International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Analysis of Intentional Noise Insertion Approach on the Copy-Move Forgery Detection in Digital Image

Serkan OZBAY[1*]

Submitted: 20/10/2021 Accepted : 26/11/2021

Abstract: In this digital age, there has been ever-increasing trend on the amount of digital image data. On the other side, in parallel with this situation, image tampering and manipulation attacks have become widespread by the use of various image editing software packages. It means that digital image data have become more vulnerable to tampering or manipulation through forgeries. Copy-move duplication is a type of image forgery involving the process of copying and then pasting an image part from one region to another location within the same image. This paper proposes a novel enhancement on the copy-move forgery detection algorithms. The proposed strategy is based on adding specific noise on the image in order to reach more robust detection. It is observed from the experimental results that, with the specific noise insertion, the copy-move forgery detection algorithms can obtain better performances in comparison to conventional methods. It is found at image level that, by the proposed strategy, with 25×25 blocks, 94.16% accuracy rate is reached. The proposed approach also provides to have reasonable precision and recall values, 92.51% and 96.11%, respectively when compared to existing algorithms.

Keywords: *Copy-move duplication, forgery detection, image tampering, noise insertion*

1. Introduction

With the wide availability of low-price electronic devices capable of generating, sharing, or manipulating digital data including digital images and videos, the digital technology is inherently the part of our lives.

As part of today’s digital medium, digital images are valuable sources providing huge amount of information about the environment we monitor. According to estimates, more than one trillion images are taken annually in recent years and it is expected to increase in the upcoming years. Digital images have been widely used in many areas including surveillance for security purposes, medical imaging for the diagnoses of diseases, forensics for investigations of crimes, media for mass communication (especially via Internet), etc.

Beside the benefits of the developments on digital image technology, powerful image editing tools have been created as well. With the presence of various image editing software packages, digital images could be manipulated or tampered in an easy manner. Hence image analyses involving authentication and verification processes have played critical role in some areas. For instance, images are being used as legal evidence in digital forensics investigations, and thus it is vital to determine the originality or forgery of the images.

By the sophisticated and competitive image editing technologies, digital image data have become vulnerable to attacks through forgeries and the forgeries are generally difficult to detect by the naked eye. Image forgery detection algorithms aim to investigate the integrity and authenticity of the images and also to identify the manipulations on the images if exist.

The strategies on detecting the forgery or verifying the originality in digital images are mainly classified as: active approaches and passive approaches. On active approaches, the main process is the verification of additional information such as digital cryptographic signature or digital watermark embedded in digital image. In order to authenticate the image, the active methods generally require priori information to analyze the image under investigation and also some active methods need special hardware in verification purposes. It is clear that those requirements limit the active approaches utilization in the wide range. To cope with the restricted use of active approaches, passive algorithms not requiring either a priori information about the image or special equipments have been introduced [1,2].

There are several forgeries including copy-move, resampling (resize, stretch, rotate), and splicing [3] made on digital images. It is known that one of the most common types among image forgeries is to clone an image part in the scene. This attack is commonly called copy-move (or copy-paste) because an image part is copied and pasted from one location to another within the same image.

Although a huge number of detection techniques on copy-move forgery have been proposed in literature, copy-move forgery detection is still considered to be one of the most actively investigated and challenging topics. This paper addresses a novel enhancement approach on the copy-move forgery detection. The contribution on the proposed algorithm is on the pre-processing level. Intentional noise insertion is the key point such that noise proportional to the blocks for which the image is divided and compatible with the feature vectors used is added. It is thought that the proposed enhancement can be applied for many existing

[1] *Department of Electrical & Electronics Engineering, Gaziantep University, Gaziantep- 27000, TURKEY*
ORCID ID : 0000-0001-5973-8243
** Corresponding Author Email:sozbay@gantep.edu.tr*

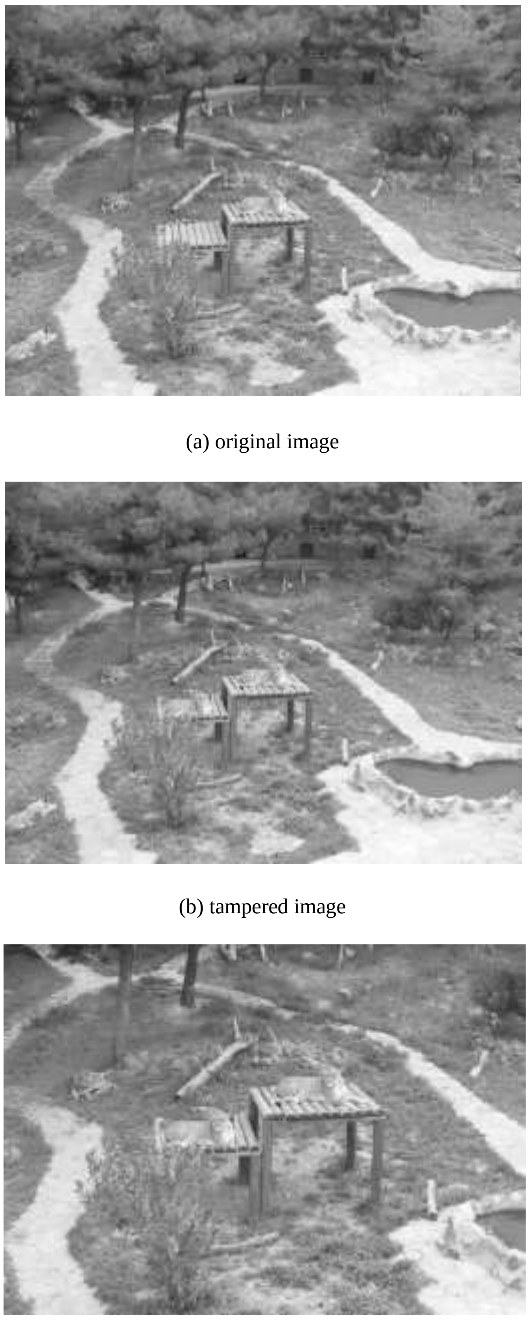
approaches.

This paper is organized as follows. In Section 2, existing copy-move forgery detection techniques have been discussed. Proposed enhancement procedure and the techniques used in the main part of the detection algorithm have been described in Section 3. Performance analysis including performance metric has been provided in Section 4 and finally the paper is concluded in Section 5. Last section also summarizes the future works showing the potential of the proposed enhancement.

2. Copy-Move Forgery Detection Techniques

On passive image forgery detection area, the algorithms can be broadly divided into five categories as [3]: pixel-based, format-based, camera-based, physics-based, and geometric-based. In pixel-based detection algorithms, the focus is on the pixels and particularly on their intensity values statistics, similarities or anomalies. It is previously stated that one of the most common image manipulations is to embed a duplicate image segment in a digital image and therefore such a type of tamper is called a copy-move attack. The main purposes for applying copy-move attack on the images are to mask an object or a person in the image, e.g., to wipe out an evidence on an investigation of crime, or to increase the emphasis on a particular object, e.g., a crowd of demonstrators [2]. A copy-move attack is treated as very easy forgery to implement and also very effective. Since an image part from a region is copied and then pasted into another region in the same image, some image properties such as colors, illuminations, shadows and noise are being well-matched between the tampered region and the image. Consequently, the forgery seems undetectable visually. An example of a copy-move type forgery is shown in Figure 1. Forgeries such as signature forgery on counterfeit checks, or photo manipulations are not new situations in the history but they were limited in the past. Nowadays they have become widespread and have been easier with the progress on digital image processing tools. There are large amount of forgery detections approaches that have been proposed by several researchers [3]. Although there are a lot of studies in the literature about copy-paste forgery detection, copy-move algorithms basically consist of the following steps: pre-processing step, feature extraction step, matching step, and visualization step (known also as decision stage) [4]. Pre-processing step is not always prerequisite for detection algorithms but optional and it mostly covers filtering for eliminating noise or color space conversion for reducing the dimension of the image or enhancing some descriptive features [5-7]. Feature extraction part aims to find out useful information capturing the characteristics of interest in the image. Matching step is treated as descriptor measuring the similarities to identify forged image segment. Finally, visualization stage allows to indicate the tampered region in the forged image.

Copy-move forgery detection algorithms are categorized as part of pixel-based methods and the related works are discussed in a good review [8]. The recent developments on copy-move forgery detection area are described in [4]. Copy-move forgery detection approaches generally use either block-based or keypoint-based techniques. The block-based approaches divide an image into either overlapping or nonoverlapping blocks and then the features are extracted from those blocks. The extracted features are compared among the blocks searching the similarities and thus manipulated parts are detected. In contrast to block-based approaches, keypoint-based methods use the entire image features to decide the tampered region. As already stated, in either block-based or keypoint-based methods, the tampered region or regions are determined by computing the similarities between features. Commonly used methods for extracting the features on block-based approaches are discrete cosine transform [9,10], discrete wavelet transform [11,12], local binary pattern [13,14], principal component analysis [15], and singular value decomposition [5,16]. In keypoint-based approaches, the features are mainly extracted by the help of scale invariant feature transform [17,18], speeded up robust features [19,20], and Harris Corner Detector [21].


(a) original image

(b) tampered image

(c) detailed image segment

Fig.1. Sample image for a typical copy-move forgery attack: (a) original image, (b) tampered image, (c) detailed image segment showing copy-move forgery region. Note that the tiger is replicated.

For matching step in block-based approaches, sorting [14,22,23], correlation [24,25], Euclidean distance [26,27] are commonly used ways to compare the features of block regions. In keypoint-based approaches, nearest neighbour [17,20] and clustering [28] are used for matching purposes.

3. Proposed Forgery Detection Procedure

This study focuses on copy-move type forgery attacks and a block-based approach is proposed. It is known that the digital images are divided into either overlapping or non-overlapping blocks.

The proposed scheme uses both overlapping and non-overlapping blocks. It starts with pre-processing stage and then the block features are determined with extraction step. Finally, features are matched and the decision is made according to the match results. The structure is the same as existing copy-move detection methods.

The main contribution and the core of the proposed scheme are on the pre-processing stage. As a first step, to reduce the dimension of the data in the image, the color input image is converted into the monochromatic (or gray scale) image. Then a specific noise is added proportional to the selected blocks and compatible with the feature vectors used. The features extraction step uses correlation, local binary pattern (LBP), and histogram as the features of each block and matching stage uses thresholding to compare correlations and Euclidean distance to compare the blocks' LBP and histogram features. Based on the similarities of the blocks, the forgery regions are detected.

Correlation is a way for determining the degree of probability that a similarity exists between two measured quantities. For monochromatic digital images, the correlation between two image parts X and Y can be determined by the coefficient given by the following relation.

$$r = \frac{\sum_m \sum_n (X_{mn} - \overline{X})(Y_{mn} - \overline{Y})}{\sqrt{(\sum_m \sum_n (X_{mn} - \overline{X})^2 (\sum_m \sum_n (Y_{mn} - \overline{Y})^2)}} \tag{1}$$

where $\overline{X}$ and $\overline{Y}$ are mean intensity values of X and Y images, respectively and X_{mn} and Y_{mn} are the pixel intensities. Correlation coefficient can take on values in between +1 and -1. If the absolute value of correlation coefficient is greater (closer to 1), it means the image parts are similar. A correlation of zero or close to zero indicates no similarity between image sections.

Local binary pattern (LBP) is another effective way of estimating the similarities of digital images. LBP makes thresholding operation on the neighbouring pixels based on center pixel intensity value. In a neighbourhood, a center pixel is chosen and then its intensity is compared with its neighbour pixels. If the intensity value of the center pixel is greater than or equal to its neighboring pixel, then the neighbour pixel intensity value is assigned to 1; otherwise, it is assigned to 0. After repeating this procedure with all the neighboring pixels, a binary number that is obtained by concatenating all these binary digits is generated for each pixel.

A histogram represents the frequency of the data occurrence in a specific dataset. In a digital image data, histogram is a graphical representation of the number of pixels in the image as the function of their intensities. In other words, the image histogram is computed by processing all pixels in the image by counting the pixels having same intensity value and ordering the total count in an order for each pixel intensity. The proposed copy-move forgery detection procedure is summarized in Table 1.

Table 1. Algorithm framework

Algorithm framework steps
Given a suspicious color image to be investigated with a size of M × N:
1. Convert the color image into monochromatic (gray scale) image to reduce the dimension and the size of the input data.
2. Set the gray scale image size to fixed value.
3. Add the intentional noise on the image.
4. Divide the image into the fixed-size blocks. The blocks are in both overlapping and nonoverlapping format with each other.
5. Obtain descriptive features from each block. Correlation, local binary pattern, and histogram are used as features.
6. Match the feature vectors of the blocks to determine the similarities. Thresholding is used to compare the correlation features and Euclidean distance is used for local binary pattern and histogram.
7. The output is the locations of tampered (copy-move forgery) regions.

The proedure described on the framework seems conventional except adding an intentional noise on the image before feature extraction step. The novelty of this study is in the pre-processing stage by noise insertion on the image. After transforming the color image format into gray scale, the image size is set to 500×500 which is a fixed value on the algorithm. A square-shaped blocks are selected to detect the forgeries in an image region and specifically they are either set to 25×25 or 50×50 value. The selected size is important in noise insertion part.

In order to increase the robustness of the detection algorithm, specifically adjusted noise which is compatible to searched area size and its corresponding features properties is added onto the image pixels' intensity values. For example, if the sizes of the blocks are adjusted to 50×50, the characteristic of the inserted noise is determined and arranged by 50×50 size.

In this study, a specific noise compatible to correlation is added to the image. With the 50×50 blocks, the image is divided into vertical strips where the width of each strip is 50 pixels. In each strip, an offset (specific noise) is added to some parts. In the proposed algorithm, from left to right in a strip, an offset value "20" is added onto the pixel intensities from 1st to 17th pixels and an offset value "-20" is added onto the pixel intensities from 34th to 50th pixels. The pixel intensities between 18th and 33rd pixels are not changed. An example of noise added image and an output are shown in Figure 2 and Figure 3, respectively. Since the correlation is selected as the focus to specify the characteristics of the noise, noise is chosen such specific form that correlation behaves more sharply in identifying the similarities.

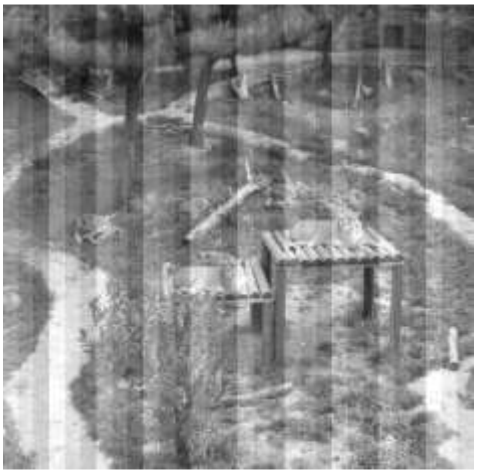


Fig. 2. Noise added image example

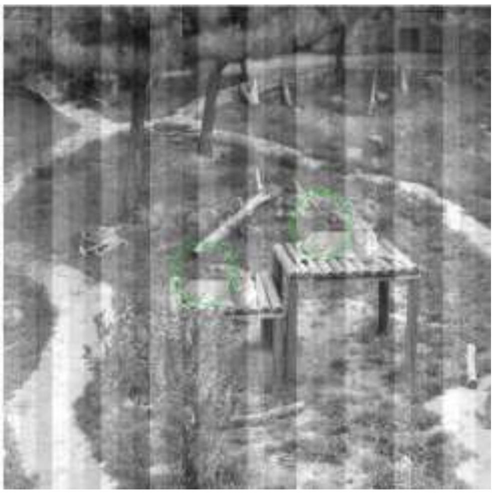


Fig. 3. Proposed algorithm output example

In Equation 1, correlation coefficient is the function of the difference between individual pixel intensities and mean intensity values of the whole pixels in the blocks. Therefore, the noise is inserted into the image in that given format in order for maintaining the existing mean values.

While keeping the mean intensity values on the blocks as constant, added noise affects the performance of the correlation function positively as a precise descriptive feature element in the feature vector.

If we compare with no noise insertion case; although each correlation coefficient is affected by the noise insertion, the larger elements are affected in such a way that the higher correlation coefficient corresponding to true match with the forged region increases but higher correlation coefficient corresponding false match with the forged region reduces.

This is the most important point of this approach. This is increasing the robustness of the detection algorithm with higher precision and recall rates.

On the other hand, all the lower correlation coefficients generally increase with noise insertion. This effect may seem disadvantageous but it is eliminated by thresholding in the matching stage.

4. Performance Analysis

4.1. Performance Indexes

A comprehensive performance of copy-move forgery detection algorithms is mostly evaluated at two levels, namely, image level and pixel level. At image level, the concern is whether or not the image has been tampered. On the other hand, at pixel level, the point is to determine how accurately tampered regions can be detected. In this study, image level indexes are used for performance evaluation.

At image level, to assess the performance, accuracy, precision, recall, and F_1 score are generally used. Figure 4 demonstrates the metrics that are utilized to compute the accuracy, precision, recall, and F_1 score.

In the confusion matrix; TP is the number of images that have been correctly labelled as forged, FP determines the number of images that have been erroneously identified as forged, FN indicates the falsely missed forged images, and TN represents the number of images estimated as not forged and that they are actually not forged.

		Actual	
		Positive	Negative
Estimated	Positive	TP	FP
	Negative	FN	TN

Fig. 4. Confusion matrix

$$accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{2}$$

$$precision = \frac{TP}{TP + FP} \tag{3}$$

$$recall = \frac{TP}{TP + FN} \tag{4}$$

$$F_1 = \frac{2 \times recall \times precision}{recall + precision} \tag{5}$$

4.2. Experimental Results

In order to evaluate the performance of the proposed detection system, a series of experiments was conducted. All the experiments were performed using MATLAB R2020b and a computer with Intel Pentium processor at 1.60 GHz and 4 GB of memory. The experimental dataset is the bunch of digital color images where they are in pairs as authentic and copy-move type forged. The images were taken from some public databases [17, 29] and some were created manually. Totally 180 image pairs were used. In the experiments, after converting the color image into monochromatic image, the image size was adjusted to 500×500 in order for satisfying the predetermined parameters on the algorithm. 25×25 and 50×50 sized square-shaped blocks were chosen, respectively, in the analyses. The intentional noise was selected in accordance with the specified blocks. Figure 5 shows some visual examples of results. On the lefts of the image pairs, there are tampered images and on the right there are outputs that show the copy-move forgeries by green circles.

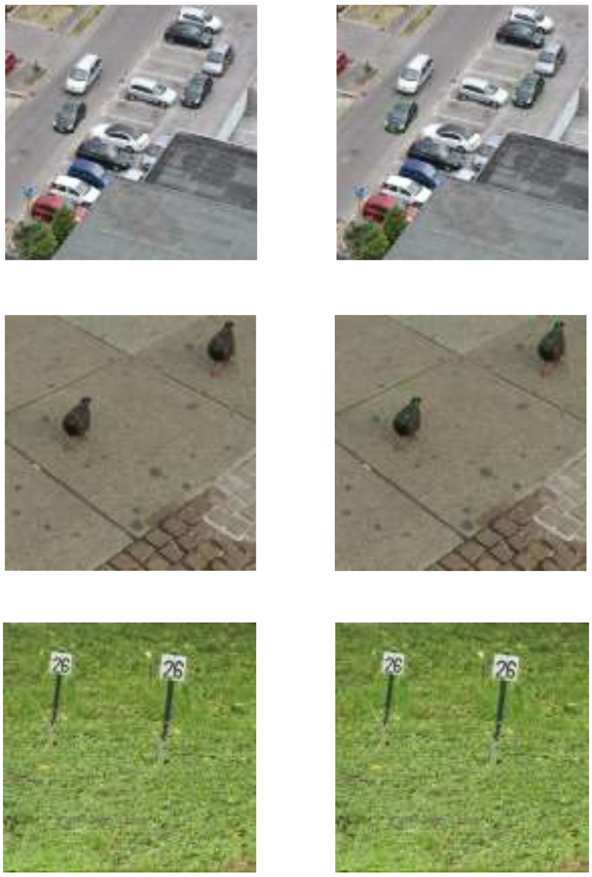


Fig. 5. Proposed algorithm output examples [29]

First, 25×25 blocks were selected, noise insertion in the pre-processing stage was not implemented. Using 180 image pairs, 180 authentic images and 180 forged images with a total of 360, the detection algorithm without enhancement strategy were executed and resulting performance metrics and indexes were obtained. Then the experiments were repeated for 50×50 block sizes. The image level outcome results and performance indexes were listed in the Tables 2 to 4.

Table 2. Image level outcomes of detection for 25×25 block size

	TP	TN	FP	FN
180 authentic images	-	160	20	-
180 forged images	166	-	-	14
Totally 360 images	166	160	20	14

Table 3. Image level outcomes of detection for 50×50 block size

	TP	TN	FP	FN
180 authentic images	-	152	28	-
180 forged images	161	-	-	19
Totally 360 images	161	152	28	19

Table 4. Image level indexes

Block Size	Accuracy	Precision	Recall	F_1
25×25	90.55%	89.24%	92.22%	90.70%
50×50	86.94%	85.18%	89.44%	87.25%

To analyze the performance of the noise insertion strategy, this enhancement was implemented for both 25×25 and 50×50 sizes of blocks. The experimental results were given on the following tables (From Table 5 to 7).

Table 5. Image level outcomes of detection for 25×25 block size (noise inserted)

	TP	TN	FP	FN
180 authentic images	-	166	14	-
180 forged images	173	-	-	7
Totally 360 images	173	166	14	7

Table 6. Image level outcomes of detection for 50×50 block size

(noise inserted)

	TP	TN	FP	FN
180 authentic images	-	155	25	-
180 forged images	166	-	-	14
Totally 360 images	166	155	25	14

Table 7. Image level indexes (noise inserted)

Block Size	Accuracy	Precision	Recall	F_1
25×25	94.16%	92.51%	96.11%	94.27%
50×50	89.16%	86.91%	92.22%	89.48%

Figures 6 and Figure 7 illustrate the comparisons of the performance indexes of the proposed algorithm at image level with noise insertion and without intentional noise for 25×25 and 50×50 blocks sizes, respectively.

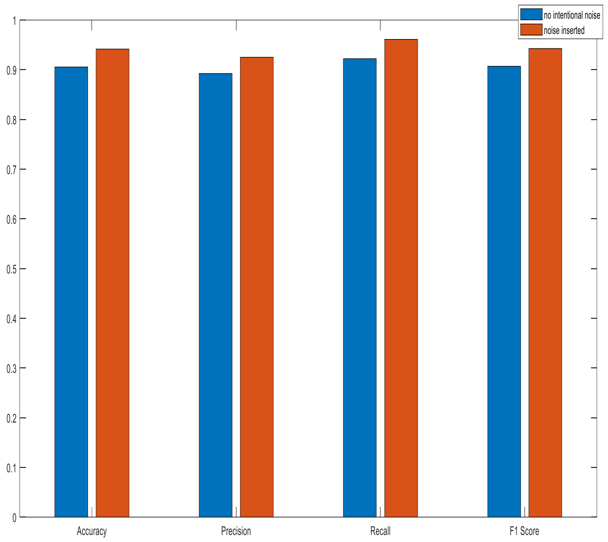


Fig. 6. Comparisons for 25×25 blocks

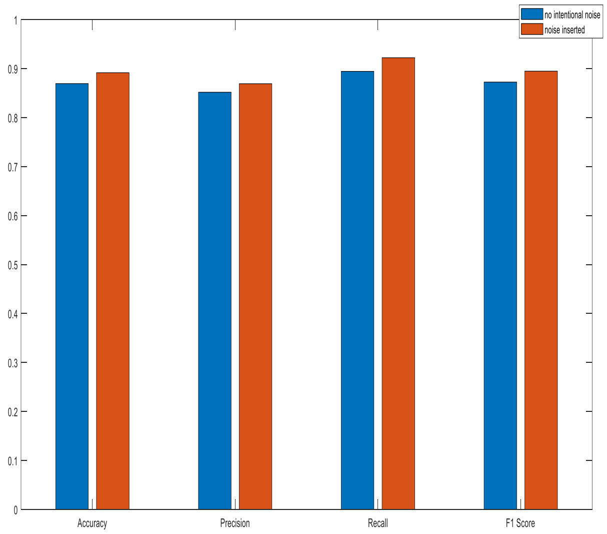


Fig. 7. Comparisons for 50×50 blocks

To verify the performance of the proposed algorithm, the experimental results are compared to [30-34] which is given on the following table.

Table 8. Comparisons to other researches

	Precision	Recall
Proposed detection algorithm (25×25 block size)	92.51%	96.11%
Proposed detection algorithm (50×50 block size)	86.91%	92.22%
Amerini et al. [30]	94.52%	93.57%
Silva et. al. [31]	97.88%	92.34%
Pun et al. [32]	92.93%	92%
Li et al. [33]	57.64%	98.17%
Huang and Ciou [34]	97.66%	96.5%

It is seen from the experimental results that selecting smaller block size as 25×25 increases the accuracy, precision, and recall. On the other hand, it increases processing time. Compared to the existing approaches, the proposed enhancement strategy enables satisfactory results. Setting the block size to 50×50 improves the processing time but it causes to lower accuracy, precision and recall values.

5. Conclusion

In this study, the major strategy focuses on the enhancement on the conventional copy-move forgery detection algorithms. A block-based approach with intentional noise insertion at pre-processing stage is proposed. The proposed algorithm uses both overlapping and non-overlapping blocks and blocks features are extracted by the help of correlation, LBP, and histogram. Finally, thresholding and Euclidean distance are used in matching stage. A noise which is predetermined and coherent to correlation funtion is inserted onto the image in order to provide more sharp classifier in detecting the forgery or verifying the originality.

The given enhancement performance has been analyzed by the experiments and it is found that the proposed strategy provides more robust operation on copy-move forgery detection. It is also clear from the experimental results that setting smaller block sizes increases the accuracy. By the novel strategy presented here, with 25×25 blocks, 94.16% accuracy rate is achieved. Moreover, the proposed algorithm enables to have reasonable precision and recall values, 92.51% and 96.11%, respectively.

It is believed that the strategy defined here may be modified and applied to other algorithms if the characteristic of the noise is well chosen and harmonious to features used in feature maps. As a future study, trying the proposed approach on noisy images and also adapting it into the other existing algorithms will be the next targets.

References

[1] O. M. Al-Qershi and B. E. Khoo, “Passive detection of copy-move forgery in digital images: State-of-the-art”, *Forensic Science International*, vol. 231, pp. 284–295, 2013.

[2] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, “An evaluation of popular copy-move forgery detection approaches”, *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp. 1841–1854, 2012.

[3] H. Farid, “Image forgery detection A survey”, *IEEE Signal Processing Magazine*, vol. 26, no. 2, pp. 16–25, March 2009.

[4] N. B. A. Warif, A. W. A. Wahab, M. Y. I. Idris et al., “Copy-move forgery detection: Survey, challenges and future directions”, *Journal of Network and Computer Applications*, vol. 75, pp. 259–278, 2016.

[5] J. Zhao and J. Guo, “Passive forensics for copy-move image forgery using a method based on DCT and SVD”, *Forensic Science International*, vol. 233, pp. 158–166, 2013.

[6] G. Lynch, F. Y. Shih, and H.-Y.M. Liao, “An efficient expanding block algorithm for image copy-move forgery detection”, *Information Sciences*, vol. 239, pp. 253–265, 2013.

[7] A. Kuznetsova and V. Myasnikov, “A new copy-move forgery detection algorithm using image preprocessing procedure”, *Procedia Engineering*, vol. 201 pp. 436–444, 2017.

[8] M. D. Ansari, S. P. Ghrera, and V. Tyagi, “Pixel-based image forgery detection: A review”, IETE Journal of Education, vol. 55, no.1, pp. 40–46, 2014.

[9] J. Fridrich, D. Soukal, and J. Lukas, “Detection of copy-move forgery in digital images,” in Proceedings of the Digital Forensic Research Workshop, pp. 5–8, August 2003.

[10] Y. Huang, W. Lu, W. Sun, and D. Long, “Improved DCT-based detection of copy-move forgery in images”, Forensic Science International, vol. 206, pp. 178–184, 2011.

[11] J. Zhang, Z. Feng, and Y. Su, “A new approach for detecting copy-move forgery in digital images”, in 11th IEEE Singapore International Conference on Communication Systems, pp.362–366, 2008.

[12] X. Wang, X. Zhang, Z. Li, and S. Wang, “A DWT-DCT based passive forensics method for copy-move attacks”, in 3rd International Conference on Multimedia Information Networking and Security, pp. 304–308, 2011.

[13] R. Davarzani, K. Yaghmaie, S. Mozaffari, and M. Tapak, ”Copy-move forgery detection using multiresolution local binary patterns”, Forensic Science International, vol. 231, pp. 61–72, 2013.

[14] G. Ulutaş, M. Ulutaş, and V. V. Nabiyev, “Copy move forgery detection based on LBP”, in 21st Signal Processing and Communications Applications Conference, April 2013.

[15] A. C. Popescu and H. Farid, “Exposing digital forgeries by detecting duplicated image regions,” Department of Computer Science, Dartmouth College, Technical Report, TR2004–515, 2004.

[16] Z. Ting and W. Rang-ding, “Copy-move forgery detection based on SVD in digital image”, in 2nd International Congress on Image and Signal Processing, October 2009.

[17] I. Amerini, L. Ballan, R. Caldelli, A. D. Bimbo, and G. Serra, “A SIFT-based forensic method for copy–move attack detection and transformation recovery”, IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 1099–1110, 2011.

[18] X. Pan and S. Lyu, “Region duplication detection using image feature matching”, IEEE Transactions on Information Forensics and Security, vol. 5, no. 4, pp. 857–867, 2010.

[19] B. L. Shivakumar and S. S. Baboo, “Detection of region duplication forgery in digital images using SURF”, International Journal of Computer Science Issues, vol. 8, no. 1, pp. 199–205, 2011.

[20] P. Mishra, N. Mishra, S. Sharma, and R. Patel, “Region duplication forgery detection technique based on SURF and HAC”, The Scientific World Journal, pp. 1–8, 2013.

[21] E. Ardizzone, A. Bruno, and G. Mazzola, “Copy-move forgery detection by matching triangles of keypoints”, IEEE Transactions on Information Forensics and Security, vol. 10, no. 10, pp. 2084–2094, 2015.

[22] Y. Gan and J. Zhong, “Image copy-move tamper blind detection algorithm based on integrated feature vectors”, Journal of Chemical and Pharmaceutical Research, vol. 6, no. 6, pp. 1584–1590, 2014.

[23] L. Li, S. Li, H. Zhu, and X. Wu, “Detecting copy-move forgery

under affine transforms for image forensics", Computers and Electrical Engineering, vol. 40, pp. 1951–1962, 2014.

[24] F. Peng, Y.Y. Nie, and M. Long, "A complete passive blind image copy-move forensics scheme based on compound statistics features", Forensic Science International, vol. 212, pp. e21–e25, 2011.

[25] H. Shao, T. Yu, M. Xu, and W. Cui, "Image region duplication detection based on circular window expansion and phase correlation", Forensic Science International, vol. 222, pp. 71–82, 2012.

[26] G. Muhammad, M. Hussain, and G. Bebis, "Passive copy move image forgery detection using undecimated dyadic wavelet transform", Digital Investigation, vol. 9, pp. 49–57, 2012.

[27] L. Zhong and W. Xu, "A robust image copy-move forgery detection based on mixed moments", in IEEE 4th International Conference on Software Engineering and Service Science, pp. 381–384, May 2013.

[28] E. Ardizzone, A. Bruno, G. Mazzola, "Detecting multiple copies in tampered images", in Proceedings of the IEEE 17th International Conference on Image Processing, pp. 2117–2120, September 2010.

[29] D. Tralic, I. Zupancic, S. Grgic, M. Grgic, "CoMoFoD-New database for copy- move forgery detection", in Proceedings of 55th International Symposium ELMAR-2013, pp. 49–54, September 2013.

[30] I. Amerini, L. Ballan, R. Caldelli et al., "Copy-move forgery detection and localization by means of robust clustering with J-linkage", Signal Processing: Image Communication, vol. 28, no. 6, pp. 659–669, 2013.

[31] E. Silva, T. Carvalho, A. Ferreira, A. Rocha, "Going deeper into copy- move forgery detection: exploring image telltales via multi-scale analysis and voting processes", Journal of Visual Communication and Image Representation, vol. 29, pp. 16–32, 2015.

[32] C.M. Pun, X.C. Yuan, X.L. Bi, "Image forgery detection using adaptive oversegmentation and feature points matching", IEEE Transactions on Information Forensics and Security, vol. 10, no. 8, pp. 1705–1716, 2015.

[33] J. Li, X. Li, B. Yang, X. Sun, "Segmentation-based image copy-move forgery detection scheme", IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 507–518, 2015.

[34] H. Huang, A. Ciou, "Copy-move forgery detection for image forensics using the superpixel segmentation and the Helmert transformation", Journal on Image and Video Processing, vol. 68, 2019.