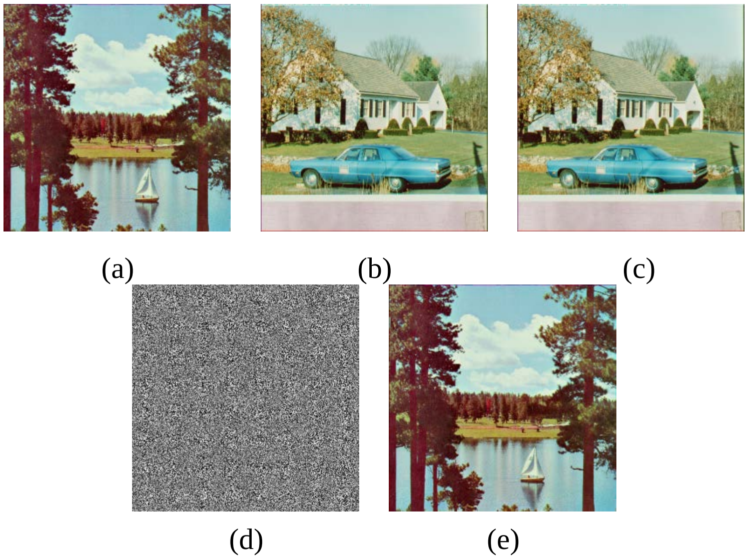
After that, by quantified difference $\Delta u' = 2|\Delta u|/\lambda$, if $\Delta u'$ is an even number, then

$\Delta u \geq 0$ and Δu can be restored by $\Delta u = \lambda * \Delta u'/2$; if $\Delta \mathrm{u}'$ is an odd number, then $\Delta u < 0$ and Δu can be restored by $\Delta u = -\lambda * \Delta u'/2$. Then each pixels of rotated blocks can remove Δu. Finally, the removed blocks can be re-assigned to the position of matched blocks in secret image by the class index of the secret image, and the secret image can be recovered.

4 Experimental Results

4.1 Parameter setting for the proposed method

In the proposed method, we adopt the Huffman code to reduce the auxiliary information, and use the RDH method in Sachnev et al. [Sachnev, Kim, Nam et al. (2009)] to embed the compressed information. For security reason, the compressed information should be encrypted before embedding, and Fig. 4 is an example that reflects security of the algorithm. Fig. 4(a) is the secret image, Fig. 4(c) is the stego-image, which is similar to the target image Fig. 4(b). If the eavesdropper has a wrong key, the messy image Fig. 4(d) will be achieved. Thus, only the receiver with correct key can restore the secret image.

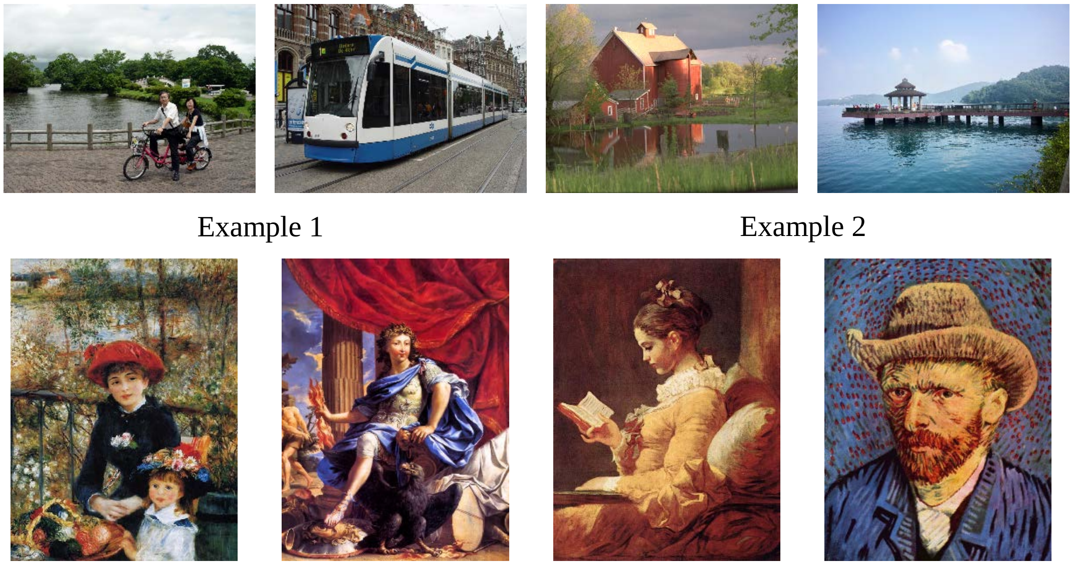


(a) (b) (c)

(d) (e)

Figure 4: An example that reflects security (a) Secret image. (b) Target image. (c) Stego-image. (d) Recovered image (wrong key). (d) Recovered image (correct key)

The experiments are carried with MATLAB-R2014a. The test machine is Asus PC with 4200 CPU @2.80GHz and 8.00 GB RAM. The test images shown in the experiments are listed, which are in the PNG format adopted by many cameras or computer equipments. In this subsection, four typical combinations of secret and target images in Fig. 5 are applied to discuss how to properly set parameters on the proposed method.



Example 1 Example 2

Example 3 Example 4

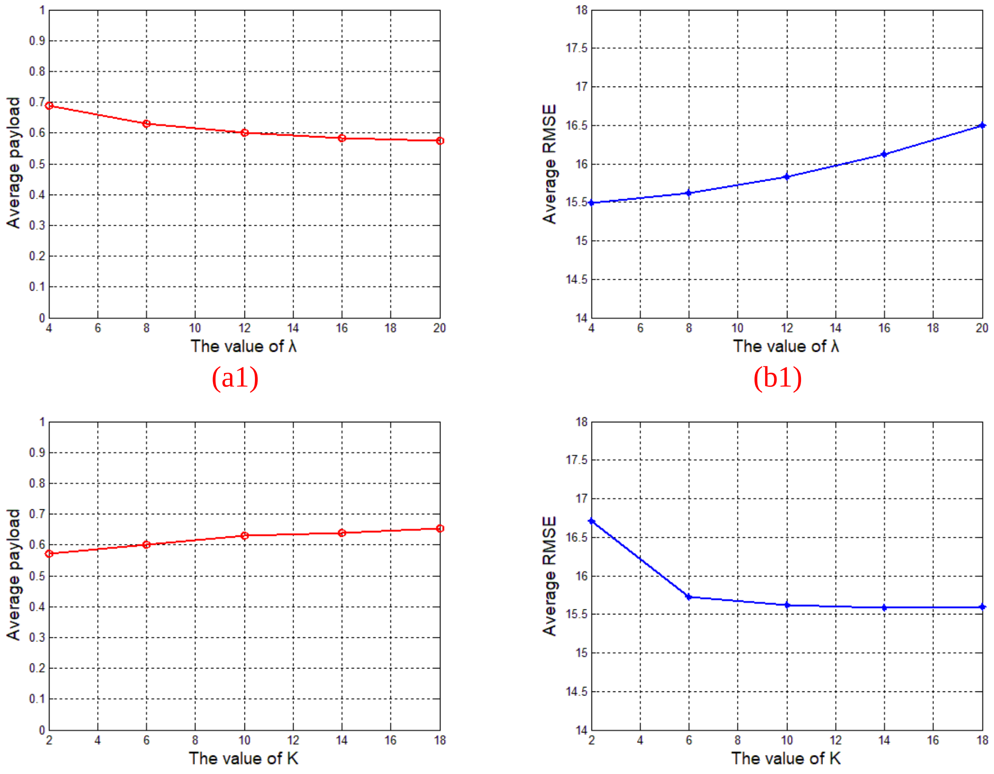
Figure 5: Four typical combinations of secret and target images

Table 1: The results for setting parameter λ, K and T

	Example 1		Example 2		Example 3		Example 4		Average	
	AI	RMSE	AI	RMSE	AI	RMSE	AI	RMSE	AI	RMSE
λ=4	0.70	19.68	0.66	13.50	0.72	17.25	0.67	11.54	0.69	15.49
λ=8	0.65	19.75	0.60	13.66	0.66	17.34	0.61	11.72	0.63	15.62
λ=12	0.62	19.90	0.57	13.89	0.63	17.53	0.58	12.00	0.60	15.83
λ=16	0.61	20.15	0.55	14.19	0.62	17.79	0.56	12.34	0.58	16.12
λ=20	0.60	20.42	0.56	14.62	0.61	18.11	0.54	12.83	0.58	16.49
K=2	0.62	21.11	0.53	14.98	0.61	18.37	0.53	12.36	0.57	16.70
K=6	0.61	19.84	0.57	13.79	0.63	17.45	0.59	11.81	0.60	15.72
K=10	0.65	19.77	0.60	13.66	0.66	17.36	0.61	11.70	0.63	15.62
K=14	0.66	19.72	0.61	13.62	0.67	17.32	0.62	11.70	0.64	15.59
K=18	0.67	19.72	0.62	13.62	0.69	17.34	0.64	11.69	0.65	15.59
T=0	0.65	19.75	0.61	13.62	0.73	16.93	0.62	11.65	0.65	15.49
T=10	0.63	19.88	0.60	13.64	0.66	17.37	0.61	11.70	0.63	15.65
T=20	0.63	19.94	0.60	13.67	0.64	17.70	0.61	11.74	0.62	15.76
T=30	0.62	20.04	0.60	13.67	0.64	17.90	0.61	11.79	0.62	15.85
T=40	0.62	20.11	0.60	13.70	0.63	18.06	0.61	11.80	0.62	15.92

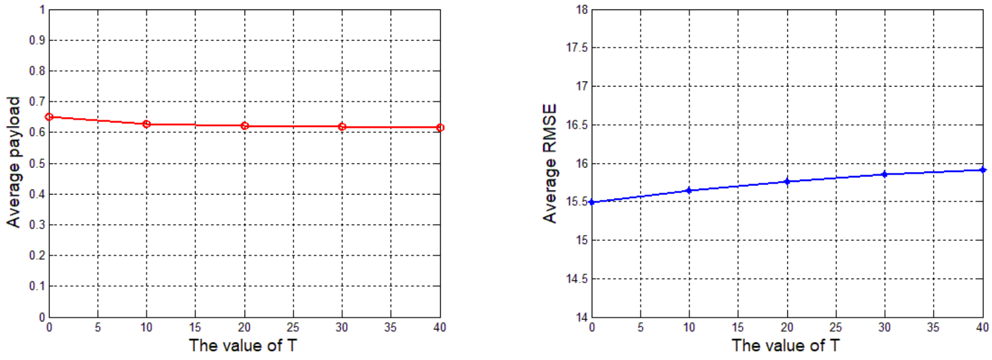
The secret and target images can be divided into the same number of 4×4 blocks. To match these two blocks, the GCML feature and clustering method is utilized to classify the blocks as K classes. To solve the overflow/underflow problem, T is set as a parameter to control the balance between the number of overflow and underflow and mean's bias of target image. To reduce the amount of auxiliary information, λ also is set as a parameter to make a trade-off between the amount of auxiliary information and the mean's bias of target image. The auxiliary information (AI) and the root of mean square error (RMSE) of the transformed image with different parameter λ, K and T for four examples are shown in Tab. 1.

Fig. 6 can express the average payload and RMSE change with parameter λ, K and T more intuitively. In formula (16), the parameter λ is used to reduce the amount of auxiliary information but it results in the mean's bias of target image blocks. To choose an appropriate λ, we maintain the parameter K, T such as $K = 10$, $T = 6$ and change the λ. In Fig. 6(a1) and Fig. 6(b1), when λ is larger than 8, the average RMSE of the created transformed image will increase rapidly but the average payload increases slowly. Thus, $\lambda = 8$ is an appropriate value.



(a1) (b1)

(a2) (b2)



(a3) (b3)

Figure 6: The average payload and RMSE change with different parameters λ, K and T

As mentioned in Section 2.1.1, the parameter K is used to classify the images blocks into K classes. To choose an appropriate K, we maintain the parameter λ, T such as $\lambda = 8$, $T = 6$ and change the value of λ. In Fig. 6(a2) and Fig. 6(b2), when K is larger than 10, the average RMSE of the created transformed image will decrease slowly but the average payload is increased slowly. Thus, $K = 10$ is an appropriate value.

In formula (14-15), the parameter T is utilized to reduce the amplitude of the mean's bias. To choose an appropriate T, we maintain the parameter K, λ such as $K = 10$, $\lambda = 8$ and change the value of T. In Fig. 6(a3) and Fig. 6(b3), when T is larger than 8, the average RMSE of the created transformed image will increase rapidly but the average payload increases slowly. Thus, $T = 10$ is an appropriate value.

4.2 Comparison with previous methods

4.2.1 Performance comparison

To compare the performance, the same compression method by Huffman coding is used to compressed the auxiliary information, and same RDH scheme proposed in Sachnev et al. [Sachnev, Kim, Nam et al. (2009)] are utilized to embed the compressed information into the transformed image for the proposed method and Hou et al.'s method. The root means square error (RMSE) and the auxiliary information (AI) are the main performance indexes to appraise the similarity between transformed and target images. The block size 4×4 usually performs best for Hou et al.'s method. Tab. 2 shows the RMSE and AI of the transformed image and stego-image with different block sizes for Example 4. And we can find that the block size 4×4 also performs best for Example 4.

From Fig. 7 and Tab. 3, we can see that the visual quality of transformed image and stego-image of the proposed method outperformed that generated by Hou et al.'s method. The root of mean square of stego-image can be reduced by 4.24% compared with the previous method and the AI approximately equals to Hou et al.'s method. The reason is that an effective feature extraction algorithm of each block is utilized to increase the accuracy of blocks matching for improving the visual quality of transformed image, and the amount of the auxiliary information for recording transformation parameters is unchanged.

Table 2: The results with different block sizes.

Block size	Transformed image (RMSE)	Stego-image (RMSE)	AI (bpp)
3 × 3	9.239	18.504	1.014
4 × 4	11.216	14.289	0.589
6 × 6	15.716	16.666	0.266
8 × 8	18.683	18.931	0.156
10 × 10	21.179	21.331	0.105
12 × 12	23.176	23.262	0.076

Table 3: Performance comparison with Hou et al.'s method

Method	RMSE of transformed image	RMSE of stego-image	AI
The Hou et al.'s method	11.820	14.895	0.593
Proposed method	11.216	14.289	0.589

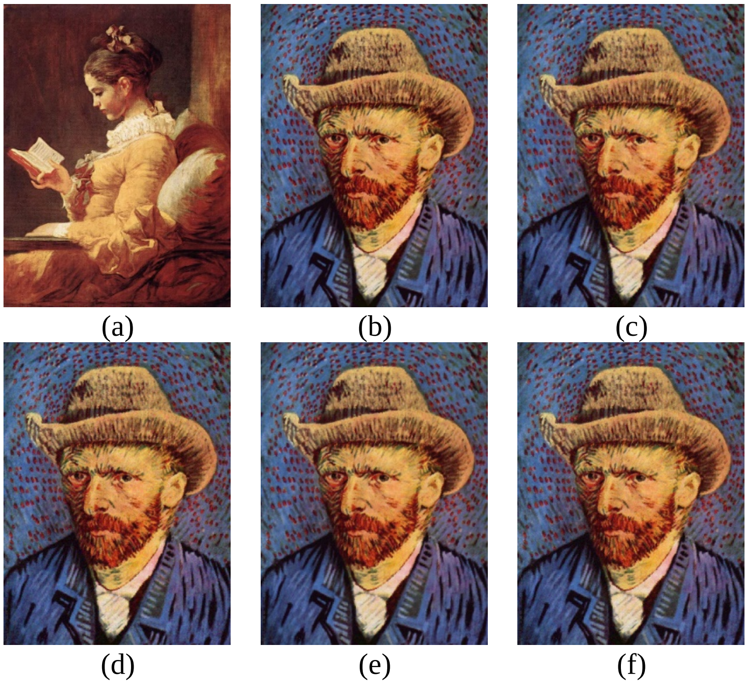


Figure 7: (a) Secret image. (b) Target image. (c) Transformed image by Hou et al.'s method. (d) Stego-image by Hou et al.'s method. e) Transformed image by the proposed method. (f) Stego-image by the proposed method

4.2.2 Feature comparison

In addition to performance comparison, features comparison from reversibility, high capacity, image expansion and strong anti-detection ability are shown in Tab. 4. The proposed method is reversible, but the recovered image is similar to the secret image in Zhou et al.'s method and Lee et al.'s method. Although Wu et al.'s method is reversible, it can not ensure a relatively large payload (more than 1 bit per pixel). But the proposed method can achieve it. Compared with Lai et al.'s method, the stego-image in the proposed method is not expanded and has the same size with secret image. Moreover, the proposed method can resist detection of strong steganalysis because it is hard to recover secret image only by the stego-image which looks like the freely-selected target image.

Table 4: Features comparison with previous methods

Method	Reversibility	High capacity	Image expansion	Anti-detection
Zhou et al.'s method	No	No	Yes	Yes
Wu et al.'s method	Yes	No	Yes	No
Yang et al.'s method	Yes	Yes	Yes	Yes
Lai et al.'s method	Yes	Yes	Yes	Yes
Lee et al.'s method	No	Yes	No	Yes
Proposed method	Yes	Yes	No	Yes

5 Conclusion

In this paper, we proposed a GLCM-feature-based approach for reversible image transformation. Effective feature extraction algorithm of each block is utilized to increase the accuracy of block matching for improving the visual quality of transformed image, and the amount of accessorial information for recording transformation parameters is unchanged. Thus, the visual quality of stego-image should be improved, and the root mean square of stego-image can be reduced by 4.24% compared with the previous method. In future work, we may further improve the visual quality of stego-image from two aspects. On the one hand, the amount of accessorial information such as quantified mean difference should be reduced, or a novel RDH method is designed to reduce the loss of transformed image caused by the accessorial information. On the other hand, more block's feature should be chosen to improve the visual quality of transformed image, and thus improve the visual quality of stego-image.

Acknowledgement: This work is supported by the National Key R&D Program of China under grant 2018YFB1003205; by the National Natural Science Foundation of China under grant 61502242, U1536206, U1405254, 61772283, 61602253, 61672294; by the Jiangsu Basic Research Programs-Natural Science Foundation under grant numbers BK20150925 and BK20151530; by the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD) fund; by the Collaborative Innovation Center of Atmospheric Environment and Equipment Technology (CICAEET) fund, China.

References

Bhatnagar, U. G.; Wu, Q. M. J.; Raman, B. (2013): Discrete fractional wavelet transform and its application to multiple encryption. *Information Sciences*, vol. 223, no. 2, pp. 297-316.

Cao, X.; Du, L.; Wei, X.; Meng, D.; Guo, X. (2016): High capacity reversible data hiding in encrypted images by patch-level sparse representation. *IEEE Transactions on Cybernetics*, vol. 46, no. 5, pp. 1132-1143.

Chan, C.; Cheng, L. (2004): Hiding data in images by simple lsb substitution. *Pattern Recognition*, vol. 37, no. 3, pp. 469-474.

Chen, X.; Chen, S.; Wu, Y. (2017): Coverless information hiding method based on the chinese character encoding. *Journal of Internet Technology*, vol. 18, no. 2, pp. 313-320.

Haralick, R. M.; Shanmugam, K.; Dinstein, I. H. (1973): Textural features for image classification. *IEEE Transactions on Systems Man & Cybernetics*, vol. 3, no. 6, pp. 610-621.

Hong, W.; Chen, T. S.; Wu, H. Y. (2012): An improved reversible data hiding in encrypted images using side match. *IEEE Signal Processing Letters*, vol. 19, no. 4, pp. 199-202.

Hou, D.; Zhang, W.; Yu, N. (2016): Image camouflage by reversible image transformation. *Journal of Visual Communication and Image Representation*, vol. 40, pp. 225-236.

Lai, I. J.; Tsai, W. H. (2011): Secret-fragment-visible mosaic image–a new computer art and its application to information hiding. *IEEE Transactions on Information Forensics & Security*, vol. 6, no. 3, pp. 936-945.

Lee, Y. L.; Tsai, W. H. (2014): A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible color transformations. *IEEE Transactions on Circuits & Systems for Video Technology*, vol. 24, no. 4, pp. 695-703.

Ma, K.; Zhang, W.; Zhao, X.; Yu, N.; Li, F. (2013): Reversible data hiding in encrypted images by reserving room before encryption. *IEEE Transactions on Information Forensics & Security*, vol. 8, no. 3, pp. 553-562.

Sachnev, V.; Kim, H. J.; Nam, J.; Suresh, S.; Shi, Y. Q. (2009): Reversible watermarking algorithm using sorting and prediction. *IEEE Transactions on Circuits & Systems for Video Technology*, vol. 19, no. 7, pp. 989-999.

Shan, M.; Chang, J.; Zhong, Z.; Hao, B. (2012): Double image encryption based on discrete multiple-parameter fractional fourier transform and chaotic maps. *Optics Communications*, vol. 285, no. 21-22, pp. 4227-4237.

Shen, J.; Shen, J.; Chen, X.; Huang, X.; Susilo, W. (2017): An efficient public auditing protocol with novel dynamic structure for cloud data. *IEEE Transactions on Information Forensics & Security*, vol. 12, no. 10, pp. 2402-2415.

Ulaby, F. T.; Kouyate, F.; Brisco, B.; Williams, T. (1986): Textural information in sar images. *IEEE Transactions on Geoscience and Remote Sensing*, vol. 24, no. 2, pp. 235-245.

Wu, K. C.; Wang, C. M. (2015): Steganography using reversible texture synthesis. *IEEE Transactions on Image Processing*, vol. 24, no. 1, pp. 130-139.

Yang, C. N.; Ouyang, J. F.; Harn, L. (2012): Steganography and authentication in image sharing without parity bits. *Optics Communications*, vol. 285, no. 7, pp. 1725-1735.

Zhang, W.; Wang, H.; Hou, D.; Yu, N. (2016): Reversible data hiding in encrypted images by reversible image transformation. *IEEE Transactions on Multimedia*, vol. 18, no. 8, pp. 1469-1479.

Zhang, X. (2011): Reversible data hiding in encrypted image. *IEEE Signal Processing Letters*, vol. 18, no. 4, pp. 255-258.

Zhou, Z.; Wu, Q. M. J.; Yang, C. N.; Sun, X.; Pan, Z. (2017): Coverless image steganography using histograms of oriented gradients-based hashing algorithm. *Journal of Internet Technology*, vol. 18, no. 5, pp. 1177-1184.