JOURNAL OF ENGINEERING AND APPLIED SCIENCE, VOL. 67, NO. 2, APR. 2020, PP. 447-466
FACULTY OF ENGINEERING, CAIRO UNIVERSITY

A NEW SPATIAL APPROACH TO DETECT COPY-MOVE FORGERIES IN DIGITAL IMAGES

T. K. ARAFA[1], B. I. ELGINDY[2] AND S. I. SHAHEEN[3]

ABSTRACT

The advancement of image manipulation and editing software platforms along with the increasing reliance on digital media in press, television networks let alone online social networks, increase the risk of tampering and editing of digital content into our visual content feeds. These platforms contain computer programs that allow for adding, altering or removing important image objects without leaving traces obvious to the naked eye. Such manipulations increase the demand to verify digital images, validate their content and detect forgeries. In this paper, we focus on detecting copy-move attacks in which a part of the image is copied and pasted somewhere else in the image to hide valuable image information. We investigate the problem of detecting the copy-move forgery, discuss major detection methods, and propose a new spatial method for copy-move forgery detection. The new method successfully detects forgery even if the image is post processed by lossy compression, noise addition or blurring. The performance of this method is compared against other methods and results are demonstrated using a common copy-move image dataset.

KEYWORDS: Image forensics, Forgery detection, copy-move, duplicated region detection, CMF, DCT, Quantization

1. INTRODUCTION

Low-cost and high-resolution digital cameras are becoming very popular, giving digital media more important role in our daily life, as digital images are used to record important occasions and events. Since digital images editing applications (for example: Photoshop) can perform increasingly sophisticated image operations yet are easy to use, digital images can be manipulated and forged without leaving visible clues making the credibility of digital content very questionable. Digital content can be used in courtrooms, insurance claims or even scientific frauds. According to statistics [1], in

[1] Computer Engineering, Faculty of Engineering, Cairo University
tarafa@hotmail.com
[2] Researcher, Computer and Systems Department, Electronics Research Institute, Egypt.
[3] Professor, Computer Engineering Department, Faculty of Engineering, Cairo University, Egypt.

one journal, as many as 20% of accepted manuscripts contain figures with inappropriate manipulations, and 1% of which with fraudulent manipulations. As a result, when the forged images are used for an inappropriate purpose, it may result in inestimable lose. Digital image forensics emerged as a new research field to reveal digital image forgery.

There are several types of tampering, however, copy-move forgery (CMF) is a common form of digital image tampering used in concealing some features/objects from natural images. Figure 1a and 1b, show a CMF example of 2 cats out of 3 replaced by copying and pasting underlying background, while Fig. 1c and 1d show another example of a group of soldiers duplicated to cover the speaker.

(a) (b) (c) (d)

Fig. 1. Samples of CMF manipulated and original images.

Researchers have developed many techniques to deal with CMF, most of which divide images into blocks and use block matching to identify which image areas are forged, several techniques will be discussed in detail in this paper. Fridrich et al. [2] used discrete cosine transform (DCT) based features instead of exhaustive search to detect region duplication, which is more effective, but their method is sensitive to variations in duplicated regions caused by additive noise. Popescu and Farid [3] proposed a new method by adopting the Principal component analysis (PCA) based features, which can endure some additive noise. J. Wang et al. [4] created circular blocks and used their features for block matching. Wu et al. [5] used log-polar transform to detect duplicate image regions that may be rotated and/or re-scaled, still the technique does not endure high noise or compression. Cao et al. [6] exploited the means of the DCT coefficients and circular blocks to extract the features, this technique reduce the feature length and show some robustness against noise and blurring but not compression. Few other techniques [7] are detailed.

In this paper, we introduce a new technique that can endure higher levels of compression, additive noise and blurring. And to test our theory, we develop all techniques mentioned above using Java and compare the results of all techniques using the same parameters, code baseline, pre-processing and post processing conditions to present our final conclusion.

2. DETECTION OF COPY-MOVE FORGERY

2.1 Algorithm Requirements

Copy-Move forgery (CMF) detection techniques aim to find correlation between original image segments and copied segments, and this correlation is used as a basis for effective detection of CMF. After pasting the forged segment, post processing alterations can take place by means of compression, noise addition or blurring, so researched agreed [7] that an effective detection algorithm should:

1. Allow for an approximate match of small image segments.
2. Work in a reasonable time.
3. Removes false positive matches and not introduce false positive matches.

2.2 Detection of Copy-Move Forgery by Block Matching

Block matching techniques use square blocks with B×B pixels. The square is slid by one pixel along the image from the upper left corner all the way to the lower right corner. For B×B block, the pixel values from the block are extracted into one row each, to form a 2D array A. The dimensions of this is array are (M–B+1)(N–B+1) rows (one row corresponds to one sliding block) and B×B columns (containing values of pixels in the sliding block) as shown in Fig. 2.

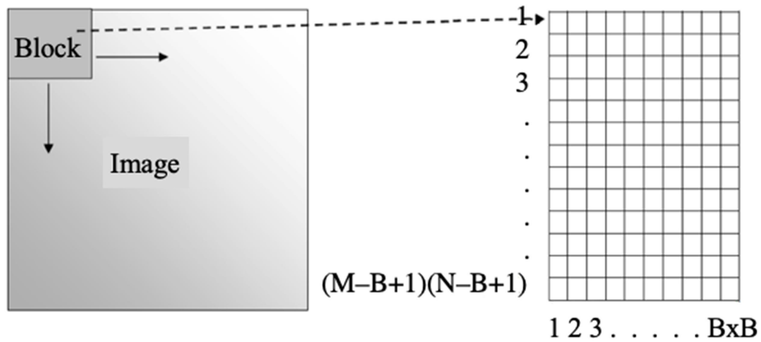

Fig. 2. Dividing an image into sliding blocks.

Two identical rows in the matrix A correspond to two identical B×B blocks. To identify the identical rows, the rows of the matrix A are lexicographically ordered (as B×B integer tuples) which is done in $MNlog_2(MN)$ steps. The matching rows are easily searched by going through all MN of the ordered matrix A and looking for two consecutive rows that are identical. The process steps are shown in Fig. 3.

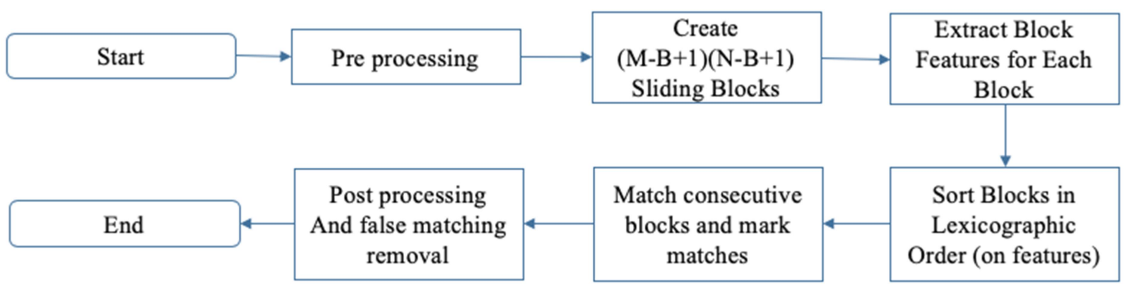

Fig. 3. Copy-move matching flowchart.

Thus, algorithms in this study work as follows:

- Each block is a 2D array of BxB pixels
- Blocks are extracted from the image and stored in an array (M-B+1)(N-B+1) rows and BxB columns
- Blocks are lexicographically sorted based on the matching feature for each block
- Consecutive blocks are compared and those with identical feature values (within a specific threshold) are considered initially matched

- Distance between initially matched blocks is stored and distance repeated most is used to promote block pairs as part of the forged images areas

2.3 Preprocessing

2.3.1 Gaussian filter

The bell-shaped smoothing Gaussian filter [8] is applied to the original image to reduce the effect of noise and smoothen the picture for better feature matching. The convolution matrix is shown in Fig. 4.

1	4	6	4	1
4	16	24	16	4
6	24	36	24	6
4	16	24	16	4
1	4	6	4	1

Fig. 4. Gaussian smoothing convolution matrix.

2.4 Matching Parameters

Below are some preprocessing methods used in different techniques to reduce false matches, as well as a new method we developed in 2.4.2. These methods are used in all implemented algorithms with the same parameters, to ensure streamlining the processes and providing comparable results.

2.4.1 Distance threshold

To ensure adjacent blocks are not falsely matched as a result of copy-move forgery, a minimum threshold is selected and matches between blocks with a distance less than the threshold are neglected as shown in Fig. 5. This distance is selected to be 60 for the algorithms studied in this paper. This is important to eliminate false matches introduced by homogeneous parts of the image. 60 is selected by trial and error and works well as copied blocks are usually more than 60 pixels a part in all copy-move cases in the sample database in this study.

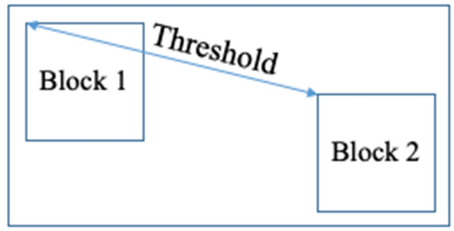

Fig. 5. Threshold distance.

2.4.2 Background blocks

Some blocks belong to the background of the image and including them in matching comparisons will lead to many false matches. We added a process to disqualify background blocks from the comparison, using standard deviation parameter.

- The mean of all pixel intensity values in the block is calculated.
- Deviations of each pixel point from the mean are calculated, then the result is squared.
- The variance is the mean of squared deviation values.
- Finally: standard deviation is equal to the square root of the variance.

If the standard deviation is less than a given threshold value, then this block is considered a background block and excluded from the matching process. This threshold is selected to be 2 for the algorithms studied in this paper based on different trails.

2.4.3 Most repeated distance

To be able to identify that a group of blocks is copy-moved, the distance between each 2 matched blocks is stored, and the distance that appears most suggests that all blocks matched with the same distance are part of a matched group [9] as in Fig. 6.

A Max-Min threshold allows for matching of blocks with distances between (Max – Threshold) and (Max + threshold). This value is selected to be 2 for the algorithms studied in this paper to allow 5 pixels variation in distance measurement.

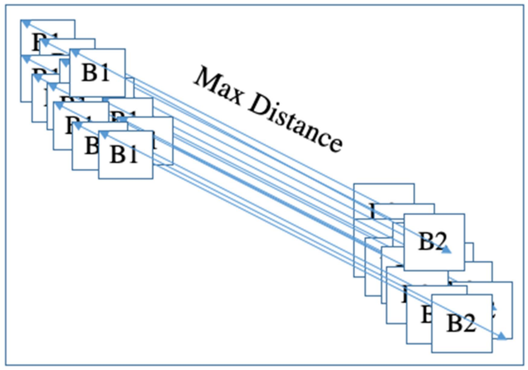

Fig. 6. Matched blocks with same distance belong to copy-moved area.

3. TECHNIQUES FOR COPY-MOVE MATCHING

3.1 Exhaustive Search

The first feature ever implemented used the pixel intensity values of blocks pixels as bases for block matching [2].

3.2 Discrete Cosine Transform (DCT)

The discrete cosine transform (DCT) [2] helps separate the image into parts (or spectral sub-bands) of differing importance (with respect to the image's visual quality). The DCT transforms a signal or image from the spatial domain to the frequency domain.

- Each block is an 8x8 square, and the 2D DCT is computed for each block based on Eq. (1).

$$F(m,n) = \frac{2}{\sqrt{MN}} C(m)C(n) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) cos \frac{(2x+1)m\pi}{2M} \cos \frac{(2y+1)n\pi}{2N} \quad (1)$$

Where $C(m), C(n) = 1/\sqrt{2}$ for $m, n = 0$ and $C(m), C(n)$=1 otherwise

- Only the low frequency values are used as features (16 features).

3.3 Principal Component Analysis Feature

Principal Component Analysis (PCA) method [3] is used for detecting duplicated regions and is similar to DCT.

While both methods employ a similar approach, the data-driven PCA basis may better capture discriminating features. PCA is more robust to additive noise and lossy JPEG compression than DCT.

- Each block is an 8x8 square.
- For each block, 8 Eigenvalues are used as matching features.
- $\overrightarrow{x_i}$ represent zero mean blocks.
- Eigenvalues are calculated based on covariance Eqs. (2-3) below.

$$C = \sum_{i=1}^{Nb} \overrightarrow{x_i}\, \overrightarrow{x_i}^T \quad (2)$$

Where C is the covariance matrix for $\overrightarrow{x_i}$

$$C\overrightarrow{e_j} = \lambda_j \overrightarrow{e_j} \quad (3)$$

For the eigenvalues and eigenvectors

3.4 Circular Blocks

The circular matching [4] is based on using circular blocks

- Each block is based on circular rings that fit within 8x8 square blocks as shown in Fig. 7a.
- Each circle would be divided into four concentric circles, which are denoted as Ω1, Ω2, Ω3 and Ω4 with radius equaling to 1, 2, 3, and 4 respectively as shown in Fig. 7b.

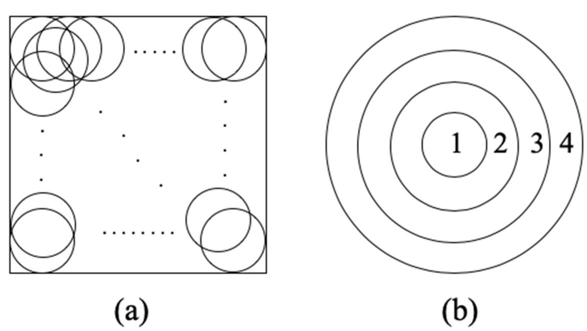

Fig. 7. Circular blocks.

- Calculate the 4 features φ1, φ2, φ3 and φ4, based on Eq. (4) (the mean of image pixel values for each circle).

$$\varphi_k = \frac{\sum x_{i,j}}{|\Omega_i|}, x_{i,j} \in \Omega_K \tag{4}$$

3.5 Log-Polar Features

Log-polar transform [5] is used to eliminate the rotation and scale effects in the input image by converting the image into a corresponding log-polar image. The log-polar transform algorithm is divided into two major steps. In the first step, the radius of the largest circle inside the given square image is used as a scan line to sample S times from 0 to 360 to produce its equivalent S x *[N/2]* polar form, So, formally, a polar form p(a, r) of the given NxN image f(x, y) can be computed as follows in Eq. (5) [10]:

$$p(a,r) = f\left(\left[\frac{N}{2}\right] + \left[r\cos\left(\frac{2\pi a}{S}\right)\right], \left[\frac{N}{2}\right] - \left[r\sin\left(\frac{2\pi a}{S}\right)\right]\right) \tag{5}$$

$$for\ a = 0, \ldots, S-1, and\ r = 0, \ldots, \left[\frac{N}{2}\right] - 1$$

The polar representation transforms the block from the x, y presentation to the a, r presentation as shown in Fig. 8.

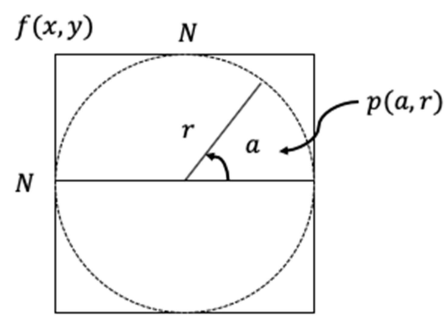

Fig. 8. Log-Polar transform of NxN image f(x,y) into SxR LP image p(a,r).

- Each block is based on circular rings that fit within 8x8 square blocks.
- For each block, an 8x4 LPR array is calculated to with LPR coefficients, to create the φ feature vectors.

3.6 DCT with Reduced Feature Vector

This DCT-circular matching [6] is based on 2 steps. First create the DCT for each block, then extract the feature vector based on the approach explained below.

- Each block is a 8x8 square.
- For each block, 8x8 DCT array is calculated to get DCT coefficients.
- Only the low frequency values are used, (4x4 array for each 8x8 block).
- Each 4x4 block, is considered a circular block with 4 sub-circles C1, C2, C3, C4, as shown in Fig. 9, with r the radius of the circle block of area: c_area = πr^2.
- The feature vector V with 4 values is calculated as follows in Eq. (6).

$$v_i = \frac{\sum x_{i,j}}{\text{c\_area}_i}, x_{i,j} \in \text{c\_area}_i, i = 1, 2, 3, 4 \tag{6}$$

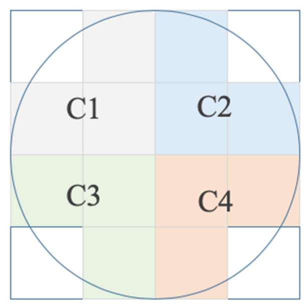

Fig. 9. Reduced Circular feature of DCT coefficients.

4. NEW TECHNIQUE FOR COPY-MOVE (9-FEATURES)

4.1 New Feature Design

All features discussed in the previous section face issues with high level of compression, additive white Gaussian noise and blurring.

To overcome these issues, we need to design a feature vector that:

- Is prune to random changes in blocks and is able to capture block similarities accurately.
- Is prune to false matching and can capture true copy-move forgeries.

Studying block dynamics, we found out that if horizontal and vertical intensity variations of blocks are truly unique to each block and would withstand noise and random changes, thus we are introducing a feature vector based on the weight of the horizontal and vertical intensities of block slices to withstand various pre-processing and post-processing operations. The following feature vector includes 9 elements in

Fig. 10 and is designed to accomplish the goals above, and we will refer to it as 9-Features in this paper.

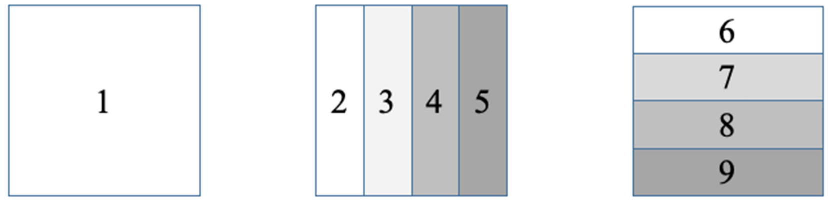

Fig. 10. 9-features, Feature Vector.

The 9 features are:

- The average intensities of all pixels in the block (1).
- The average intensities of 4 equal vertical rectangles (2-5), to capture vertical edges and changes in block intensities.
- The average intensities of 4 equal horizontal rectangles (6-9), to capture horizontal edges and changes in block intensities.
- The number of features will always be 9 irrespective of the block size, which reduces the block matching complexities for larger blocks.

Then the algorithm works as follows:

- Each block is a 2D array of 8x8 pixels.
- Blocks are extracted from the image and stored in an array (M-8+1)(N-8+1) rows and 64 columns.
- For each block, a "9 elements" feature vector is calculated as above.
- Blocks are lexicographically stored based on values of their feature vectors.
- The absolute difference between each value pairs are added up and then divided by size of the block.
- If the difference is zero for any 2 blocks, the 2 blocks are flagged matching.
- This technique has an added step to remove salt and pepper matching (heat-map) algorithm:
  - o A matching map is created with all (x, y) coordinates of source and destination matching blocks.

- After all matching is done a second round of correction is made to remove matches that are singular (matched block with no surrounding matching blocks).
- This technique removes the salt-n-pepper matches introduced due to technique sensitivity.

It is important to highlight that the size of the 9-Feature feature vector doesn't change when you change the matching block size, which is important from memory consumption perspective if you decide to increase block sizes, as seen in Table 1 below.

Table 1. Feature size for different techniques and block sizes.

Technique / Block Size	**8**	**16**	**32**	**64**
Exhaustive	64	256	1024	4096
DCT	16	64	256	1024
PCA	8	16	32	64
Circular	4	8	16	32
Log Polar	32	64	128	256
Modified DCT	4	4	5	4
9 Features	9	9	9	9

4.2 System Implementation

4.2.1 ImageJ

ImageJ is a public domain Java image processing program inspired by NIH Image for the Macintosh. It runs, either as an online applet or as a downloadable application, on any computer with a Java 1.4 or later virtual machine. Downloadable distributions are available for Windows, Mac OS, Mac OS X and Linux. [11]

It can display, edit, analyze, process, save and print 8-bit, 16-bit and 32-bit images. It can read many image formats including TIFF, GIF, JPEG, BMP, DICOM, FITS and "raw". It supports "stacks", a series of images that share a single window. It is multithreaded, so time-consuming operations such as image file reading can be performed in parallel with other operations.

4.2.2 Image analysis application

Our application consists of various java classes that run as a plugin on top of imageJ engine. Each copy-move forgery detection technique is implemented as an ImageJ plugin that takes an image + parameters as input, complete the detection process, and delivers a forgery map that shows the copied-moved objects, as an output.

5. COPY-MOVE DETECTION POST PROCESSING OPERATIONS

Most techniques provide acceptable results in ideal conditions, in which images include robust/correct data for matching techniques to use and produce correct matches. Forgers are aware of this and are increasingly implementing hindering operations to fool matching techniques and disable finding correct matches. The more robust the matching technique, the better it will hold against hindering operations and produce correct matches. The 3 major post processing operations and their effect on image quality are discussed below.

5.1 JPEG Compression

JPEG is a commonly used method of lossy compression for digital images, particularly for those images produced by digital photography. The degree of compression can be adjusted, allowing a selectable tradeoff between storage size and image quality. JPEG typically achieves 10:1 compression with little perceptible loss in image quality.

Adding JPEG compression as a post-processing step after copy-move will reduce the capability of copy-move detection techniques as it changes blocks in random fashion and matched blocks become no longer matched.

The amount of JPEG compression is typically measured as a percentage of the quality level. An image at 100% quality has (almost) no loss, and 1% quality is a very low-quality image. In general, quality levels of 90% or higher are considered "high quality", 70%-90% is "medium quality", and below 70% is low quality. For the purpose of this study we will use compression levels from 80% to 20%.

5.2 Additive White Gaussian Noise (AWGN)

AWGN is another post-processing technique that can be used to fool forgery detection techniques. It is simply done by adding random noise value to each pixel of the image. This is done mathematically by adding a random value between 0 and 1, multiplied by the STD of the noise, which will range from 2 to 8 in our experiments.

AWGN also reduces the capability of copy-move detection techniques as matched blocks become no longer matched with the added noise.

5.3 Image Blurring

Blurring uses convolution with a Gaussian function to smooth the image. Sigma (Radius) means the radius of decay to exp (-0.5) ~ 61%, i.e. the standard deviation sigma of the Gaussian. Scaled Units mean that the value of sigma is not in pixels but rather in units defined by the x and y image scale (for images with spatial calibration). This is an ImajeJ implementation. Sigma will range from 0.5 to 2 in our experiments.

Image blurring hides detailed of images and reduces the capability of copy-move detection techniques to detect copy-move forgeries.

6. RESULTS

Most techniques provide acceptable results in ideal conditions, in which images include robust/correct data, but forgers are aware of this and are increasingly implementing hindering operations to disable finding the correct matches.

6.1 JPEG Compression

To illustrate the effect of compression on copy-move detection techniques, 50 images are selected from CoMoFoD Image Database for CP Forgery Detection [12].

Original images as well as compressed versions in different qualities from 80 to 20 are used, and all techniques are applied to find the correct matches. A match is considered correct if 60% of the forged area is covered by the technique.

As compression increases, techniques fail to identify matched, while 9-features still finds 34 out of 50 matches with Jpeg 20 as shown in Table 2 and Fig. 11.

6.2 Additive White Gaussian Noise

The effect of AWGN is very similar to compression on copy-move detection techniques. As AWGN increases, techniques fail to identify matched correctly. With AWGN 8: almost all features fail, while 9-features finds 33 out of 50 matches as shown in Table 3 and Fig. 12.

Table 2. Table of compression results.

Type	Orig.	Jpeg 80	Jpeg 60	Jpeg 40	Jpeg 20
Exhaustive	48	42	17	0	0
DCT	45	36	0	0	0
PCA	43	3	0	0	0
Circular	42	3	0	0	0
Log Polar	46	44	32	18	3
Modified DCT	43	3	0	0	0
9 Features	48	45	40	38	34

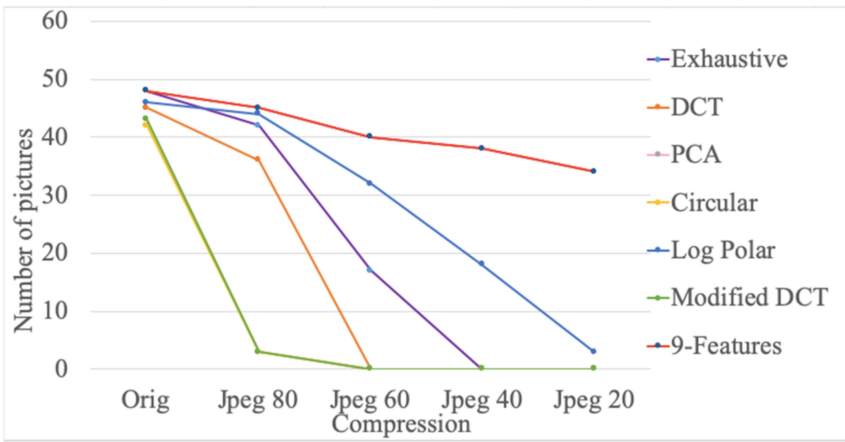

Fig. 11. Graph of compression results.

Table 3. Table of AWGN results.

Type	Orig.	AWGN2	AWGN4	AWGN6	AWGN8
Exhaustive	47	44	17	0	0
DCT	45	35	0	0	0
PCA	42	3	0	0	0
Circular	42	3	0	0	0
Log Polar	47	45	23	15	5
Modified DCT	42	3	0	0	0
9 Features	48	45	43	38	33

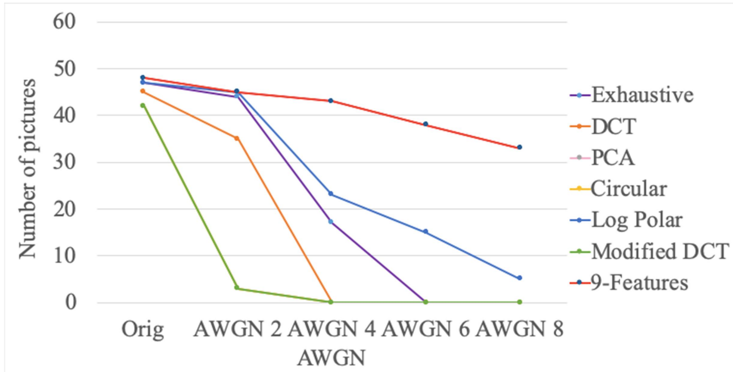

Fig. 12. Graph of AWGN results.

6.3 Image blurring

Blurring doesn't have strong hindering effects on the copy-move techniques in study. Technique remain acceptable with high blurring as shown in Table 4 and Fig. 13.

Table 4. Table of Blurring Results.

Type	Orig.	Blurr, 0.5	Blurr, 1	Blurr, 1.5	Blurr, 2
Exhaustive	48	48	47	47	46
DCT	45	45	45	45	43
PCA	42	42	41	40	38
Circular	42	43	43	40	40
Log Polar	47	47	47	46	46
Modified DCT	43	43	42	40	40
9 Features	48	48	47	47	46

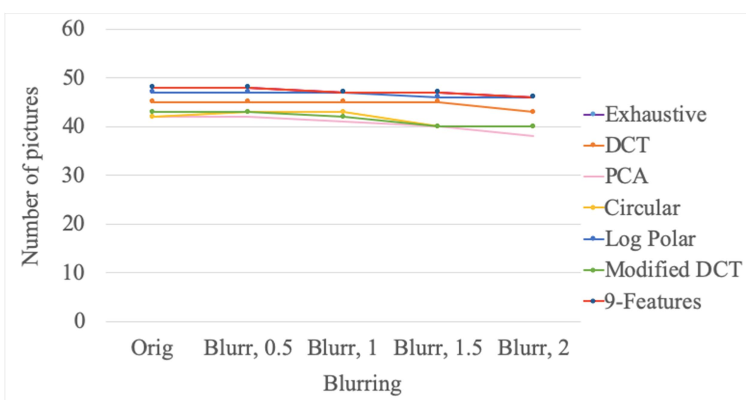

Fig. 13. Graph of blurring results.

6.4 Image Samples

In this section, we show the output of 9-Features for Original images, compressed, AWGNed and blurred images. The examples below in Figs. 14-17 are true output of the implemented java system.

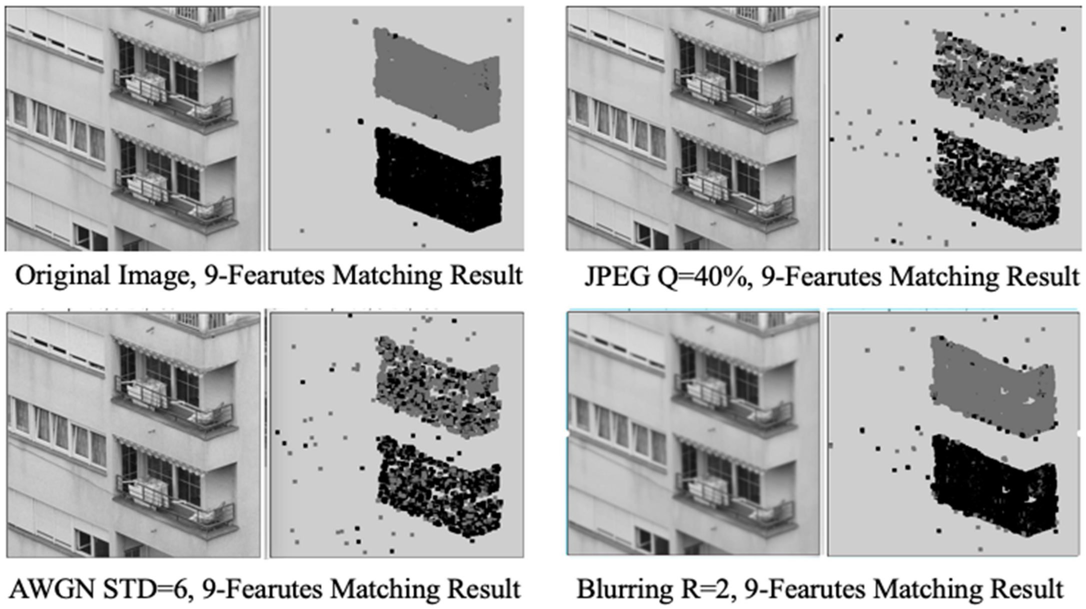

Fig. 14. 9-Features technique for large copy-move area.

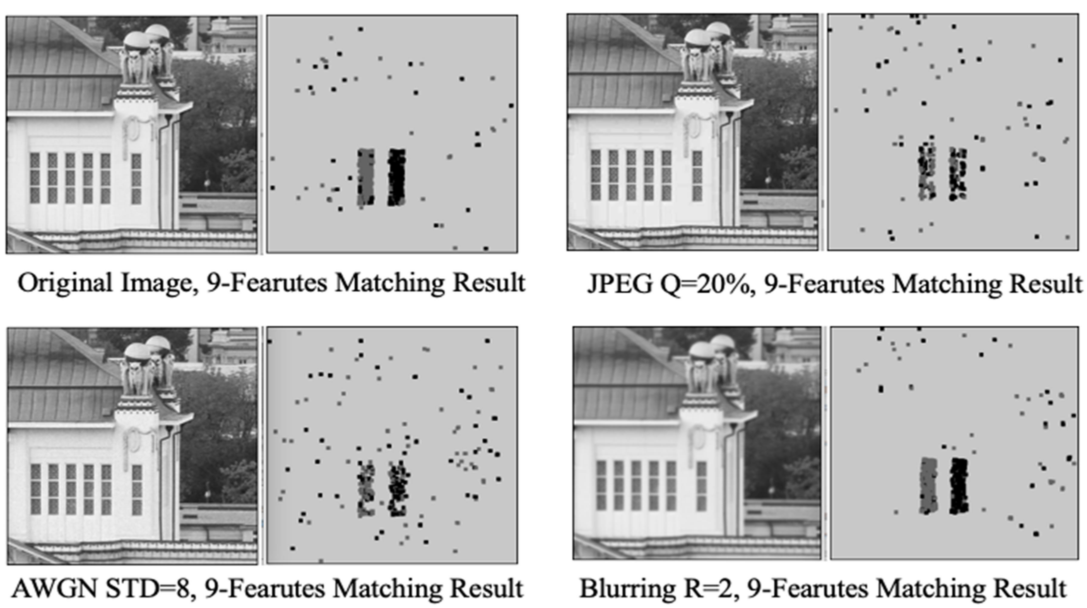

Fig. 15. 9-Features technique for small copy-move area.

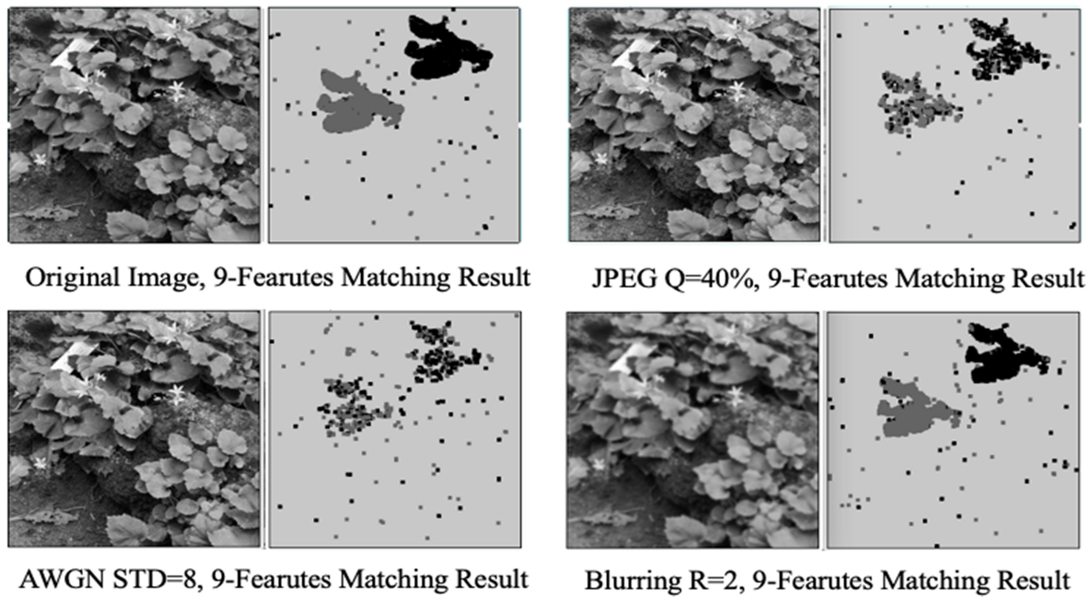

Fig. 16. 9-Features technique for blinded copy-move area.

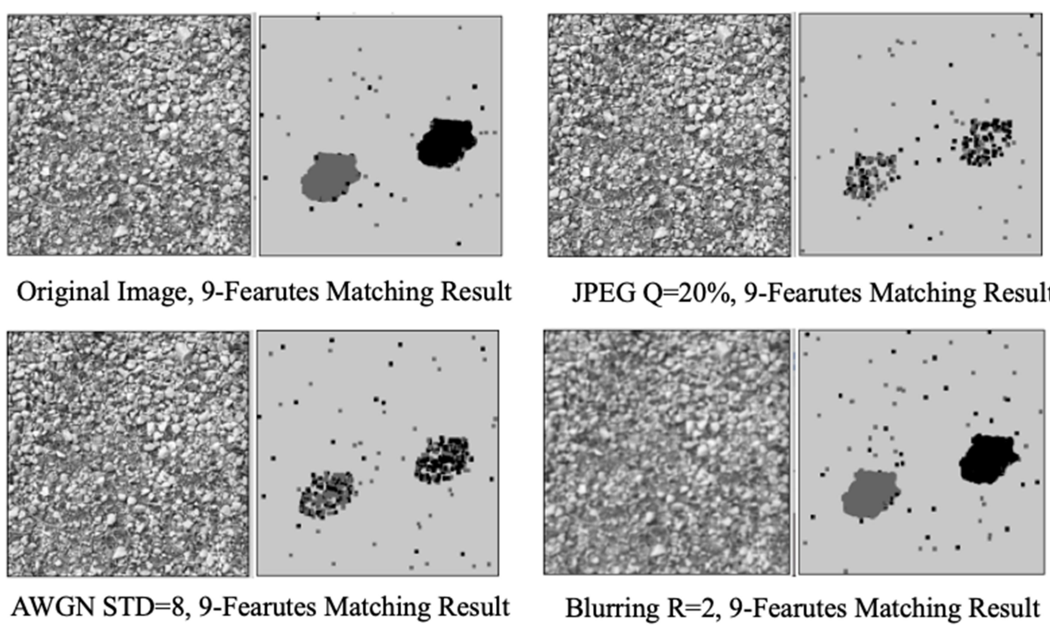

Fig. 17. 9-Features technique for background copy-move area.

7. CONCLUSION

9-Features technique is a new approach to solve the copy-move forgery detection problem. While other techniques provide acceptable results for images that have not been post processed, using compression or AWGN will cause most techniques to fail with right degree of tampering. 9-Featues provides superior results in case of compression, AGWN and blurring, when other techniques fail to get any results. 9-Features remain consistent at post processing levels that the naked eye can't easily catch, and it also uses same feature vector size of 9, no matter what block size you use. For future work, this technique is to be modified to be able to find matches for resized or rotated blocks (affine transformation copy-move).

DECLARATION OF CONFLICT OF INTERESTS

The authors have declared no conflict of interests.

REFERENCES

1. Farid, H., "Exposing Digital Forgeries in Scientific Images", Proceedings of the 8th Workshop on Multimedia and Security, Geneva, Switzerland, 2006.
2. Fridrich, J., Soukal, D., and Lukas, J. "Detection of Copy-Move Forgery in Digital Images", Proceedings of Digital Forensic Research Workshop, pp. 55-61, 2003.
3. Popescu, A., and Farid, H., "Exposing Digital Forgeries by Detecting Duplicated Image Regions", Technical Report TR2004-515, Dartmouth College, 2004.
4. Wang, J., Liu, G., Li, H., Dai, Y., and Wang, Z., "Detection of Image Region Duplication Forgery Using Model with Circle Block", International Conference on Multimedia Information Networking and Security, 2009.
5. Wu, Q., Wang, S., and Zhang, X., "Log-Polar Based Scheme for Revealing Duplicated Regions in Digital Images", IEEE Signal Processing Letters, Vol. 18, No. 10, 2011.
6. Cao, Y., Gao, T., Fan, L., and Yang, Q., "A Robust Detection Algorithm for Copy-Move Forgery in Digital Images", Forensic Science International, Vol. 214, pp. 33-43, 2012.
7. Mahmood, T., Nawaz, T., Ashraf, R., Shah, M., Khan, Z., Irtaza, A., and Mehmood, Z., "A Survey on Block Based Copy Move Image Forgery Detection Techniques", Emerging Technologies (ICET) International Conference, 2015.
8. Pratt, W., "Digital Image Processing: PIKS Inside, Third Edition", John Wiley and Sons Inc., ISBN: 0-471-37407-5, 2001.

9. Li, G., Wu, Q., Tu, D., and Sun, S., "A Sorted Neighborhood Approach for Detecting Duplicated Regions in Image Forgeries Based on DWT and SVD", in Multimedia and Expo, IEEE International Conference, 2007.
10. Pun, C. and Lee, M., "Log-Polar Wavelet Energy Signatures for Rotation and Scale Invariant Texture Classification", IEEE Transaction on Pattern Analysis and Machine Intelligence, Vol. 25, No. 5, 2003.
11. ImageJ Java Image Processing Program, https://imagej.nih.gov/, (Accessed 5/5/2019.
12. Comofod Image Database for Copy-Move Forgery Detection, University of Zagreb, Video Communications Lab (VCL), http://www.vcl.fer.hr/comofod, 2013.

أسلوب جديد لاكتشاف تزييف الصور الرقميه

تناول البحث دراسة للوسائل المختلفة المستخدمة لكشف تحريف وتزييف محتويات الصور الرقمية باستخدام اجزاء من نفس الصورة لإخفاء أو تغيير محتوياتها. كما يتناول البحث طرح أسلوب جديد يمتاز بالقدرة على اكتشاف التزوير بدقة حتى في حالة استخدام وسائل إخفاء اضافية مثل ضغط الصورة او اضافه تشويش رقمي للصورة الامر الذي لا تستطيع الوسائل الأخرى اكتشافه. وأخيرا يحتوي البحث على مقارنة مستفيضة لنتائج كشف التحريف بين الأساليب الحالية والأسلوب الجديد في ظروف مختلفة من الضغط والتشويش واضافة بيانات مغلوطة.