International Journal of Engineering & Technology, 7 (2.13) (2018) 79-87

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper



Detection of copy-move image forgery using SVD and cuckoo search algorithm

Abhishek Kashyap [1] *, Megha Agarwal [1], Hariom Gupta [1]

[1] Department of Electronics and Communication Engineering jaypee Institute of Information Technology, Noida-201304, Uttar Pradesh, India
**Corresponding author E-mail: abhishek.kashyap@jiit.ac.in*

Abstract

Copy-move Copy move forgery (CMF) is one of the straightforward strategies to create forged images. To detect this kind of forgery one of the widely used method is single value decomposition (SVD). Few methods based on SVD are most acceptable but some methods are less acceptable because these methods highly depend on those parameters value, which is manually selected depending upon the tampered images. For different images, we require different parameter values. In this paper, we have proposed a novel method, which uses both copy-move forgery detection using SVD and Cuckoo search (CS) algorithm. It utilizes Cuckoo search algorithm to generate customized parameter values for different tampered images, which are used in copy-move forgery detection (CMFD) under block based framework.

Keywords: *Image Forgery Detection; Copy-Move; SVD; Cuckoo Search Algorithm.*

1. Introduction

Nowadays we are surviving in the era of digital revolution and it is very easy to access, process and transfer digital data. Advanced image processing methods make it possible to tamper the digital images, let suppose forgers want to misguide people or make a rummer then they can alter the details of the original image and develop a tampered image, now the task of the forensic department to deal with the image for identifying the fact behind it. As we know, the different type of image forgeries and their detection methods are available at the present time.

There are different type digital image forgeries such as Image splicing, cloning and image re-touching etc. Image re-touching is very less harmful kind of digital image forgery, in which certain features are reduced or enhanced from the original image, splicing is formed by the combination of two or more images for hiding important information from the original image and cloning is extremely destructive sort of image forgery problem, which is created by copying one part of the image and paste onto the another part of the same image for hiding some secret information. Active and passive methods are generally utilized for image forgery detection [11]. In active methods, we include some authentic information inside an image at the time of capturing or after the capturing in form of watermarking for unwavering quality check and passive methods purely work on the analysis of the digital binary information present in the image, there is no need to insert any information inside an image for authentication purpose.

Many copy-move forgery detection (CMFD) methods have been proposed throughout the most recent decade. In [12] the authors proposed such a sort of technique in light of blur moment invariants. It is endeavoring to distinguish copy-move forgery using block based method. Fridrich [13] proposed a strategy to recognize the tampered part even when the copied area is enhanced/retouched or to combine it with the background and when the tampered image is saved in a lossy format, such as JPEG and the technique [15] functions as to apply a principal component analysis (PCA) on small fixed-size image blocks to yield a diminished measurement portrayal that is robust to minor variations in the image due to lossy compression or additive noise. In [17] authors proposed an algorithm to detect copy-move forgery, depends on extracting feature vectors and SVD, which have some critical properties of geometric invariance and insensitiveness to noise. Bayram [18] presented a method for recognizing copy-move forgery in digital images, which is impressively more vigorous to lossy compression, rotation and scaling type of manipulations. Lin [20] proposed an effective strategy for copy-move forgery detection using radix sort, which has the capacity to resist various attacks such as Gaussian noise and JPEG compression. Huang [26] exhibited a strategy based on improved DCT to recognize copy-move forgery even when an image was distorted by blurring, JPEG compression, or by additive white Gaussian noise. Zhang [27] presented a new blind forensics algorithm for detecting copy-move forgery in the light of DWT (Discrete Wavelet Transform), which has lower computational complexity and robust to various types of copy-move post processing attacks. In [29] authors proposed an algorithm based on wavelet decomposition to detect copy-move forgery, the large size of the image is processed using this algorithm within small processing time. In spite of the fact that the improvement is significant, the outcomes are still a long way from satisfactory for practical forensic scenarios. In this paper, we propose an improved framework to deal with the problem of image forgery confinement with the assistance of SVD and cuckoo search algorithm. Our experimental outcomes demonstrate that the proposed CMFD scheme outperforms most prior arts, especially the block-based ones regarding detection rate.

The rest of the paper is structured as follows. A review of image forgery detection is introduced in section 1. In Section 2 we exhibit problem formulation for forgery detection. In section 3 we propose a novel strategy in light of SVD and CS algorithm for forgery detection. In section 4 we provide experiments and simulation results. In section 5 we exhibit conclusions and scope for the future wor

Copyright © 2018 Abhishek Kashyap et. al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

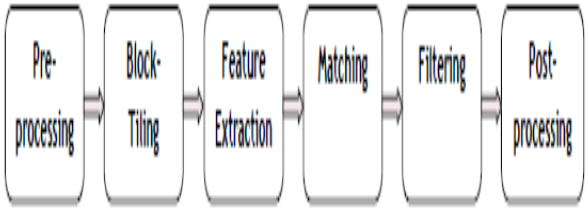


Fig. 1:.Common Flow Work of Block-Based CMF Detection Framework.

2. Formulation of problem

This section analyzes the problem in the parameter setting after a brief description of the Block based framework.

2.1. The block-based framework

By and large, copy-move forgery detection approaches under the block-based framework may be divided into pre-processing, block tiling, feature extraction, matching, filtering and post-processing as shown in Fig. 1. The pre-processing step is to prepare an image for identification, such as converting an RGB image into a grayscale image with standard color space conversion. The image is subdivided into rectangular blocks in the block based method. A feature vector is computed for each block. Comparative feature vectors are subsequently matched. They can be gathered into singular values of reduced rank. Feature extraction is constructed a descriptor or feature vector for each key point in light of its association with the surrounding pixels. Matching is to determine matched key-points based on feature vector. The regions around the matched key points are probably duplicated regions. Filtering is to eliminate mismatch key points, which are identified as matched key points during matching, but actually, they are not. Post-processing is to delete duplicated regions or estimate geometric transformation parameters.

2.2. Problems in parameter values selection

An obvious drawback exists in existing CMF detection approach, as detection results highly depend on the selection of parameter values. Normally, these parameter values are determined by experiences or results of the test against number forged images. However, different research teams choose different values, which are applicable to certain images. The following limitations appear, When they are used to detect a large number of images: i) Duplicated regions can't be detected when matched block pairs do not satisfy
the matching conditions; ii) Detected region is not duplicated ones, if there are too many similar objects in an image and parameter values are chosen inappropriately, some similar regions may be mistakenly regarded as the duplicated region, though actually, they are native regions in the original images.

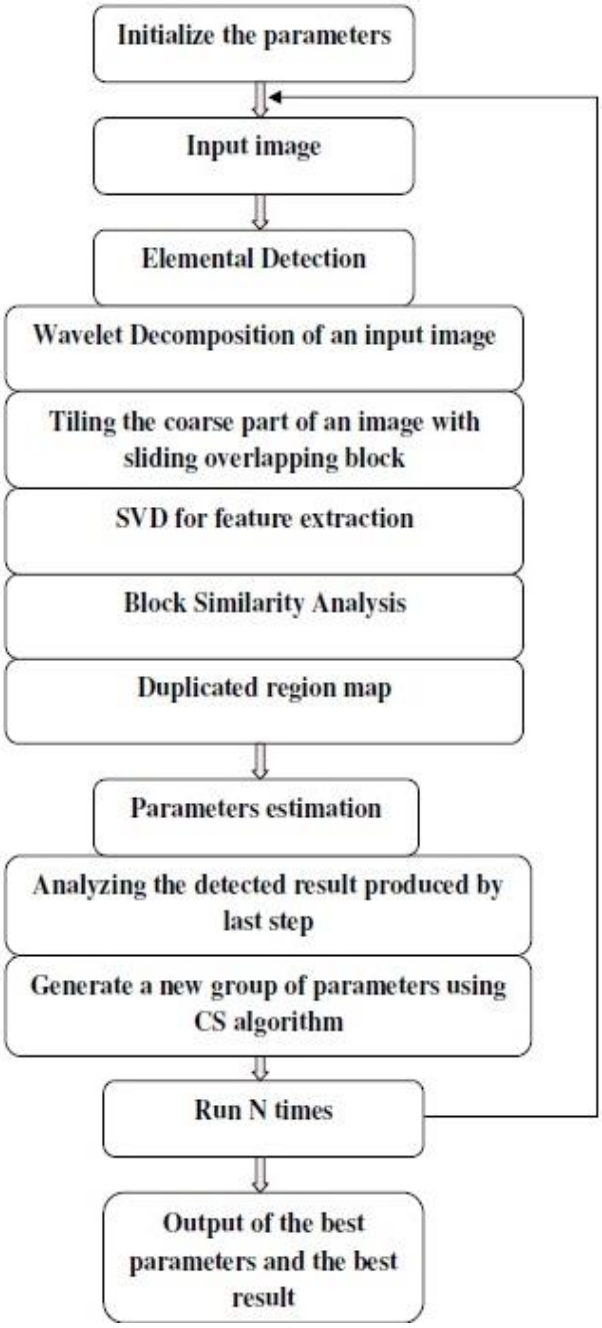


Fig. 2:.The Flow Chart of Our Approach, CMFD-CS.

3. Design of our approach

The goal of our approach, CMFD-CS is to automatically generate suitable parameter value for each test image. The comprehensive algorithm of CMFD-CS is shown in the Fig. 2. It includes two components, one of which is elemental detection and the other is parameter estimation. Elemental Detection is derived from the block based frame work. Its task is to detect copy-move forgery. Parameters estimation is new phenomena, which can generate suitable parameter values for each image. The corresponding image may produce a satisfactory result using these values. The CS algorithm is applied to estimate parameter values. To our knowledge, none of the existing CMF detection approaches use the CS algorithm. CMFD-CS automatically produces appropriate parameter values for each image as per the available feature of the given image. With these parameter values, elemental detection can produce better results. The first step is to identify the input and the output of the block-based frame work. The input includes an image and a group of parameters. The output

is only the number of matched blocks. Which is used to evaluate whether the result is good or not? We turn parameter value estimation into an issue of the optimal solution. An evaluation criterion is created to make detection decision. The criterion is formed by the number of matched blocks, when the criterion reaches extreme value optimal solution turn out.

3.1. Cuckoo search algorithm

For depicting Cuckoo-Search Algorithm [7] in a simple way we are following three admired tenets: (i) Each cuckoo lays one egg at once, and dump its egg in discretionarily picked nest; (ii) The best nests with high caliber of eggs will proceed to the next generations; (iii) The quantity of open host nests are fixed, and the egg laid by a cuckoo is found by the host bird with a likelihood $p_a \in [0, 1]$. For this circumstance, the host bird can either dispose the egg or surrender the nest and build an absolutely new nest. For ease, this last assumption can be approximated by the division pa of the n nest are supplanted by new nests [8]–[9].

For a maximization problem, the quality of a solution or fitness value can be simply proportional to the value of the objective function.

Initial population generation of n host nests z_i (i = 1, 2,…, n)
While t < MaxGeneration or stop criterion do
Randomly ret a cuckoo by Levy flights
Measure its fitness or quality F_i
Randomly choose a nest among n (say, j)
If $F_i > F_j$ then
Replace j by the new solution
End if
Fractions (P_a) of worse nests are unrestrained and new ones are built
Keep the best outcomes (or nests with better quality solutions)
Rank the solutions and find the current best

In view of these standards, the fundamental steps of the Cuckoo Search (CS) can be analyzed as the pseudo code. For a cuckoo i, Levy flight is performed for producing new arrangements or solutions $z^{(t+1)}$:

$$Z_i^{(t+1)} = Z_i^{(t)} + \alpha \oplus \text{Levy}(\lambda) \quad (1)$$

Where $\alpha > 0$, it is the step size, which ought to be identified with the scale of the issue of interests. In most cases, we can utilize $\alpha = 1$. Fundamentally, the Levy flight gives a sporadic walk while the sporadic step length is drawn from a Levy distribution:

$$Levy \sim u = t^{-\lambda}, (1 \leq \lambda \leq 3) \quad (2)$$

This has an infinite mean with an infinite variance. Here the steps essentially frame an arbitrary walk process with a power-law step-length distribution with a significant tail. Some of the new outcomes ought to be produced by Levy walk around the best outcomes so far, this will accelerate the local search. However, a significant fraction of the new outcomes ought to be generated by far field randomization and whose locations should be adequately a long way from the current best solution, this will ensure that the framework would not be trapped in a local optimum. There are some important complexities between CS and some other optimization algorithm, randomization is more proficient as the step length is significantly tailed, and any huge step is possible and the number of parameters to be tuned is not as much as GA and PSO [2]. So that it is potentially more generic to adapt to a more extensive class of optimization problems.

At first, irregular or manually produced initialization parameter values are used to detect image forgery using
CMFD-CS. Then the following two operations are executed N times. i) Elemental discussion detects the input images with the detection parameter values and then delivers the detection result to the operation (2). ii) According to the result of the operation (1), a new group of parameter values to operation (1) and start the next round. The best detection result is chosen from the operation of N rounds. Then this result and relevant parameter values are output. In our experiment, we set the value of N to 500.

3.2. The elemental detection

The proposed elemental detection method of digital image forgery includes the accompanying strides: A) Wavelet decomposition of the input image; B) Tiling the image with overlapping grid block; C) Singular Value Decomposition (SVD) of each tile block; D) Investigation of block similarity; E) Duplicated regions map.

a) Wavelet decomposition: This procedure begins with the calculation of wavelet transform of the input image, after computing wavelet transform; we have the high-low bands, the low-high bands and the high-high bands of the input image at different scales. At that point, we have processed the coarse part of the image for image imitation recognition.

We have utilized Harr wavelet, $\psi(z)$, which is orthogonal to the scaling function ϕ_2 (z-m) and it is characterized [30] by-

$$\psi(z) = \sum_{m=-\infty}^{\infty} (-1)^m a_{N-1-m} \sqrt{2} \phi(2z - m) \quad (3)$$

Wavelet decomposition of the function f(x; y) in two dimensions is characterized as [30],

$$f(z, y) = \sum_{j=-\infty}^{\infty} \sum_{k=-\infty}^{\infty} \sum_{l=-\infty}^{\infty} w_{j,k,l} \psi_{j,k}(z) \psi_{j,l}(y) \quad (4)$$

Where $a_{(N-1-m)}$ and $w_{j,k,l}$ are the weighting factor and handle as a constant.

b) Tiling the image with overlapping grid block: The coarse part of the image is being tiled [12] by the square block of (R × R) pixels, which is obtained after wavelet decomposition. This block horizontally slides from left to right and top to bottom as shown in Fig. 3. Here we have assumed, the copied region size must be bigger than the square block size and the total overlapping blocks are (M-R+1) × (N-R+1) for the digital image size of (M×N) pixels.

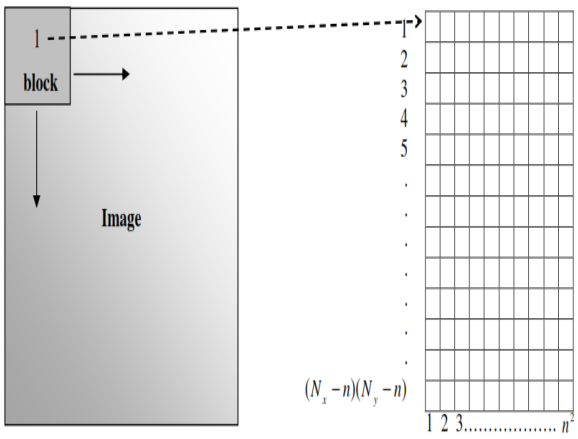


Fig. 3: Square Block Scan by Pixels and Array Dimensions for the Matching Algorithm. [29].

c) Singular Value decomposition of each tiled block: Each tiled block can be represent with the help of SVD [3], factorization of a real or complex matrix is obtained by SVD, which is generally used in useful applications of statistics and signal processing [4]. If A is an (m1×n1) complex matrix or real, a decomposition of this matrix A could be:

$$A = U \Sigma V^T \quad (5)$$

Where $U \in m_1 \times m_1$ and $V \in n_1 \times n_1$ (V^T is the transpose of V) are complex or real unitary matrices and $\Sigma \in m_1 \times n_1$ is a rectangular diagonal matrix in which its diagonal elements consist of non-negative real numbers arranged in descending order. In this manner, the diagonal of Σ is considered as the singular values of A.

$$Sv = diagonal\ of\ (\Sigma) \quad (6)$$

The correlated variables can be transformed into an arrangement of uncorrelated ones to better exhibit the different relationships among the original dataset by SVD technique [5]. For the alteration of copy-move fraud process, it can show the soft relationship between the rows and column of the digital image. So to get the adjusted correlation among the digital image pixels, singular values can be applied in copy-move recognition technique. A function is expected to give equal emphasis on singular values since the copy-move process has the different impact on singular values. The logarithm of the inverse power of singular values is introduced for the feature extraction of the digital image. The proposed method divides the digital image into sub-block or tiled block of size R _ R to evaluate inter block and intra-block correlation due to high dependency of the image pixels. For feature extraction, we need to calculate the singular value vector (Sv) for each sub-blocks a:

$$Sv_a = [\alpha_{1a}, \alpha_{2a}, \alpha_{3a}, \dots, \alpha_{na}];\ n \in no.of\ features, \alpha = 1,2, \dots, (M-R+1) \times (N-R+1) \quad (7)$$

At that point, find out the inverse of natural logarithm of each singular value is calculated and the outcomes are summed for each sub-blocks j:

$$SVB_a = \sum_{d=1}^{n} log(\alpha_{da}^{-1}) \quad (8)$$

d) Block similarity analysis: In this step, the similarity between the sub-blocks is obtained by calculating Euclidean distance. If we found any sub-block has lesser Euclidean distance, at that point, we can say they are similar. This is not a sufficient but a necessary condition. Additionally, we need to check their neighborhood sub-blocks for finding similarity. If their neighborhood is additionally comparable, by then there is a high probability that they are duplicated and they ought to be marked.

The similarity measure S (B_a, B_b) [12] between two sub-blocks B_a and B_b is defined as:

$$S(B_a, B_b) = \frac{1}{1+\rho(B_a, B_b)} \quad (9)$$

Where ρ is Euclidean distance between two sub-blocks, a = 1, 2… (M-R+1) × (N-R+1) and b = 1, 2… (M-R+1) × (N-R+1).

$$\rho(B_a, B_b) = (\sum_{d=1}^{n} (B_a[d] - B_b[d])^2)^{1/2} \quad (10)$$

If S (B_a, B_b) > T, at that point we have further investigated the neighboring blocks of B_a and B_b. Threshold (T) is the minimum required similarity and it played a very vital role to obtain the degree of reliability between sub-blocks a and b, which is utilized to make a decision for digital image forgery. We have picked 16 neighboring sub-blocks r with a most extreme separation of 4 pixels from the analyzed sub-block for investigating the neighborhood blocks.

$$S\big(block(i + x_r, s + y_r), block(i + x_r, s + y_r)\big) \geq T \quad (11)$$

Where $x_r \in 2$ (-4, -3…3, 4) and $y_r \in 2$ (-4, -3…3, 4) and r = 1… 6.

If S (block (a, s), block (b, t)) > T, but

$$\left(\sqrt{(a-b)^2 + (s-t)^2}\right) \leq D \quad (12)$$

We have obtained the optimum size of forged area using equation (11) and (12). If the similarity between sub-blocks is more prominent than the threshold T but the separation between them is not as much as the threshold D, then these sub-blocks will not be further analyzed and will not be assigned as a copied region. Threshold D is utilized to decide the minimum separation between the duplicated regions and it plays a vital role to provide more precise outcomes for digital image forgery detection.

Finally, we got an outcome in the form of a matrix Q, which will be the same size of the coarse part of the input image. An element of this matrix is set to one if the block at this position is copied otherwise set to zero.

e) Duplicated regions map creation: Duplicated regions map is formed by the multiplication of each element of I (x, y) by its respective element in Q (x, y).

3.3. The parameter estimation

The CS algorithm is utilized to look through the adjustable parameters. The CS algorithm is suitable for solving minimization or maximization problems.

a) Parameter for elemental detection: The parameters of the block-based framework should be optimized and their boundaries are listed in table I. The purpose behind the choice of these parameters is that these parameters will make an evident effect on the final detection results.

b) Evaluation function: Although metrics for detection approaches are different in various literatures, the core idea is similar: true matched Blocks (TMB), less mismatched Blocks (MMB) and less missing matched Blocks (Miss-MB). Therefore in the process of building the evaluation function, these factors should be considered. The ideal solution is that the number of the TMB is as large as possible. The large number of TMB is not only conductive to estimating the duplicate region accurately, but also make the detection results more convicting. Therefore, the evaluation function is built as the following:

$$P_{match} = \frac{TMB_t}{TMB_t + \phi}, \phi = \begin{cases} MMB_t,\ MMB_t > D \\ 10,\ MMB_t \leq D \end{cases} \quad (13)$$

Where, TMB_t and MMB_t are the number of the true matched blocks or mismatched blocks in fact. They are both determining by the affine transform at filtering. The pairs of blocks meeting the affine transform are regarded as true matched key points TMB_t and other pair are taken as the mismatched key points MMB_t does not include the eliminated pair of matched blocks that the distance between them less than D. ϕ gives a default minimum value for MMB_t and it is the mismatch coefficient. P_{match} is the probability of real matching. The evaluation criterion of CMFD-CS is P_{match}. Parameters Estimation will choose the highest value of P_{match} as the best result

Table 1: Optimization Parameters (Parameters in Block-Based Framework)

Parameters	Meaning	Lower bound	Upper bound
R	Block size	4	20
r	Number of neighbourhoods	4	16
D	The minimum distance	10	40
T	The parameter useful for rejecting unstable blocks	.001	.9

4. Experiments and results

4.1. Metrics

The critical measures are the number of successfully recognized forged images (T_P), the number of images that have been falsely recognized as forged (F_P) and the erroneously missed forged images (F_N) at the image level. From these, we have computed the measures precision (p) and recall (r). They are characterized as:

$$p = T_P/(T_P + F_P\ ), and\ r = T_P/(T_P + F_N\ ) \quad (14)$$

Precision demonstrates the likelihood that a distinguished forgery is a genuinely forged, while recall demonstrates the likelihood that the forged image is recognized. The recall is also known as true positive rate. For a reasonable comparison with all the outcomes obtained from the tested images, localization performance of the forged image is evaluated with the F_1-score, which is characterized as:

$$F_1 = 2.\frac{Precision.Recall}{Precision+Recall} = \frac{2T_P}{2T_P+F_N+F_P} \quad (15)$$

4.2. Results

In this section, we have talked about the outcomes of the proposed method described in section 3. All experiments are performed on CoMoFoD (DB-1) [33], MICC-F600 (DB-2) [34] and MICC-F2000 (DB-3) [34] database. Due to the variety of images, these databases are being utilized by specialists in various scientific articles of CMFD. Different performance measures like precision, recall and F_1-score are computed to contrast the performance of proposed methods and some of already published papers Babak [12], Fridrich [13], Popescu [15], Kang [17], Bayram [18], Lin [20], Huang [26], Zhang [27] and Wave. Dec. [29]. It is difficult to achieve a high numeric value for both precision and recall. In the ideal case, both precision and recall ought to accomplish 100%.

a) CoMoFoD database (DB-1): CoMoFoD database for a copy-move imitation recognition comprises of 260 forged image sets in two categories (small 512 × 512, and large 3000 2000). Images are assembled into various groups according to applied manipulation: scaling, translation, distortion, and combination. Distinctive sorts of post-processing techniques, for example, blurring, noise adding, color reduction and JPEG compression etc., are applied to all forged and original images. At the point when forged images have processed to our proposed algorithm for the detection of copy-move forgery, we have a conceivable indication of the tempering. A few examples of original images, tampered images, and their detection results are shown in Fig. 4 based on DB-1.

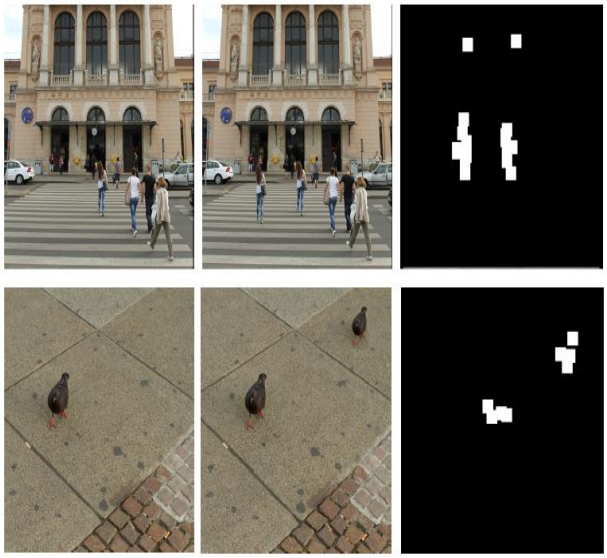


Fig. 4: Some Examples of Original Images are Placed in the First Column; Their Tampered Images Appear in the Second Column and the Corresponding Detection Results are Reported in the Third Column Based on DB-1.

Table 2: Detection Results of Plain Copy-Move Forgery Based on Db1

Methods	Precision (%)	Recall (%)	F1 (%)
Babak [12]	86.48	84.12	85.28
Fridrich [13]	86.79	84.59	85.68
Popescu [15]	87.85	85.49	86.65
Kang [17]	88.48	86.47	87.46
Bayram [18]	90.89	87.89	89.36
Lin [20]	92.65	88.45	90.50
Huang [26]	88.69	90.87	89.77
Zhang [27]	89.65	90.34	89.99
Wave. Dec. [29]	94.31	91.32	92.79
Proposed CMFD-CS	96.13	92.3	94.18

Copyright © 2018 Abhishek Kashyap et. al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

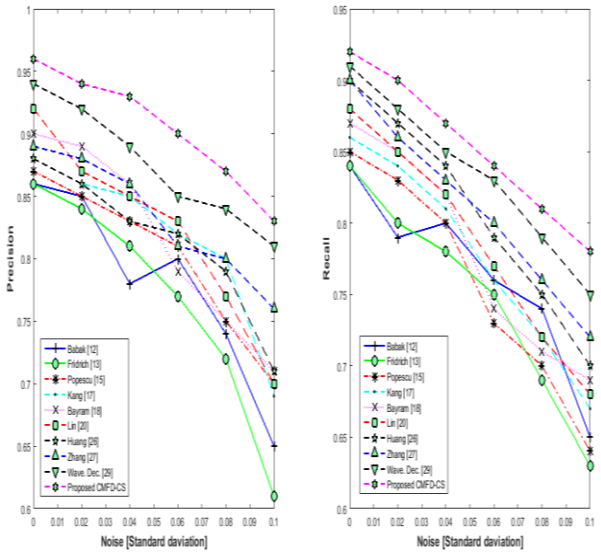


Fig. 5: Comparison between Proposed CMFD-CS and Exiting Algorithms, when Adding Gaussian Noise Based on DB-1.

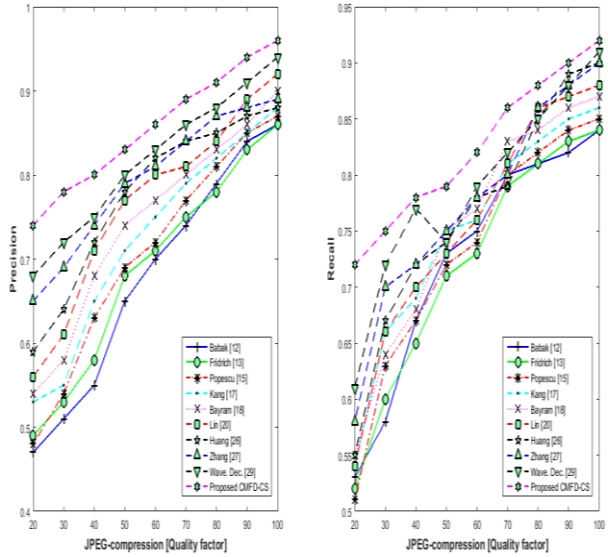


Fig. 6:.Comparison between Proposed CMFD-CS and Exiting Algorithms, when Performed JPEG Compression Based on DB-1.

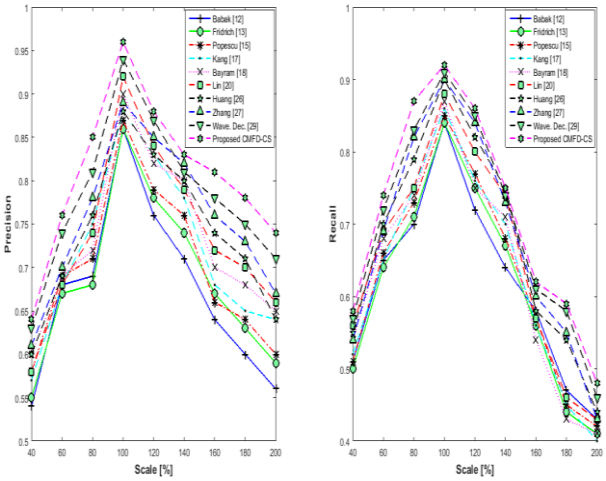


Fig. 7: Comparison between Proposed CMFD-CS and Exiting Algorithms, when Performed Scaling Based on DB-1.

We test the robustness of CMFD-CS against different attacks, which incorporate plain copy-move, JPEG compression, Gaussian noise, and scaling. The maximum number of fitness evaluation is 500 and the population size is 50. The duplicated regions will be translated as follows:

i) Plain copy-move: The duplicate region is moved to the target location without any additional modification.

ii) Add Gaussian noise: The images intensities are normalized to the value of 0 and 1 and include zero mean Gaussian noise with standard deviations of 0.02, 0.04, 0.06, 0.08 and 0.10 to the duplicated regions.

iii) JPEG compression: JPEG compression is a common global disturbance. The quality factor fluctuated in the vicinity of 100 and 20 in the steps of 10 degrees.

iv) Scaling: The duplicated regions are rescaled by 40%, 60%, 80%, 100%, 120%, 140%, 160%, 160% and 200%.

Experiments are performed to calculate parameters given by Eq. 14 and 15. Table II indicates precision, recall and F_1-score for proposed and distinctive existing strategies based on DB-1 and our proposed method has average precision, recall and F_1-score 96.13, 92.3 and 94.18 respectively. This was obtained, when we have performed a blind analysis on DB-1, containing an unknown mixture of genuine and tampered images. Fig. 5 shows the comparison between proposed CMFD-CS and existing methods when adding Gaussian noise. According to Fig. 5, our proposed method shows better precision and recall values than the existing algorithms and these values would be reduced, when we include zero mean Gaussian noise with standard deviations of 0.02, 0.04, 0.06, 0.08 and 0.10 to the duplicated regions. Fig. 6 shows the comparison between proposed CMFD-CS and existing methods when JPEG compression performed. For plain copy-move forgery, when JPEG compression has not performed, our proposed method has better precision and recall values than the existing methods and its values have reduced when quality factor fluctuated between 100 and 20 in the steps of 10 degrees. Fig. 7 demonstrates the comparison between proposed CMFD-CS and existing methods when scaling performed. For plain copy-move forgery, when scaling has not performed, then precision and recall have highest values but its values reduced to lower values when duplicate regions have rescaled by the factor of 40%, 60%, 80%, 120%, 140%, 160%, 160% and 200%.



Fig. 8:.Some Examples of Original Images Are placed in the First Column; Their Tampered Images Appear in the Second Column and the Corresponding Detection Results Are Reported in the Third Column Based on DB-2.

b) MICC-F600 (DB-2): MICC-F600 dataset is formed by 440 unique images, 160 altered images, and 160 ground truth images. A few cases of unique images, tampered images, and their detection results are shown in Fig. 8 based on DB-2. Table III indicates precision, recall, and F1-score for proposed and distinctive existing strategies based on DB-2 and average precision, recall, and F1-score of our proposed method are 93.25, 90.47 and 91.84 respectively. Fig. 9 shows

the comparison between proposed CMFD-CS and existing algorithms when adding Gaussian noise. According to Fig. 9, our proposed method shows better precision and recall than the existing algorithms and their values would be decreased, when we include zero mean Gaussian noise with standard deviations of 0.02, 0.04, 0.06, 0.08 and 0.10 to the duplicated regions. Fig. 10 shows the comparison between proposed CMFD-CS and existing methods when JPEG compression performed. For plain copy-move forgery, when JPEG compression has not performed, our proposed method has better precision and recall value than the existing methods and its value has reduced, when quality factor fluctuated between 100 and 20 in the steps of 10 degrees. Fig. 11 demonstrates the comparison between proposed CMFD-CS and existing methods when scaling performed. For plain copy-move forgery, when scaling has not performed, then precision and recall have highest values but its values reduced to lower values when duplicate regions have rescaled by the factor of 40%, 60%, 80%, 120%, 140%, 160%, 160% and 200%.

Table 3: Detection Results of Plain Copy-Move Forgery Based on Db-2

Methods	Precision (%) Recall (%) F1 (%)		
Babak [12]	87.65	85.37	86.49
Fridrich [13]	87.89	86.65	87.26
Popescu [15]	88.67	87.36	88.01
Kang [17]	89.54	86.12	87.79
Bayram [18]	88.12	86.59	87.35
Lin [20]	88.65	87.65	88.15
Huang [26]	89.75	88.54	89.14
Zhang [27]	90.65	89.12	89.88
Wave. Dec. [29]	91.78	89.85	90.80
Proposed CMFD-CS	93.25	90.47	91.84

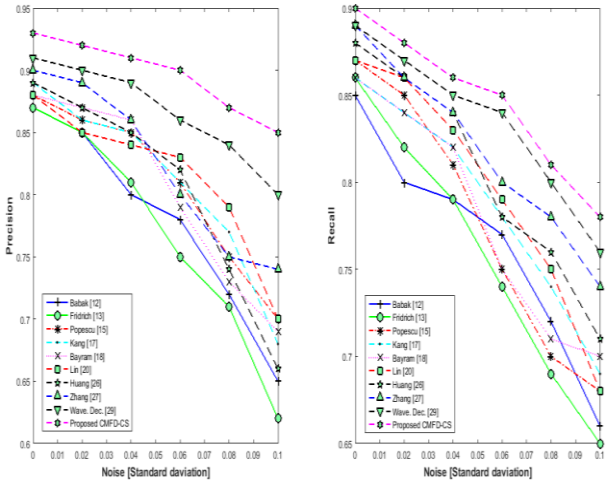


Fig. 9: Comparison between Proposed CMFD-CS and Exiting Algorithms, when Adding Gaussian Noise Based on DB-2.

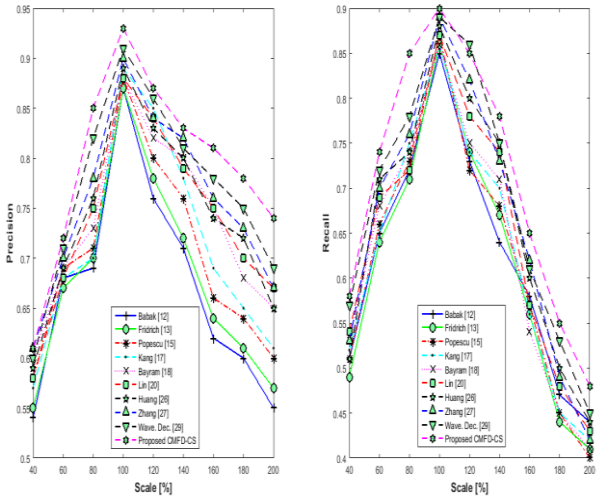


Fig. 11:.Comparison between Proposed CMFD-CS and Exiting Algorithms, when Performed Scaling Based On DB-2.

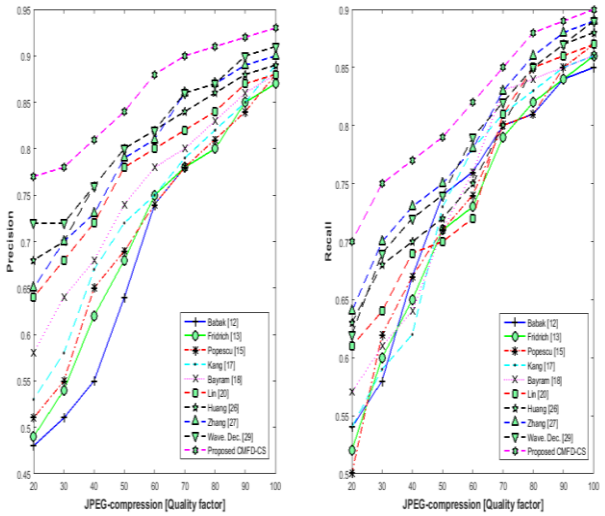


Fig. 10:.Comparison between Proposed CMFD-CS and Exiting Algorithms, when Performed JPEG Compression Based on DB-2.

c) MICC-F2000 (DB-3): MICC-F2000 dataset is created by 2000 images, in which 700 are tampered and 1300 original images. Some examples of original images, tampered images, and their detection results are shown in Fig. 12 based on DB-1. Table IV shows precision, recall and F1-score for proposed and distinctive existing strategies based on DB-3 and average precision, recall and F1-score of our proposed method are 95.87, 92.59 and 94.20 respectively. Fig. 13 shows the comparison between proposed CMFD-CS and existing methods, when adding Gaussian noise. Precision and recall of proposed method have better results and its values would be reduced, when we include zero mean Gaussian noise with standard deviations of 0.02, 0.04, 0.06, 0.08 and 0.10 to the duplicated regions. Fig. 14 shows the comparison between proposed CMFD-CS and existing methods when JPEG compression performed. For plain copy-move forgery, when JPEG compression has not performed, our proposed method has better precision and recall values than the existing methods and its values have reduced when quality factor fluctuated between 100 and 20 in the steps of 10 degrees. Fig. 15 demonstrates the comparison between proposed CMFD-CS and existing methods when scaling performed. For plain copy-move forgery, when scaling has not performed, then precision and recall have highest values but its values reduced to lower values when duplicate regions have rescaled by the factor of 40%, 60%, 80%, 120%, 140%, 160%, 160%

and 200%. From Table II-IV and Fig. 7-15, it has been observed that the results of our proposed algorithm are superior to the existing methods such as Babak [12], Fridrich [13], Popescu [15], Kang [17], Bayram [18], Lin [20], Huang [26], Zhang [27] and Wave. Dec. [29]. Finally, we can say that our proposed method performs better with the datasets, where block based methods have worse results.

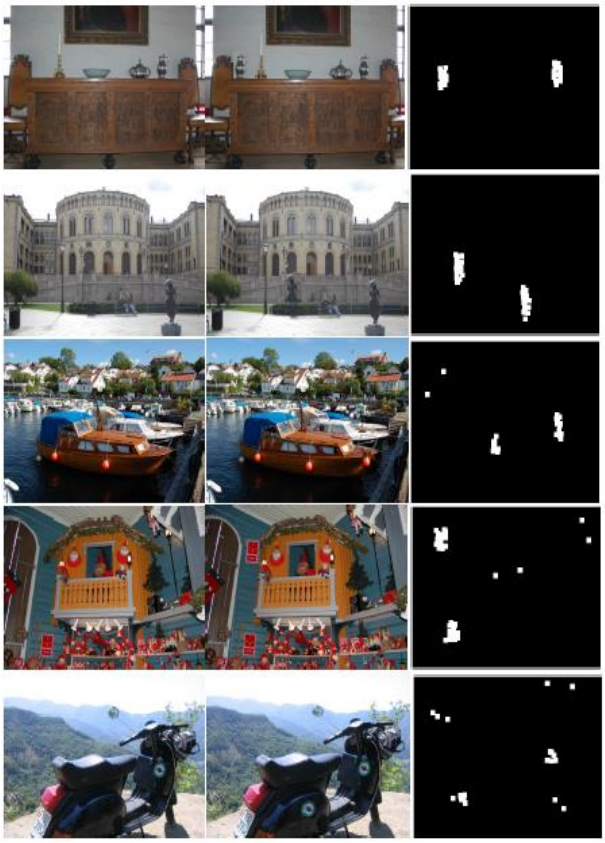


Fig. 12:.Some Examples of Original Images Are placed in the First Column; Their Tampered Images Appear in the Second Column and the Corresponding Detection Results Are Reported in the Third Column Based on DB-3.

Table 4: .Detection Results of Plain Copy-Move Forgery Based on Db-3

Methods	Precision (%)	Recall (%)	F1 (%)
Babak [12]	89.54	84.35	86.87
Fridrich [13]	92.31	85.72	88.89
Popescu [15]	86.47	82.79	84.59
Kang [17]	89.57	85.64	87.56
Bayram [18]	90.46	86.78	88.58
Lin [20]	91.52	87.21	89.31
Huang [26]	87.58	91.28	89.39
Zhang [27]	86.78	89.42	88.08
Wave. Dec. [29]	93.42	90.65	92.01
Proposed CMFD-CS	95.87	92.59	94.20

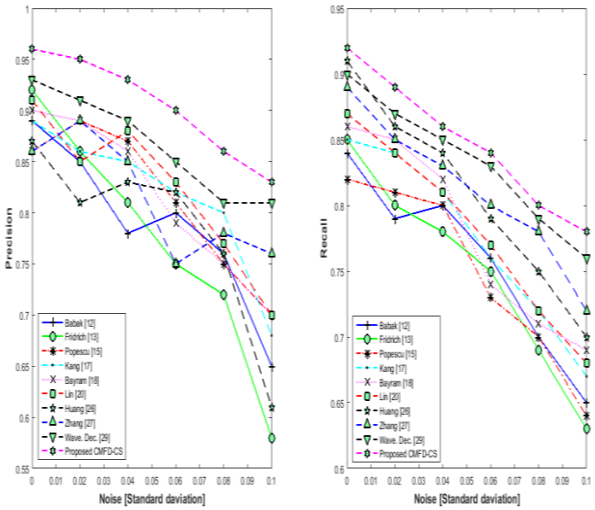


Fig. 13:.Comparison Between Proposed CMFD-CS and Exiting Algorithms, when adding Gaussian Noise Based onDB-3.

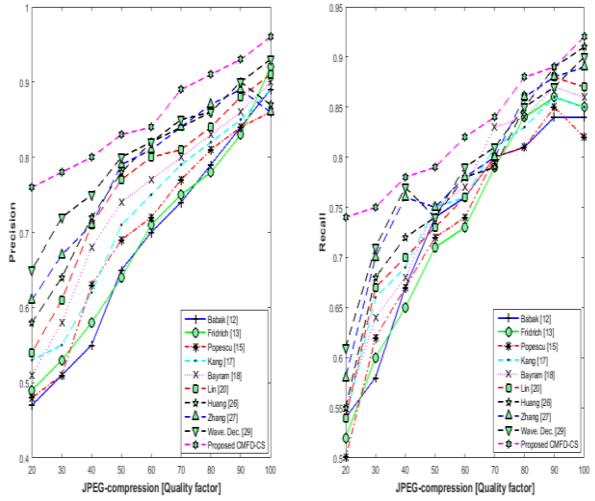


Fig. 14:.Comparison between Proposed CMFD-CS and Exiting Algorithms, When Performed JPEG Compression Based on DB-3.

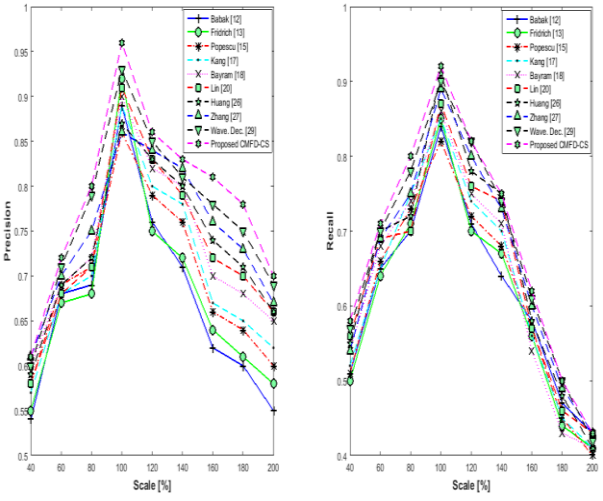


Fig. 15: Comparison between Proposed CMFD-CS and Exiting Algorithms, when Performed Scaling Based on DB-3.

5. Conclusion and scope for future work

In this paper, we propose a novel approach CMFD-CS to identify copy-move forgery in the digital images. Comparing with existing work, this paper makes three contributions. (i) It advances the idea of applying the CS algorithm to recognition of copy-move forgery.

(ii) It incorporates the CS algorithm into the block-based framework to perform copy-move forgery detection. (iii) It separates principles to automatically decide customized parameter values for the given images that are to be detected. Experimental results show that CMFD-CS can automatically generate customized parameter values for doctored images. This is independent of neither experiences nor experiments. CMFD-CS can accomplish much better results than the existing techniques. It can recognize matched points that its counterpart can't, and it can drastically build the number of true matched blocks, which make the detection of the duplicated region more accurate and more acceptable. Although CMFD-CS is applicable to most of the copy-move forged images, but we observe that the block based framework methods can't find reliably matched blocks in uniform texture regions or when the duplicate regions are too small.

Conflict of interest

The author confirms that this article content has no conflict of interest.

References

[1] 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, Dec. 2012.

[2] S. Wenchang, Z. Fei, Q. Bo and L. Bin, "Improving image copy-move forgery detection with particle swarm optimization techniques," in Proc. in China Communications, vol. 13, no. 1, pp. 139-149, Jan. 2016.

[3] Z. Moghaddasi, H. A. Jalab and R. M. Noor, "SVD-based image splicing detection," in Proc. IEEE Int. Conf. Image Processing (ICIP), Singapore, Oct. 24-27, 2004, Vol.2, pp. 1169-1172.

[4] G. Gul and F. Kurugollu, "SVD-Based Universal Spatial Domain Image Steganalysis," IEEE Transactions on Information Forensics and Security, vol. 5, no. 2, pp. 349-353, June 2010.

[5] Baker, K., "Singular value decomposition tutorial," The Ohio State University, 2005.

[6] Rahul Pandit; Nindhiya Khosla; Gurjeet Singh; Hiteshwari Sharma, "Image Compression and Quality Factor in case of JPEG Image Format," International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 7, July 2013.

[7] X. S. Yang and Suash Deb, "Cuckoo Search via Levy flights," in World Congress on Nature and Biologically Inspired Computing, (NaBIC) 2009, Coimbatore, 2009, pp. 210-214.

[8] S. Tian et al., "Application of Cuckoo Search algorithm in power network planning," in Proc. IEEE 5th Int. Conf. Electric Utility Deregulation and Restructuring and Power Technologies (DRPT), 2015, Changsha, 2015, pp. 604-608.

[9] H. Rakhshani, A. Rahati and E. Dehghanian, "Cuckoo search algorithm and its application for secondary protein structure prediction," in Proc. IEEE 2nd Int. Conf. Knowledge-Based Engineering and Innovation (KBEI), 2015, Tehran, 2015, pp. 412-417.

[10] Q. Liu , A. Sung, M. Qiao, Z. Chen and B. Ribeiro, "An Improved Approach to Steganalysis of JPEG Images," in Information Sciences, 180 (9), pp. 1643-1655, 2010.

[11] H. Farid, "Image forgery detection," IEEE Signal Processing Magazine, vol. 26, no. 2, pp. 16-25, March 2009.

[12] Babak Mahdian; Stanislav Saic, "Detection of copy-move forgery using a method based on blur moment invariants," in Forensic Science International, vol. 171, nos. 23, pp. 180-189, Sep. 2006.

[13] J. Fridrich, D. Soukal, and J. Lukas, "Detection of copy-move forgery in digital images," in in Proc. Digit. Forensic Res. Workshop (DFRWS), Cleveland, OH, USA, 2003, pp. 134-137.

[14] J. Flusser and T. Suk, "Degraded image analysis: an invariant approach," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, no. 6, pp. 590-603, Jun 1998.

[15] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," in Dept. Comput. Sci., Dartmouth College, Hanover, NH, USA, Tech. Rep. TR, 2004.

[16] Khodayari Bavil, A., Razavi, S.E., On the thermo-flow behavior in a rectangular channel with skewed circular ribs, Mechanics & Industry, 18 2 (2017) 225, https://doi.org/10.1051/meca/2016057.

[17] X. Kang and S. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics," in in Proc. Int. Conf. Comput. Sci. Softw. Eng., vol. 3. Dec. 2008, pp. 926-930.

[18] S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in in Proc. IEEE Int. Conf. Acoust, Speech Signal Process. (ICASSP), Apr. 2009, pp. 1053-1056.

[19] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of resampling," IEEE Transactions on Signal Processing, vol. 53, no. 2, pp. 758-767, Feb. 2005.

[20] H.J. Lin, C.W. Wang, and Y.T. Kao, "Fast copy-move forgery detection," in WSEAS Trans. Signal Process., vol. 5, no. 5, pp. 188-197, May 2009.

[21] Khan, S.; Kulkarni, A., "Robust method for detection of copy-move forgery in digital images," in Proc. IEEE Int. Conf. Signal and Image Processing (ICSIP), 15-17 Dec. 2010, pp.69-73.

[22] Barni, M.; Costanzo, A.; Sabatini, L., "Identification of cut and paste tampering by means of double-JPEG detection and image segmentation," in Proceedings of 2010 IEEE International Symposium on Circuits and Systems (ISCAS), May 30 2010-June 2 2010, pp. 1687-1690.

[23] Li, Weihai, Yuan Yuan, and Nenghai Yu.,"Detecting copy-paste forgery of jpeg image via block artifact grid extraction," in International Workshop on Local and Non-Local Approximation in Image Processing, 2008.

[24] Ardizzone, Edoardo, Alessandro Bruno, and Giuseppe Mazzola. "Copy-move forgery detection via texture description," in Proceedings.
Of the second ACM workshop on Multimedia in forensics, security and intelligence, ACM, 2010.

[25] Mo Chen; Fridrich, J.; Goljan, M.; Lukas, J., "Determining Image Origin and Integrity Using Sensor Noise," IEEE Trans. Information Forensics and Security,, vol.3, no.1, pp.74,90, March 2008.

[26] Huang, Y., Lu, W., Sun, W., et al., "Improved DCT-based detection of copy-move forgery in images," in Forensic Sci. Int., 2011, 206, (1), pp. 178-184.

[27] Zhang, J., Feng, Z., Su, Y., "A new approach for detecting copy-move forgery in digital images," in 11th IEEE Singapore Int. Conf. on.
Communication Systems, 2008, pp. 362-366.

[28] H. Farid, "Photo Fakery and Forensics," in In Advances in Computers, Volume 77, 2009.

[29] Kashyap, Abhishek; Joshi, Shiv Dutt, "Detection of copy-move forgery using wavelet decomposition," in Proc. IEEE Int. Cof. Signal Processing and Communication (ICSC), Noida, Dec.12-14, 2013, pp.396-400.

[30] Jiwani, L.K.; Joshi, S.D.; Visweswaran, G.S., "Spectral Density Driven Wavelet Representation of 2-D Images," in Proc. IEEE Int. Symposium Signal Processing and Information Technology, Aug. 2006, pp. 138-143.

[31] Kashyap, Abhishek; B. Suresh; Agrawal, Megha; Gupta, Hariom; Joshi, Shiv Dutt, "Detection of splicing forgery using wavelet decomposition," in Proc. IEEE Int. Conf. Computing, Communication and Automation (ICCCA 2015), 15-16 May 2015.

[32] Mahdian, Babak; Saic, Stanislav, "Blind Authentication Using Periodic Properties of Interpolation," IEEE Trans. Information Forensics and Security, vol.3, no.3, pp.529-538, Sept. 2008.

[33] Khosravi M., Mosaddeghi F., Oveisi, M., khodayari-b, A., Aerodynamic drag reduction of heavy vehicles using append devices by CFD analysis, Journal of Central South University, Volume 22, 2015, pp 4645–4652.

[34] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, G. Serra, "A SIFT-based forensic method for copy-move attack detection and transformation recovery," IEEE Transactions on Information Forensics and Security, vol. 6, issue 3, pp. 1099-1110, 2011.