Rotation Invariant Copy Move Forgery Detection Method

Emre Gürbüz[1], Güzin Ulutaş[2], and Mustafa Ulutaş[2]

[1]Gaziosmanpaşa University, Tokat Technical Sciences Vocational School, Tokat, Turkey
emregurbuz@msn.com
[2]Karadeniz Technical University, Department of Computer Engineering, Trabzon, Turkey
guzin@ieee.org, ulutas@ieee.org

Abstract

In recent years, due to the increment in the image editing software applications and the easiness of using these, the probability of malicious changes on the images has also increased. Copy–move forgery is one of the most widely applied modification types on the images. In case of that the copied region is rotated before being pasted, forgery detection becomes difficult. Many researchers try on proposing new rotation–invariant techniques for detecting forgeries. For this purpose, various techniques such as Zernike invariants and log–polar transform have been utilized. In this study, Circular Projection technique is used for generating feature vectors from the image blocks. When compared with the results of the studies in the same field, it is observed that the proposed method gives better results even on the rotation operations with greater angles. Experimental results show that the proposed technique is robust against scaling and mirroring operations.

1. Introduction

The increment in the number of open source or commercial image editing software applications and the easiness of using these have increased the probability of malevolent people to make changes on any image without leaving any visible marks. Therefore, usage of digital images in the fields that require authentication (e.g. while presenting to the court of law during judgment, or diagnosing the medical images belonging to significant people) has become impossible. In recent studies, the techniques used for authenticating digital images are categorized in two sub–classes: active techniques and passive techniques.

Techniques that are named as "digital watermarking" and belong to the first class are based on hiding a specifically generated data (watermark) into the image, before the stage of authentication. In order for the watermark to be hidden, the image capturing device must be specially equipped, or the watermark must be inserted into the image via a special software application after acquiring the image. High prices of the image capturing devices with the ability of watermarking, or the difficulty on applying an extra process on the acquired image to insert watermark cause the usage of the active techniques in the field of image authentication to be more difficult. As being different from the active ones, the passive techniques do not need any extra information for authenticating digital images. These techniques, which authenticate the digital images by using the statistical features existing in the images, draw interest from the researchers especially in recent times.

One of the most widely implemented forgery techniques which is tried to be detected by the passive techniques is copy–move forgery. The first method for detecting this kind of forgery, which is based on covering a region (that is intended to be hidden) by another region on the same image, was proposed by Fridrich et. al, in 2003 [1]. In that study, the image is assumed to consist of the blocks with sizes of 8×8, and feature vectors are extracted from each block by using Discrete Cosine Transform (DCT). The mentioned study, which lexicographically sorts the feature vectors extracted from the blocks, tests the similarities between the adjacent blocks by using Euclidian distance. The blocks represented by the vectors, which are decided to be similar are marked as forged by the technique. After this study, which is based on the usage of DCT and uses feature vectors with size of 1×64, Popescu et. al. used Principal Component Analysis (PCA) for acquiring feature vectors from the blocks, in 2006 [2]. The main goal of using PCA is reducing the sizes of the feature vectors and decreasing the operational complexity during authentication. The main drawback of both of these techniques is that the authentication process fails in case blurring and noise addition operations are applied for removing the marks after tampering the image. For this purpose, Mahdian et. al. used blur invariants for extracting feature vectors in their study, in 2007 [3]. Thus, their technique has gained robustness against blurring and noise addition operations. In 2011, Huang et. al. used previously determined parts of the feature vectors that are acquired after applying DCT, for representing the blocks [4]. Results of the mentioned study, which proposes a novel algorithm for detecting the similarities between the vectors, showed that the method is robust against blurring, noise addition and JPEG compression operations. In 2012, Cao et. al. separated the frequency components which are acquired after applying DCT to the image blocks, into four regions [5]. Mean values of each region were used for constructing the feature vector. It was shown by the study that the feature vectors with sizes of 1×4 were robust against blurring and noise addition operations.

The probability of the copied region to be rotated before pasting was firstly considered by Myrna et. al., in 2007 [6]. In their study, they reduced the dimensions of the image by using Wavelet Transform, and then constructed the feature vectors by representing the blocks in log–polar coordinate system. By using Fourier–Mellin transform, Bayram et. al. showed that satisfactory results can be obtained even if the copied region is rotated before being pasted, in 2009 [7]. But their technique is not able to produce reliable authentication results in case of the rotation operations having more than 10 degrees of angle. In 2009, Bravo–Solorio et. al. produced single–dimensional feature vectors by applying projection on polar axis, after representing the blocks acquired from the image on the log–polar coordinate system [8]. As being different from the study of Myrna et. al., computation of the feature vectors on single dimension contributed to decrement of the operational complexity. However, when the results of these studies are examined, it is observed that the authentication success rates are low if the rotation angles are high.

In this study, it is aimed to propose a novel rotation invariant copy–move forgery detection methodology. For this purpose, in the stage of acquiring feature vectors, Circular Projection technique is utilized for the first time in the literature. According to the experimental results acquired, when compared with the study of Bravo–Solorio et. al., it is shown that the proposed method has higher correct authentication rates even on the rotations with high angles. Also, experimental results show that the technique is robust against scaling and mirroring operations.

The rest of the study is organized as follows: Chapter 2 describes the Circular Projection technique. While Chapter 3 explains the details of the proposed technique, Chapter 4 gives the experimental results. Finally, conclusions about the proposed methodology are given in Chapter 5.

2. Representation of Circular Projection

Texture matching techniques basically consist of two stages: representation of the texture and deciding the similarity by comparing the feature vectors used in the representation. So as to reduce the time complexity in the stage of matching and render the matching process independent of rotation, Tsai et. al. proposed Circular Projection transform, in 2002 [9]. The proposed technique can be defined as representing a two–dimensional grayscale image as a single dimensional feature vector.

Assume that the texture feature of which is to be extracted exists in a circular area having a radius of R. Circular Projection of an image which exists on a Cartesian coordinate system denoted by *I(x, y)* is calculated as follows. Firstly, Cartesian coordinate system is transformed to polar coordinates by using (1).

$$x = r.\cos\theta, \qquad y = r.\sin\theta \tag{1}$$

Let the circular projection with radius of r of an image denoted by I be denoted by *p(r)*. The equation used for calculating the circular projection value for the mentioned radius is given in (2).

$$p(r) = \frac{1}{n_r}\sum\nolimits_k I(r.\cos\theta_k,\ r.\sin\theta_k) \tag{2}$$

r value given on the expression changes between *0* and R. n_r value shows the total number of pixels which exist in the circle given with radius r. Thus, a single–dimensional feature vector is acquired by calculating the mean energy of the texture in different radiuses. In the computation of correlation which is used for measuring the similarity of the feature vectors, *p(r)* values belonging to each of the circles have the same priority. During the generation of the single–dimensional feature vector, since the circles with increasing radius values are used, the generated vector is invariant against rotation.

In the stage of comparing the extracted feature vectors, normalized correlation statement is used. Let P_D and P_R be single–dimensional feature vectors which are determined by using different radius values corresponding to the texture and the reference, respectively. The normalized correlation between these two vectors is computed by using (3).

$$\rho = \frac{\sum_{r=0}^{R}\left[P_R(r)-\mu_R\right]\left[P_D(r)-\mu_D\right]}{\left\{\sum_{r=0}^{R}\left[P_R(r)-\mu_R\right]^2 \cdot \sum_{r=0}^{R}\left[P_D(r)-\mu_D\right]^2\right\}^{1/2}} \tag{3}$$

Means of the feature vectors which are acquired by using the texture and the reference texture are denoted by μ_D and μ_R, respectively. The normalization factor obtained after the operation is within the range of -1 to 1.

3. Proposed Technique

In this study, by using the circular projection technique, the process of acquiring the feature vectors from the image blocks is performed. It is assumed that the image consists of overlapping blocks, and by computing the correlation factors between the vectors which represent the blocks, determination of the similar blocks is carried out. The proposed algorithm consists of three parts. In the first part, the image is separated into overlapping blocks and the feature vectors corresponding to each of these blocks are generated. As the result of the first part, a lexicographically sorted matrix which includes the feature vectors belonging to all of the blocks is generated. In the second part, the similarities between the rows of the mentioned matrix are examined and various information corresponding to the vectors which are determined as similar (shift vectors) are stored in another matrix. In the last part, the amount of the shift vectors which exist in the matrix generated in the previous step is examined, and the blocks which are represented by the shift vectors amounts of which are more than a determined threshold value are marked as tampered. In this section of the study, the mentioned parts are going to be expressed in detail.

3.1. Acquisition of Feature Vectors

As the first step in acquiring the feature vectors, the 24–bit image with size of $M\times N$ that is to be authenticated is separated into overlapping blocks with sizes of $B\times B$. The number of feature vectors that will be generated for such an image is $(N-B+1)\cdot(M-B+1)$. The increment in the block size decreases the number of feature vectors to be constructed, and so that, contributes to the decrement in the time complexity. But the increment in the block size decreases the authentication performance of the method in case the copied and pasted region is smaller than the block size. Because of this, for the method to operate perfectly, one of the most important parameters is the block size.

The steps followed for constructing a feature vector with $(4+B/2)$ elements from each block, which are acquired depending on the preferred block size, are as the following. The mean values of the red (R'), green (G') and blue (B') components belonging to the block being processed constitutes the first three elements of the feature vector. The luminance values computed on the block by using (4) are used for computing the entropy value belonging to the block.

$$Y = 0.2126R' + 0.7152G' + 0.0722B' \tag{4}$$

The expression used for computing the entropy is given in (5). Here, p_k value represents the probability of each luminance value to exist in that block.

$$-\sum\nolimits_k p_k \log_2 p_k \tag{5}$$

By using the luminance values computed in the previous step, circular projection is implemented. The radius values used during the projection are between 1 and $B/2$, and the expression used for constructing the vector is given in (2).

The first three elements of the feature vector contain the color information belonging to the block and they represent the color features mentioned in the study by Luo et. al. [10]. While the fourth element gives information about the complexity belonging to the block, the remaining $B/2$ elements are the results of the circular projection. The reason in determining the maximum radius as $B/2$ is that the biggest circle which can be inserted into a block with size $B \times B$ has radius of $B/2$. In this way, the feature vectors from all of the blocks are acquired and inserted into a matrix. Then the matrix, with size of $\left((N - B + 1) \cdot (M - B + 1)\right) \cdot (4 + B/2)$, is lexicographically sorted.

3.2. Comparison of the Feature Vectors

In this stage, each feature vector is compared with its neighbors and in case they fulfill some determined conditions, shift vectors are constructed. The threshold values used in the comparisons are τ_c, τ_e, τ_d and τ_{corr} respectively. During the comparison of the feature vectors, firstly, the first four elements of the vectors are considered. In case the required condition is satisfied, the correlation factor between the values of the remaining elements will enable the eventual decision to be made. Let two vectors to be compared be denoted by $\mathbf{V}^i$ and $\mathbf{V}^j$. In case the condition given in (6) is satisfied, the distance between the blocks represented by these vectors will be controlled to see whether it is less than or equal to the threshold value τ_d. In (6), $\mathbf{V}_k^i$ denotes the k^{th} element of the vector represented by i, while $\mathbf{V}_k^j$ denotes the k^{th} element of the vector represented by j.

$$\left(\left|\mathrm{V}_k^i - \mathrm{V}_k^j\right| \le \tau_c\right) for\ (1 \le k \le 3) \wedge \left(\left|\mathrm{V}_4^i - \mathrm{V}_4^j\right| \le \tau_e\right) \quad (6)$$

Let the upper–left corner coordinate of the block which corresponds to the vector denoted by i be (x_i, y_i), and the upper–left corner coordinate of the block which corresponds to the vector denoted by j be (x_j, y_j). In this case, the condition given in (7) must be satisfied.

$$\sqrt{\left(x_i - x_j\right)^2 + \left(y_i - y_j\right)^2} \le \tau_d \quad (7)$$

In case the color, entropy and distance information corresponding to the mentioned two blocks satisfies the necessary conditions, the correlation factor of the projection vectors related to these blocks are computed by using (3). If the result of the calculation is less than or equal to τ_{corr}, the vectors are considered as similar, and the coordinate values and shift vectors related to the blocks represented by these vectors are stored in matrix **C**. The matrix input generated in case the vectors being talked about are considered as similar is given in (8).

$$\mathrm{C}^m = \left[\left|x_i - x_j\right|, \left|y_i - y_j\right|, x_i, y_i, x_j, y_j\right] \quad (8)$$

While the first two elements of the matrix give the shift vector, the remaining ones are the upper–left corner coordinates of the mentioned two blocks, which are considered as similar.

3.3. Marking the Repetitive Regions

By evaluating the number of the shift vectors which exist in the matrix **C** obtained in the previous step of the algorithm, the image regions which are considered as repeating are marked. In order to reduce the time complexity during the process of marking, the matrix is lexicographically sorted before the search operations. After the sort operation, each vector of the matrix is compared with the subsequent ones, thus, the same shift vectors are determined. In case a different shift vector is detected, the algorithm stops the comparisons being made for the shift vector in the hand, and considers the next shift vector. As the result of this step of the algorithm, the region which is supposed to be copied and pasted will be marked.

So far, the details related with the proposed algorithm have been given under subtitles. In the next section, the experimental results acquired are going to be interpreted.

4. Experimental Results

In this part of the study, so as to be able to make a performance analysis of the proposed technique, various experiments are performed. The aims of these experiments are to be able to have an idea about the performance of the proposed technique, and to be able to make required comparisons with the study in [8]. During the comparisons, the authentication rate is denoted by p, and the error rate is denoted by f. Descriptions related with these metrics are given in (9).

$$p = \frac{\left|D_1 \cap R_1\right| + \left|D_2 \cap R_2\right|}{\left|D_1\right| + \left|D_2\right|}, \quad f = \frac{\left|D_1 \cup R_1\right| + \left|D_2 \cup R_2\right|}{\left|D_1\right| + \left|D_2\right|} - p \quad (9)$$

While D_1, D_2 represent the copied and pasted regions which do not overlap, the copied and pasted regions which are determined by the algorithm are represented by R_1, R_2. The symbols $|\ldots|$, $\cap$ and $\cup$ stand for the area represented by the region, intersection operation and union operation, respectively. In the experiments performed, the parameters symbolized by τ_c, τ_e, τ_d and τ_{corr} are determined as 1, 0.3, 32 and 0.99 respectively. The block size is chosen as 32×32, while the threshold value which is given in Chapter 3 and used in comparing the amounts of the shift vectors is chosen as 10.

In the first experiment, the color image given in Fig. 1(a) with size of 166×250 has been used. Fig. 1(b) and Fig. 1(c) show the doctored image obtained after the copy–move forgery and the repeating regions marked by the algorithm, respectively. The authentication rate and the error rate acquired as the result of the experiment are given in the caption of Fig. 1. The condition that the copied and pasted region has an irregular shape while the shapes of the blocks that are used for obtaining the feature vectors are in square form affects the authentication rate directly.

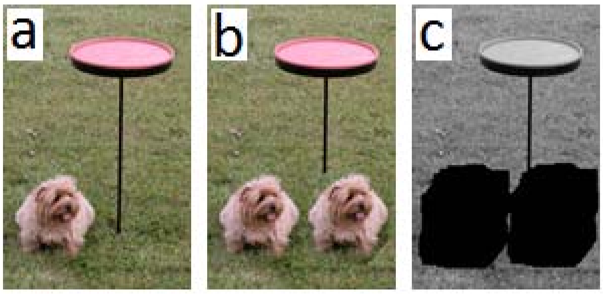

Fig. 1. Test results of the proposed technique for copy–move forgery (a) Test image (b) Doctored image (c) The result image generated by the algorithm (p=1,f=0.12)

In another experiment which is performed in order to observe the robustness of the algorithm against rotation, mirroring and scaling, the color image given in Fig. 2(a) with size of 389×259 is used. The forged regions of the doctored images which are exposed to rotation with degree of 30, scaling with ratio of 1.05 and mirroring respectively (Fig. 2(b), Fig. 2(d), Fig. 2(f)) are determined and shown (Fig. 2(c), Fig. 2(e), Fig. 2(g)). The authentication rates and the error rates acquired as the results of the experiments can be found in the caption of Fig. 2.

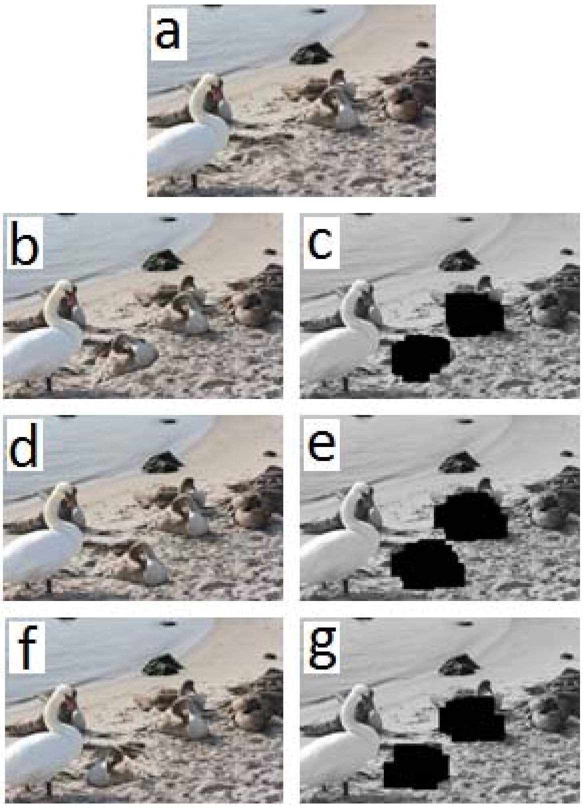

Fig. 2. Test results of the proposed technique in terms of robustness against rotation, scaling and mirroring operations (a) Test image (b) Rotation image with degree of 30 (c) Result image for the rotation image with degree of 30 (p=0.92,f=0.29) (d) Scaling image with ratio of 1.05 (e) Result image for the scaling image with ratio of 1.05 (p=0.88,f=0.25) (f) Mirroring image (g) Result image for the mirroring image (p=0.97,f=0.28)

When both the authentication rates and the visual results are examined, it can be expressed that the technique gives high authentication rates even when scaling, mirroring and rotation transformations are performed.

In order to compare the proposed method with the study in [8] in terms of robustness against rotation, the color image given in Fig. 3(b) with size of 256×256 has been generated specially by forging the original image given in Fig. 3(a). When the authentication rates of both of the methods are examined, it is observed that the proposed technique which uses Circular Projection gives better results than the study in [8]. As stated in Fig. 3(c) and Fig. 3(d), the proposed method gives better results in terms of authentication rate.

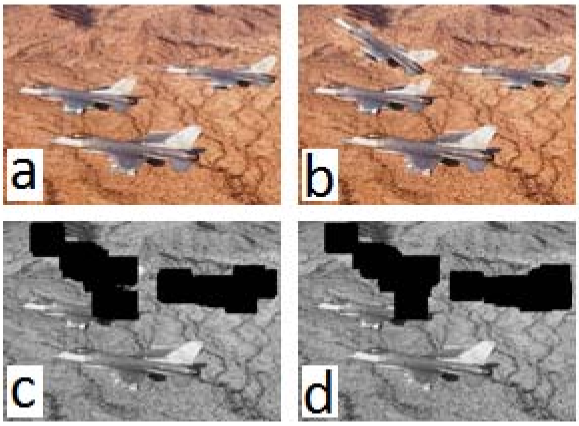

Fig. 3. Comparison results of the proposed technique with the study in [8] in terms of robustness against rotation (a) Test image (b) Forgery image (c) Result image generated by using the technique in [8] (p=0.88,f=0.49) (d) Result image generated by using the proposed technique (p=0.93,f=0.38)

In order to test the robustnesses of the studies against rotation, fake regions with sizes of 100×100 have been created on 20 test images with sizes of 326×245. Mean values belonging to the authentication and error rates of both of the techniques are given in Table 1. As seen in the table, the proposed method gains advantage over the study in [8] in terms of authentication rate, while the rotation angle increases. The condition that the Circular Projection algorithm is used in the process of determining the feature vectors renders the proposed technique more robust against rotation operation. In addition, it has been shown in the results that the proposed technique is also robust against scaling and mirroring operations.

Table 1. Comparison of the proposed technique with the study in [8] for different degrees of rotation in terms of robustness

	5°	15°	30°	45°
[8]	p=0.98 f=0.13	p=0.89 f=0.28	p=0.71 f=0.41	p=0.31 f=1.28
Proposed Technique	p=0.98 f=0.14	p=0.97 f=0.32	p=0.85 f=0.17	p=0.61 f=1.3

5. Conclusions

In recent years, various techniques have been proposed by the researchers for detection of copy–move forgery. Especially, the probability that the copied region is exposed to rotation before being pasted has increased the need for the techniques which are robust against rotation. The study in [8] uses log–polar transformation in order to obtain rotational invariance. However, it is observed that the authentication rate of the mentioned technique decreases while the rotation angle increases. In this study, the Circular Projection algorithm, which is a rotation invariant feature extraction technique, has been used for determining the feature vectors. In addition, means of the red, green and blue components' values, which are proposed by Luo et. al. have been adapted to the algorithm in order to increase the success rate of the technique [10]. As can be observed from the experimental results, when compared with the technique in [8], the proposed algorithm gives higher authentication rates. Especially, while the rotation angle increases, the authentication rates of the proposed method become higher than the ones generated by the study in [8]. In addition, it is observed that the proposed methodology is robust against scaling and mirroring operations. For the future work, it is being planned to examine the contribution of the Radial Projection method in the frequency domain.

6. References

[1] Fridrich, J., "Detection of copy-move forgery in digital images", *Digital Forensic Research Workshop*, Cleveland, OH, 2003, pp. 19–23.

[2] Popescu, A. C., Farid, H., "Exposing digital forgeries by detecting duplicated image regions", *Tech. Rep. TR2004-515*, Dartmouth College, 2004.

[3] Mahdian, B., Saic, S., "Detection of copy move forgery using a method based on blur moment invariants", *Forensic Science International*, vol. 171, pp. 180-189, 2007.

[4] Huang, Y., Lu, W., Sun, W., Long, D., "Improved DCT-based detection of copy-move forgery in images", *Forensic Science International*, vol. 206(1-3), pp. 178-184, 2011.

[5] Cao, Y., Gao, T., Fan, L., Yang, Q., "A robust detection algorithm for copy move forgery in digital images", *Forensic Science International*, vol. 214, pp. 33-43, 2012.

[6] Myrna, A. N., Venkateshmurthy, M. G., Patil, C. G., "Detection of region duplication forgery in digital images using wavelets and log-polar mapping", *Conference on Computational Intelligence and Multimedia Applications*, Sivakasi, Tamil Nadu, vol. 3, 2007, pp. 371-377.

[7] Bayram, S, Sencar, H., Memon, N., "An efficient and robust method for detecting copy-move forgery", *IEEE International Conference on Acoustics, Speech and Signal Processing*, Taipei, 2009, pp. 1053- 1056.

[8] Bravo-Solorio, S., Nandi, A. K., "Passive forensic method for detecting duplicated regions affected by reflection, rotation and scaling", *European Signal Processing Conference*, Glasgow, Scotland, 2009, pp. 824-828.

[9] Tsai, D. M., Chen, C. H., "Rotation invariant pattern matching using wavelet decomposition", *Pattern Recognition Letters*, vol. 23, pp. 191-201, 2002.

[10] Luo, W., Huang, J., Qiu, G., Weiqi, L., Jiwu, H., Guoping, Q., "Robust detection of region duplication forgery in digital image", *18th International Conference on Pattern Recognition*, Hong Kong, vol. 4, 2006, pp. 746-749.