International Journal for Housing Science and Its Applications
Publish August 4, 2025. Volume 46, Issue 3 Pages 1660-1669

https://doi.org/10.70517/ijhsa463129

Research on image forgery method based on the combination of target detection algorithm and image forgery analysis technology

Wenyue Ma[1,*]
[1] International College, Chongqing University of Posts and Telecommunications, Chongqing, 400065, China
Corresponding authors: (e-mail: 13863262820@163.com).

Abstract The rapid development of information technology, while promoting the wide dissemination of digital images and other multimedia information, has also given rise to a variety of image forgery means. The proliferation of forged images has put forward higher requirements for current image forgery techniques in terms of accuracy and fineness. This paper discusses the mathematical principle of CFAR target detection algorithm from two perspectives: the clutter statistical modeling of CFAR and CFAR detector, which is used as a target detection method for ordinary images. After completing the detection of ordinary images, the object shadow in ordinary images is taken as the entry point to explore the scene information provided by the object shadow. Based on the principle of planar homology, the co-point line constraint and intersection ratio consistency constraint methods are proposed to detect the image forgery region using the geometric features of the shadow. On the basis of the obtained image forgery regions, the image forgery model is constructed by integrating the traditional forgery methods such as ELA analysis method, spatial color method and CNN network algorithm. The designed forgery algorithm shows optimal performance in the forgery experiment of high-fake passports, and the leakage rate is as low as 0.288, which provides an effective technical reference for the identification of image forgery.

Index Terms image forgery, CFAR target detection algorithm, image forgery analysis, planar homology

I. Introduction

With the introduction of new software for cell phones and tablet computers, image tampering can be accomplished not only on professional systems and equipment, but also by every ordinary person through a variety of “beauty software” to modify photos [1], [2]. Although positive image tampering can make the photo more perfect, more pleasing to the eye, but there is no lack of many unscrupulous people using various means of forging pictures to fake the real, the Internet spreads fast, not only may have a huge impact on the reputation and interests of the individual, but also is not conducive to the stability and unity of the community, and may even have a huge impact on national security [3]-[6]. Therefore, to do a good job of digital image forensics, to maintain social order, maintaining national corporate security and so on is an initiative to promote the benefits and eliminate the disadvantages [7], [8].

Image tampering techniques can be categorized into traditional methods and deep learning methods. The traditional method is to analyze the extracted image natural features and man-made features to determine whether the image has been tampered with or not, and this method has limited expressive ability and cannot cope with all the image tampering techniques, and most of them can only be used for one kind of image tampering method [9]-[11]. This approach can be mainly subdivided into three forms of image alignment processing algorithms, including geometric feature-based, feature point-based, and border-based stamp alignment algorithms [12]. Zhong, J. et al. investigated block-based copy-move forgery detection (CMFD) algorithm using auxiliary overlapping circles on digitally forged image data in order to extract the local and internal features of the image and achieve good image geometric distortion discrimination performance [13]. Li, Y. and Zhou, J. designed an identification algorithm for copy-move forgery images with a limited number of keypoints in small or smooth regions by lowering the contrast threshold and scaling the input image in order to generate a sufficient number of keypoints, and at the same time matching the keypoints based on a hierarchical strategy to achieve good image forgery [14]. Uliyan, D. M. et al. examined the detection of fuzzy artifact forged images by segmenting the image into multiple regions of interest using statistical analysis and color texture analysis methods and using fuzziness estimation methods to identify the normal and forged image features and to obtain a high performance of detection of forged fuzzy artifact regions [15].

Deep learning mainly uses convolutional neural network models to automatically extract and combine features, through which classifiers are trained to realize an end-to-end adaptive learning model [16], [17]. The biggest advantage of this end-to-end automatic detection system is that it automatically learns the feature parameters and adapts to multiple modes of recognition [18]. Kuznetsov, A. proposed a splicing detection algorithm based on VGG-16 convolutional neural network to identify digitally forged images, which trains an image classifier using image chunks as input data to identify the original image and spliced image regions with high classification accuracy [19]. Qazi, E. U. H. et al. established a deep learning architecture based on ResNet50v2, combined with the weight calculation method of YOLO convolutional neural network, to realize the accurate original and fake image discrimination function in image stitching detection system [20]. Al_Azrak, F. M. et al. introduced convolutional neural networks to perform chunking and block transform feature extraction tasks and showed that one- and two-dimensional Fourier transforms are effective geometric feature extraction methods for detecting tampered regions of an image, and play an important role in detecting digital watermarked images or tampered images with signatures [21].

Among them, as the target detection method has been widely used in the fields of big data modeling, aerospace science and technology, and smart home, a large number of scholars have shifted their attention to the field of forgery image recognition based on target detection algorithms [22], [23]. As the method can quickly and accurately identify and locate specific targets from massive visual data, and then classify images to improve image detection efficiency, it lays the foundation for more intelligent image forgery scenarios and applications [24]-[26].

For the recognition and identification of multiple categories of forged images in the Internet, this paper takes image detection - forged image detection - forged image identification as the research idea. Firstly, it describes the operation method of CFAR algorithm based on the sliding window processing mechanism, and the structural composition of the detector. Secondly, on the theoretical basis of planar homology principle, it discusses the detection steps of image forgery region using the geometric features of the shadow of ordinary image objects, and puts forward the image forgery detection method based on the constraints of the shadow set. Again combining the traditional image forgery feature method and neural network method, the image forgery model based on the traditional method and deep learning method is constructed. Finally, based on the image detection method and the forgery method designed in this paper, the research and comparison of forgery algorithms for passport images and the comparison of detection correctness are carried out in turn.

II. Common image CFAR target detection

II. A. Overview of the CFAR algorithm

CFAR is characterized by constant false alarm rate and adaptive thresholding, and it is the most widely and deeply researched method for target detection in ordinary images.CFAR performs target detection by comparing the pixels to be detected on an ordinary image with a detection threshold in a sliding-window manner, where this threshold is determined by the statistical properties of the clutter around the pixel to be detected at a given false alarm rate. A schematic of the CFAR sliding window is given in Fig. 1, where the clutter region is for estimating the detection threshold, and the guard region is for preventing the pixel points of the extended target from leaking into the clutter region to affect the clutter model parameter estimation, and the size of the guard region is set according to the target size and image resolution.

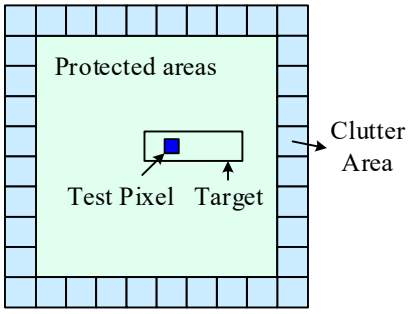

Figure 1: CFAR sliding window signal

The current research on CFAR algorithms is mainly carried out in the following two aspects:

First, research on statistical modeling of clutter in CFAR. In CFAR, the purpose of statistical modeling of ordinary image clutter is to use statistical methods to describe the ordinary image clutter data, so as to further obtain the detection threshold according to the set false alarm rate. For uniform clutter, some simple statistical distribution

models, such as Gaussian distribution, lognormal, Gamma distribution, etc., can usually be used to fit the common image effectively. For non-uniform clutter, simple statistical distribution models are less effective, and more complex statistical distribution models, such as K distribution, generalized Gamma distribution, etc., need to be utilized to fit ordinary images. However, for scenes with multiple types of clutter (e.g., buildings, roads, trees, and grass in urban areas), it is difficult to provide a uniform and effective description of the clutter in the whole scene even by utilizing some complex statistical distribution models.

Second, the CFAR detector is studied. When CFAR performs sliding window on an image, the pixels located in the clutter window are not necessarily homogeneous and may be heterogeneous regions, which makes the CFAR detection results have more false alarms or missed alarms.Rohling categorizes the background clutter faced by common image target detection into three typical cases: uniform clutter background, clutter edges, and multi-targets. Uniform clutter background means that the clutter in the sliding window is uniform and homogeneous. A clutter edge is when the sliding window is at the junction of two or more different clutter types. Multi-target means that when two or more targets are in close proximity to each other, the signals from the other targets leak into the clutter window of the current target to be detected. The Cell Average Constant False Alarm Rate (CA-CFAR) addresses the uniform clutter background case, and Lincoln Laboratory's two-parameter CFAR is a CA-CFAR algorithm.GO-CFAR addresses the clutter edge case.SO-CFAR, OS-CFAR, etc. address the multi-target case.

II. B.CFAR Detector

II. B. 1) 2.2.1 CA-CFAR

The adaptive threshold of CA-CFAR consists of two parts, one is Z_{CA} estimated from the mean value of the pixel points in the whole clutter window, and the other is the threshold scale factor γ. Thus the threshold value can be expressed as equation (1):

$$\begin{aligned} T_{CA} &= \alpha Z_{CA} \\ Z_{CA} &= \hat{\mu}_{CA} = \frac{1}{N}\sum_{i=1}^{N} x_i \\ \gamma &= N\left(P_{fa}^{-\frac{1}{N}} - 1\right) \end{aligned} \tag{1}$$

After obtaining the threshold T_{CA} of CA-CFAR according to Eq. (1), the test pixel point X_{test} is compared with T_{CA}, and the test pixel point is judged to be a target if $X_{test} \geq T_{CA}$, otherwise it is judged to be a clutter.

CA-CFAR is more effective in the case of homogeneous clutter background and only one target exists in the sliding window, however, when there are heterogeneous clutter or multiple targets interfering, the detection performance degrades rapidly.

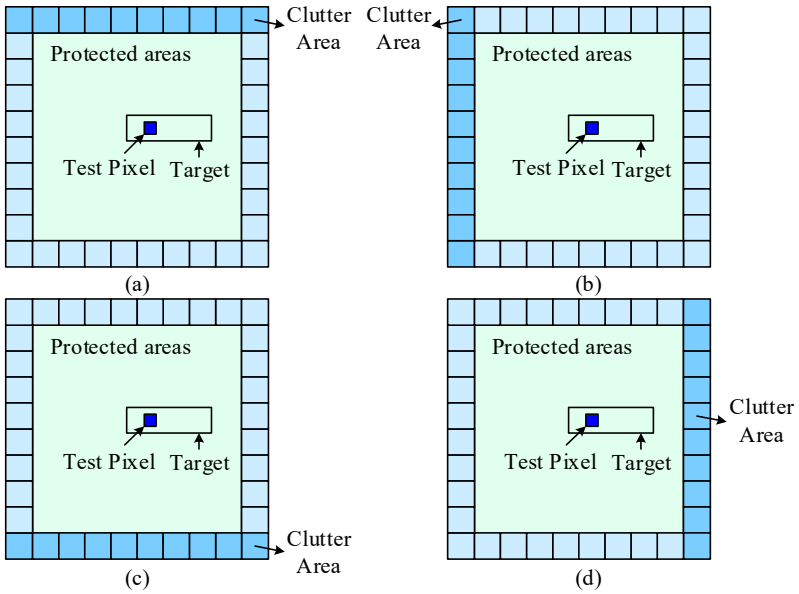

Figure 2: Four strategies for defining front and rear edge Windows

II. B. 2) 2.2.2 SO-CFAR and GO-CFAR

Four strategies for defining leading and trailing edge windows are given in Fig. 2, where Fig. 2(a) shows the upper leading edge window, Fig. 2(b) the left leading edge window, Fig. 2(c) the lower leading edge window, and Fig. 2(d) the right trailing edge window. Here the pixel points labeled in green are the leading edge or trailing edge windows relative to the test pixel points.

It can be seen that compared to the 1D radar data, there are 2 types of leading and trailing edge windows for the 2D normal image, i.e., the leading edge window is categorized into the upper leading edge window and the left leading edge window, and the trailing edge window is categorized into the lower leading edge window and the trailing edge window. Here the pixel points labeled in green are the leading edge windows or trailing edge windows relative to the test pixel points. Assuming that the number of pixel points in each window is N_w, then there is equation (2):

$$mean_{top} = \frac{\sum_{i=1}^{N_w} x_{i,top}}{N_w} \qquad mean_{left} = \frac{\sum_{i=1}^{N_w} x_{i,left}}{N_w}$$
$$mean_{bottom} = \frac{\sum_{i=1}^{N_w} x_{i,bottom}}{N_w} \qquad mean_{right} = \frac{\sum_{i=1}^{N_w} x_{i,right}}{N_w} \tag{2}$$

Here $mean_{top}$, $mean_{left}$, $mean_{bottom}$, and $mean_{right}$ are the mean values of the pixel points in the upper leading edge window, left leading edge window, lower leading edge window, and right trailing edge window, respectively, and $x_{i,top}$, $x_{i,left}$, $x_{i,bottom}$, and $x_{i,right}$ are the i th pixel points in the upper leading edge window, left leading edge window, lower leading edge window, and right trailing edge window, respectively.

GO-CFAR is proposed to solve the clutter edge problem and its threshold is calculated according to equation (3):

$$\begin{aligned} T_{GO} &= \alpha Z_{GO} \\ Z_{GO} &= \hat{\mu}_{GO} \\ &= \max\left\{mean_{top}, mean_{left}, mean_{bottom}, mean_{right}\right\} \end{aligned} \tag{3}$$

III. Image forgery detection methods and image authentication methods

III. A. Image forgery detection method based on shadow geometry constraints

The principle of planar homology is shown in Figure 3.

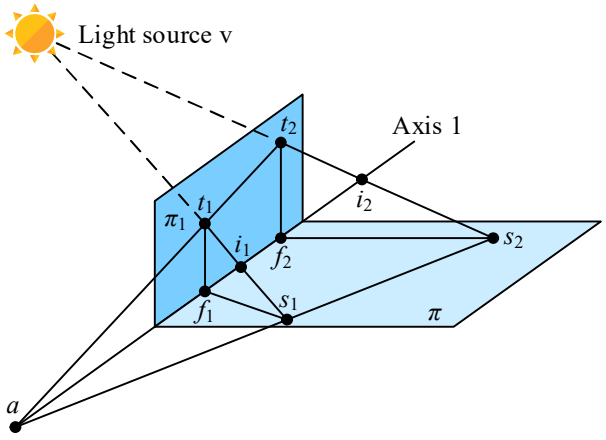

Figure 3: Plane homology principle

As shown in Fig. 3, a planar homology refers to a planar mapping transformation H, which consists of a line with a fixed point (axis 1) and a fixed point (vertex v) not on the axis as in equation (4):

$$H = I + (\mu - 1)\frac{vl^T}{v^T l} \tag{4}$$

where μ denotes the intersection ratio. In this paper, the vertex v is the image of the light source, and axis 1 is the image of the intersection line of the planes π and π_1. Note that in the real 3D world, i_2 does not exist because there is no actual intersection of the two lines, but in the image 2D plane, the intersection exists, and the significance of introducing the intersection here lies in the geometrical constraints mentioned in this paper:

(1) The lines of corresponding points always intersect at one point. By "corresponding" we mean head to head, foot to foot, and point on shadow to point on shadow. Whether point or parallel, the edges of parallel objects in a plane, such as a shadow on the ground, intersect at a common point v on the image plane, where the parallel light source should intersect at the vanishing point on the image plane. Parallel edges can be found everywhere: people walking upright, edges of buildings, edges of interior windows, bottles, glue sticks, and so on. By counting the shadows l_s produced by a large number of parallel edges in an image, the intersection point v of these shadows can be calculated. Shadows that deviate from this intersection point are then likely to be produced by forged objects. The judgment criterion based on light source consistency is defined in this paper as $d = d(v, l_s)$. The shadows l_s are fitted using least squares. Each of the two shadows will define a candidate intersection v_i, and the median of all candidate intersections gives its final estimate.

(2) The intersection ratio μ defined by the light source v, the head t, the feet s, and the intersection point i is consistent across objects. This constraint is utilized to detect synthesis in natural images. Note that t_1, f_1, t_2, f_2 must be coplanar, and f_1, f_2 must be on the line of intersection of the plane π_1 and the plane π. In the real world, vertical objects on the ground all satisfy this assumption. For example, standing people, streetlights, trees and buildings are common. In addition, people like to insert a new person into the target scene who is also usually upright or vertical.

The shadow geometry based image forgery detection techniques in this section include co-pointing line constraints and intersection ratio consistency constraints. For the obtained images or video frames, the shading geometric features are used to detect the forged regions. Specifically, for a pair of objects perpendicular to the ground in the image, find the vertices of the head, the foot, and the shadow of each object, a total of three points, respectively, use the corresponding points to connect the line of co-points and the intersection ratio consistency to determine whether the two objects are from the same photo, if not, then at least one of them is forged, and the comparison between multiple pairs of objects can find out which object is forged. The specific steps are as follows:

(1) Selecting the shadow region

For a given image, find the objects perpendicular to the ground and label the regions where all three points of the head, feet and their shadow vertices are visible as $R_1, \cdots, R_n$ with $n > 1$.

(2) Find the three points needed for each region

For the ith region, manually mark the locations of the three key points: the object's head, the object's feet, and the shadow's vertex, v is the light source, which can be the sun or any other point light source, $t_1 f_1$ and $t_2 f_2$ are the objects perpendicular to the ground, which produce the shadows on the ground $f_1 s_1$ and $f_2 s_2$, at which point it is necessary to label the points $\{t_1, f_1, s_1\}$ and $\{t_2, f_2, s_2\}$.

(3) Determining image forgery with co-pointing line constraints

According to the plane homology constraint, the lines connecting the three keypoints corresponding to two or two objects should intersect at one point, $t_1 t_2$, $f_1 f_2$ and $s_1 s_2$ the three lines must intersect at one point, and the intersection point is noted as a. This constraint can be written as equation (5):

$$\left((t_2 \times t_1) \times (s_2 \times s_1)\right) \cdot \left(f_2 \times f_1\right) = 0 \tag{5}$$

At least one of the regions that do not satisfy this constraint is a forged region, and the comparison between multiple pairs of regions two by two can find out which region belongs to the forged region.

(4) Determining image forgery with intersection ratio constraints

Although the straight lines $f_1 f_2$ and $t_1 s_1$ and $t_2 s_2$ don't intersect in the real world, they can intersect in the image plane and the intersection is meaningful, which is denoted as i. From planar homology, the intersection ratio between two shadow regions $\{v, t_m, s_m, i_m\}$ and $\{v, t_n, s_n, i_n\}$ should be consistent. Cross ratio should be consistent, if a certain object is copied from other pictures, its shadow length, angle and other attributes usually can not be well consistent with the object in the target picture, this thesis utilizes this property for image authenticity identification. This geometric constraint can be expressed as in equation (6):

$$\{v, t_1; s_1, i_1\} = \{v, t_2; s_2, i_2\} \tag{6}$$

This constraint defines the cross ratio but does not specify a specific calculation method; in fact, any reasonable order satisfies this constraint. The calculation method used in this paper is equation (7):

$$CrossRatio(p)=\frac{|vt_p|*|i_ps_p|}{|vi_p|*|t_ps_p|},CrossRatio(q)=\frac{|vt_q|*|i_qs_q|}{|vi_q|*|t_qs_q|} \tag{7}$$

$CrossRatio(p)$, $CrossRatio(q)$ are the intersection ratios of the p th and q th regions when the p th and q th regions are paired, respectively, and $|AB|$ is the distance between the two points of A, B. The distance between the two points. It should be noted that for the same region, the change of its pairing region affects the value of its intersection ratio, because the change of pairing affects the change of intersection points, which in turn leads to the change of intersection ratio.

An image that does not satisfy either of the intersecting line constraints in step (3) and the intersection ratio constraints in step (4) can be judged to be a forged image, and the forged region can be given by using the method on a different pair of objects.

III. B. Image Forensics Based on Traditional and Deep Learning Methods

Traditional image tampering forensics usually has the ability to discriminate a single tampering technique, and deep learning can adaptively extract tampering features, but such adaptive features are weakly controllable and may contain feature information unrelated to the tampering features, which leads to an increase in computation and even affects the accuracy rate. Therefore, in this paper, ELA, CMYK, Laplacian and GLCM are fused with deep learning methods, and the images processed by traditional methods are input into the built CNN network for model training.

Commonly used feature fusion methods are: splicing concatenate and add, this paper uses add for feature fusion, this fusion of the image dimension is unchanged, the feature information under each dimension is increasing, to avoid the increase in the number of parameters, and then avoid the model amplitude is larger resulting in the training difficulty, not only to retain a variety of features and can be adjusted to the alpha weight to assign the features accounted for For example, equation (8):

$$image=img_1\times(1-alpha)+img_2\times alpha \tag{8}$$

In this paper, after many experiments, it is found that the fusion of Laplacian and GLCM isometric fusion with the ELA error level value under CMYK color channel with alpha set to 0.2 effect, and then fused with the ELA error level value under RGB color channel isometric fusion is the best effect. Thus fusion of ELA on the basis of GLCM, CMYK, Laplacian, i.e., adding the underlying features of the image (color, contour, texture) on the basis of ELA for better tamper recognition.

Let the length be x pixels and the width be y pixels, then the final feature of a location (x,y) is equation (9):

$$\begin{aligned}F(x,y)=F_{RGB\_ELA}(x,y)+\{0.8\times F_{CMYK\_ELA}(x,y)+0.2\\ \times[F_{Laplacian}(x,y)+F_{GLCM}(x,y)]\}\end{aligned} \tag{9}$$

The Feature_map obtained after completing this series of operations is fed into the CNN network for training, and the trained model will determine whether the image has been tampered with or not to make the final result of the tampering probability.

IV. Image forgery detection and performance testing of image authentication methods

Since the passport UV security pattern has rich color information and texture information, the fineness of the authentication algorithm is required to be higher. Therefore, based on the deep learning algorithm proposed above, this chapter carries out the research of passport forgery algorithm, and designs the comparison experiment between this paper's algorithm and the commonly used forgery algorithm for passport forgery. Then the performance analysis of this paper's algorithm under different strategy combinations is carried out. Under the best combination of strategies, the correctness of image detection is compared between this paper's algorithm and commonly used forgery algorithms.

IV. A. Passport authentication methods

IV. A. 1) Research on passport forgery algorithms

The gray-scale map of the real passport UV spectral image is processed to obtain the basic CNN map, and the corresponding CNN data frequency is shown in Fig. 4.

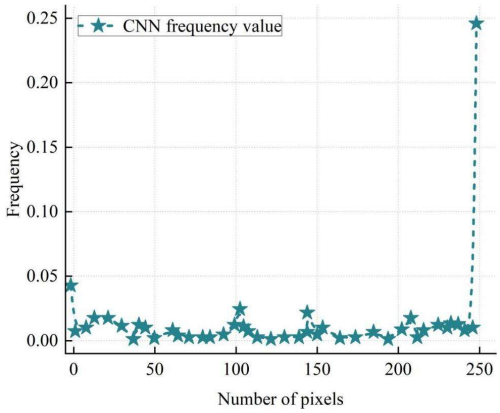

Figure 4: LBP frequency distribution

The length of the feature vector extracted by the basic CNN algorithm is 256 dimensions, and the computational efficiency will be reduced due to the high dimensionality in the subsequent chunking of the passport image to compute the texture features. The basic CNN algorithm for dimensionality reduction is mainly divided into two ways, namely, rotational invariant CNN and improved CNN, due to the multispectral image acquisition equipment passport insertion port width is almost the same as the width of the passport, so there is no directional rotation of the collected passport UV spectral images, the use of rotationally invariant CNN mode will reduce the accuracy of the forensic counterfeiting, so this paper adopts the improved CNN algorithm Instead of the basic CNN algorithm, the extracted feature vectors are dimensionality reduced. The specific calculation formula is shown in equation (10):

$$U(CNN_{P,R}) = \left|S(g_p - g_c) - S(g_0 - g_c)\right| + \sum_{p=1}^{P-1}\left|S(g_p - g_c) - S(g_{p-1} - g_c)\right| \tag{10}$$

The algorithm connects the first and last of the binary numbers generated during the computation of the CNN atlas, and treats the CNN pattern values with less than or equal to two jumps from 0 to 1 or 1 to 0 in the corresponding cyclic binary numbers as an equivalent pattern class, and the ones with more than two jumps are categorized as other classes. In this way the 256-dimensional feature vector generated by the base CNN algorithm is downscaled to 59 dimensions. The final extracted improved CNN frequency statistics are shown in Fig. 5.

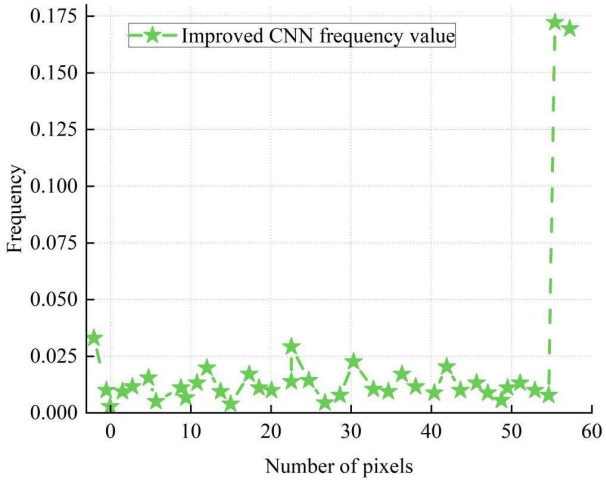

Figure 5: Improved CNN frequency distribution

IV. A. 2) Comparison Experiments of the Authentication Algorithms

Selected similar forgery algorithms (W1) SIFT matching, (W2) HOG + Euclidean distance, (W3) color histogram + Euclidean distance, (W4) GLCM + Euclidean distance, (W5) LBP + Euclidean distance, (W6) CFOG + Euclidean distance, unfolding and (W7) this paper's algorithms based on the traditional characteristics of the passport forgery experiments, the false positive rate and the leakage rate of the simple passport (SP), and leakage rate (HP)

comparison results in high protection photos are shown in Figure 6. The comparison results of the leakage recognition rate (HP) on the high protection photo are shown in Fig. 6, in which (W7) this paper's algorithm in the false recognition rate and leakage recognition rate of the simple forged passport is the lowest among the seven algorithms, respectively 0.037, 0.289. The leakage recognition rate of the high imitation passport is also the lowest among the seven algorithms, only 0.288. However, the average time consumed by the seven algorithms is the longest, 65ms.

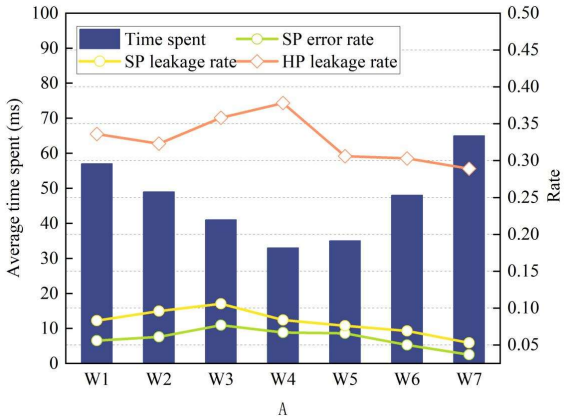

Figure 6: Comparison result of passport authentication algorithm

IV. B. Performance analysis

From the analysis in the previous section, it can be seen that although the image forgery algorithm designed in this paper can effectively carry out the forgery of different categories of forged passports, there is still room for improvement in the average time consumed. Under the same parameter settings, the comparison results of (C1) without any improvement, (C2) only 1000 unforged image samples (represented by only introducing unforged samples in Table 1), and (C3) introducing both unforged image samples and optimizing the deep learning algorithm (using the introduced samples to optimize self-learning in Table 1) are shown in Table 1. The results show that both the introduction of forgery-free image samples and the optimization of the deep learning algorithm can improve the detection performance of the network, in which the strategy of introducing both forgery-free image samples and optimizing the deep learning algorithm has the best overall performance, with an accuracy of up to 20.52% for the target image and a recall rate of only 8.76%.

Table 1: Performance analysis

Strategy profile		C1	C2	C3
Number of samples		15000	15000	15000
Accuracy (%)	Original	90.11	90.11	90.22
	Source	23.58	21.4	28.79
	Target	14.64	17.65	20.52
Recall rate (%)	Original	97.68	98.8	95.78
	Source	11.93	13.85	13.65
	Target	10.31	12.69	8.76
F1-score	Original	0.939	0.947	0.941
	Source	0.178	0.177	0.213
	Target	0.118	0.167	0.141

Different numbers or proportions of forgery-free image samples can have an impact on the detection performance of the network. In this paper, we experimentally compare the effects of not introducing, introducing 100 pairs, introducing 1,000 pairs, and introducing 10,000 pairs of forgery-free image samples in the training procedure on the detection accuracy, and the detection results on 15,000 test samples of the USCISI-CMFD dataset are shown in Table 2. The results show that the number of forged-free samples added during training is not the more the better, and the order of magnitude is roughly around 1,000 (the ratio of the number of samples to the forged images is 1:80) can achieve better comprehensive performance, with an accuracy of 99.35% for the target image and a recall of 0.843%.

Table 2: Effect of introducing different numbers of copy-move-free samples

The number of samples of unforged images is introduced		0	100	1000	10000	15000
Quantity ratio (no forgery: forgery)		90.22	90.74	91.32	90.37	90.22
Accuracy (%)	Original	28.79	29.83	31.74	13.94	28.79
	Source	17.65	21.92	30.53	14.3	17.65
	Target	97.78	97.1	99.35	97.09	97.78
Recall rate (%)	Original	13.67	19.72	11.22	21.94	13.67
	Source	10.31	12.34	20.74	10.94	10.31
	Target	0.941	0.94	0.843	0.949	0.941
F1-score	Original	0.213	0.249	0.263	0.127	0.213
	Source	0.141	0.172	0.257	0.127	0.141
	Target	90.22	90.74	91.32	90.37	90.22

IV. C. Comparison of detection correctness

Using (W8) image forgery detection method based on shadow geometry constraints with commonly used image forgery detection methods (W9) FAST algorithm, (W10) SIFT algorithm, (W11) SURF algorithm to complete the forgery detection of tampered images with different rotational angles, the average correct detection rate is taken as the quantitative results are shown in Fig. 7. With the increment of the rotation angle of the image, the correct rate of all the methods shows a decreasing trend. However, the (W8) image forgery method based on shadow geometry constraints designed in this paper maintains a much higher average correct detection rate than similar algorithms at different angles, with an average correct detection rate as high as 0.948 for the unrotated graph.

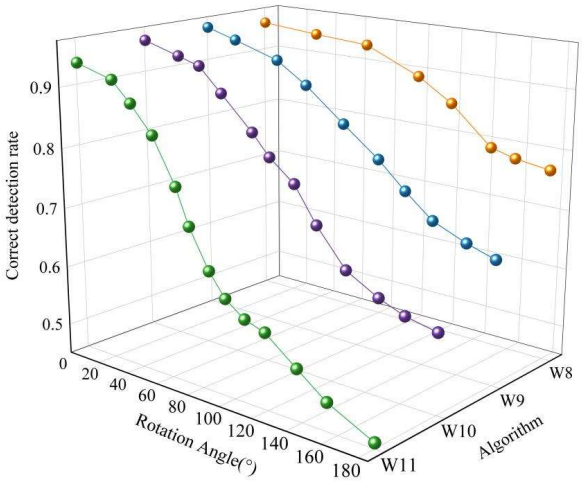

Figure 7: Different rotation angles tamper with image detection accuracy

V. Conclusion

In this paper, based on CFAR target detection algorithm, we design a detection method for ordinary images. On this basis, an image forgery detection method based on shadow geometry constraints is proposed, and an image forgery identification method is constructed by combining traditional methods with deep learning methods. The proposed image detection method can accurately search and detect image targets, and assist the image forgery identification method to efficiently identify forged images.

In passport image identification, the improved image forgery identification method has a misidentification rate of only 0.037 and a leakage rate of only 0.288, and in rotated image detection, the average correct detection rate can reach up to 0.948.

References

[1] Zheng, L., Zhang, Y., & Thing, V. L. (2019). A survey on image tampering and its detection in real-world photos. Journal of Visual Communication and Image Representation, 58, 380-399.

[2] da Costa, K. A., Papa, J. P., Passos, L. A., Colombo, D., Del Ser, J., Muhammad, K., & de Albuquerque, V. H. C. (2020). A critical literature survey and prospects on tampering and anomaly detection in image data. Applied Soft Computing, 97, 106727.

[3] Lin, X., Wang, S., Deng, J., Fu, Y., Bai, X., Chen, X., ... & Tang, W. (2023). Image manipulation detection by multiple tampering traces and edge artifact enhancement. Pattern Recognition, 133, 109026.
[4] Li, H., Luo, W., Qiu, X., & Huang, J. (2017). Image forgery localization via integrating tampering possibility maps. IEEE Transactions on Information Forensics and Security, 12(5), 1240-1252.
[5] Vega, E. A. A., Fernández, E. G., Orozco, A. L. S., & Villalba, L. J. G. (2020). Image tampering detection by estimating interpolation patterns. Future Generation Computer Systems, 107, 229-237.
[6] Dong, L., Liang, W., & Wang, R. (2024). Robust text image tampering localization via forgery traces enhancement and multiscale attention. IEEE Transactions on Consumer Electronics.
[7] Tyagi, S., & Yadav, D. (2023). A detailed analysis of image and video forgery detection techniques. The Visual Computer, 39(3), 813-833.
[8] Singh, S., & Kumar, R. (2024). Image forgery detection: comprehensive review of digital forensics approaches. Journal of Computational Social Science, 7(1), 877-915.
[9] Saber, A. H., Khan, M. A., & Mejbel, B. G. (2020). A survey on image forgery detection using different forensic approaches. Advances in Science, Technology and Engineering Systems Journal, 5(3), 361-370.
[10] Kumar, B. S., Karthi, S., Karthika, K., & Cristin, R. (2018). A systematic study of image forgery detection. Journal of computational and theoretical Nanoscience, 15(8), 2560-2564.
[11] Zhang, Z., Wang, C., & Zhou, X. (2018). A survey on passive image copy-move forgery detection. Journal of Information Processing Systems, 14(1), 6-31.
[12] Deb, P., Deb, S., Das, A., & Kar, N. (2024). Image Forgery Detection Techniques: Latest Trends And Key Challenges. IEEE Access.
[13] Zhong, J., Gan, Y., Young, J., Huang, L., & Lin, P. (2017). A new block-based method for copy move forgery detection under image geometric transforms. Multimedia Tools and Applications, 76, 14887-14903.
[14] Li, Y., & Zhou, J. (2018). Fast and effective image copy-move forgery detection via hierarchical feature point matching. IEEE Transactions on Information Forensics and Security, 14(5), 1307-1322.
[15] Uliyan, D. M., Jalab, H. A., Wahab, A. W. A., Shivakumara, P., & Sadeghi, S. (2016). A novel forged blurred region detection system for image forensic applications. Expert Systems with Applications, 64, 1-10.
[16] Ali, S. S., Ganapathi, I. I., Vu, N. S., Ali, S. D., Saxena, N., & Werghi, N. (2022). Image forgery detection using deep learning by recompressing images. Electronics, 11(3), 403.
[17] Zanardelli, M., Guerrini, F., Leonardi, R., & Adami, N. (2023). Image forgery detection: a survey of recent deep-learning approaches. Multimedia Tools and Applications, 82(12), 17521-17566.
[18] Mehrjardi, F. Z., Latif, A. M., Zarchi, M. S., & Sheikhpour, R. (2023). A survey on deep learning-based image forgery detection. Pattern Recognition, 144, 109778.
[19] Kuznetsov, A. (2019, November). Digital image forgery detection using deep learning approach. In Journal of Physics: Conference Series (Vol. 1368, No. 3, p. 032028). IOP Publishing.
[20] Qazi, E. U. H., Zia, T., & Almorjan, A. (2022). Deep learning-based digital image forgery detection system. Applied Sciences, 12(6), 2851.
[21] Al_Azrak, F. M., Sedik, A., Dessowky, M. I., El Banby, G. M., Khalaf, A. A., Elkorany, A. S., & Abd. El-Samie, F. E. (2020). An efficient method for image forgery detection based on trigonometric transforms and deep learning. Multimedia Tools and Applications, 79, 18221-18243.
[22] Elaskily, M. A., Elnemr, H. A., Dessouky, M. M., & Faragallah, O. S. (2019). Two stages object recognition based copy-move forgery detection algorithm. Multimedia Tools and Applications, 78, 15353-15373.
[23] Yao, Y., Shi, Y., Weng, S., & Guan, B. (2017). Deep learning for detection of object-based forgery in advanced video. Symmetry, 10(1), 3.
[24] alZahir, S., & Hammad, R. (2020). Image forgery detection using image similarity. Multimedia Tools and Applications, 79(39), 28643-28659.
[25] Aloraini, M., Sharifzadeh, M., & Schonfeld, D. (2020). Sequential and patch analyses for object removal video forgery detection and localization. IEEE Transactions on Circuits and Systems for Video Technology, 31(3), 917-930.
[26] Raskar, P. S., & Shah, S. K. (2021). Real time object-based video forgery detection using YOLO (V2). Forensic Science International, 327, 110979.