KICS The Korean Institute of Communications and Information Sciences

Available online at www.sciencedirect.com

ScienceDirect

ICT Express 8 (2022) 244–249

www.elsevier.com/locate/icte

An optimized technique for copy–move forgery localization using statistical features

S B G Tilak Babu[a,b,*], Ch Srinivasa Rao[c]

[a] *Department of ECE, JNTUK, Kakinada, India*
[b] *Department of ECE, Aditya Engineering College, Surampalem, India*
[c] *Department of ECE, JNTUK UCEV, Vizianagaram, India*

Received 22 March 2021; received in revised form 7 May 2021; accepted 11 August 2021
Available online 26 August 2021

Abstract

Copy–Move Forgery Detection (CMFD) helps to detect copied and pasted areas in one image. It plays a crucial role in legal evidence, forensic investigation, defence, and many more places. In the proposed CMFD method, a two-step identification of forgery is presented. In step one, the suspected image will be classified into either one of two classes that are forged or authentic. Step two is carried out only if the suspected is classified as forged, then forged location will be identified using the block-matching procedure. Initially, the suspected image is decomposed into different orientations using Steerable Pyramid Transform (SPT); Grey Level Co-occurrence Matrix (GLCM) features are extracted from each orientation. These features are used to train Optimized Support Vector Machine (OSVM) as well as to classify. If the suspected image is categorized into forged, then the suspected grey image is converted into overlapping blocks, and from each block, GLCM features are extracted. The proper similarity threshold value and distance threshold value can locate the forged region using GLCM block features. The performance of the proposed method is tested using standard datasets CoMoFoD and CASIA Datasets. The proposed CMFD approach results are consistent, even the forged image suffered from attacks like JPEG compression, scaling, and rotation. The OSVM classifier is showing superiority over the Optimized Naive Bayes Classifier (ONBC), Extreme Learning Machine (ELM) and Support Vector Machine (SVM).

Keywords: CMFD; Copy paste forgery detection; Image cloning detection; SPT; GLCM; OSVM

1. Introduction

With the fast development in image processing technology, digital image manipulation becomes much easier for an inexperienced counterfeiter with the aid of some simple-to-use photo editing tools, such as Adobe Photoshop and Gimp. Digital image integrity and authenticity must be safeguarded in time to prevent copyright issues, fraud, and misleading modifications. Copy–Move Forgery (CMF) is one of the increasing falsifications of the numerous digital image falsifications. Copy–Move Forgery Detection (CMFD) helps to identify copied and pasted places in one image. It plays a crucial role in legal testimony, forensic analysis, and much more. The example of CMF image can be observed in Fig. 1. There are three different conventional CMFD techniques available in the literature: block matching, Keypoint matching, and classification methods [1–5]. In block-based CMFD, the suspected image will be converted into overlapping/non-overlapping blocks. From these overlapping/non-overlapping blocks, features will be extracted using feature extractors, the extracted features will be sorted and compared for similarity. Finally, similar blocks will be identified and mapped as copy–move forged areas.

The Copy–Move Forgery Detection using block-matching started by J. Fridrich et al. [6] In this, the suspected image's overlapping blocks are given to Discrete Cosine Transform to obtain the feature set. These overlapping block features are arranged in a matrix and lexicographically sorted. In this sorted matrix, similarity identified among feature sets (rows of the matrix) and similar features (rows/overlapping blocks) are marked as forged. To overcome the drawback in Fridrich

* Corresponding author at: Department of ECE, Aditya Engineering College, Surampalem, India.
E-mail addresses: thilaksayila@gmail.com (S.B.G.T. Babu), chsrao.ece@jntukucev.ac.in (C.S. Rao).

Peer review under responsibility of The Korean Institute of Communications and Information Sciences (KICS).

https://doi.org/10.1016/j.icte.2021.08.016

(a) (b) (c)

Fig. 1. Example for copy–move forgery (a) Original image (b) Copy–Move forged image (c) forged region marked image.

et al. method, Popescu [7] updated literature of CMFD using Principal Component Analysis (PCA) with reduction of the number of computations and time, but two methods are further replaced with updations to computations, speed, and accuracy of detection.

SURF Keypoint features-based hybrid CMFD method is in literature from Badal Soni et al. [8]. This method is computationally high as to the block-based method and consumes more time than conventional keypoint-based CMFD methods. Optimization is essential in any methodology. SIH Wenchang et al. [9] proposed Particle Swarm Optimization (PSO) and Keypoint dependent detection method for CMF, PSO outperformed conventional keypoint methods. A block matching method was proposed in 2018 by Chen et al. [10]. The algorithm is tested on FAU and GRIP datasets. In continuation, Chen et al. [11] extended his work, and his method improved efficiency, but it consumed much time in producing the localized map. Mahmood et al. [12] used UCID V2, CoMoFoD datasets. They converted RGB suspected image into YCbCr to select a better image instead of a grey image, as grey image Luminance (Y) manipulations are sensitive to human eyes, so attackers take care and manipulate in Chrominance channels. Here, the suspected image's chrominance components are given to SWT, and the decomposed part is given to DCT to extract the features set. These features are sorted and similarity is verified using thresholding methods. Falsely matched blocks are removed using morphological operators. The method [13] uses a Doubly Stochastic Model (DSM) and Extreme Learning Machine (ELM) for classifying a suspected image to either authentic or forged class. This method outperformed SVM but not OSVM.

To address these challenges, a two times forgery verification methodology is proposed in this paper. The suspected image was initially classified as one of the two forged or authentic types. Step two shall be carried out only where the suspected image has been listed as forged, so a counterfeit position is found by block matching. The computational time is reduced if the image is authentic and confirmation is also taken using block matching if the suspected image is classified as forged. The paper is set as follows, existing literature with its pros and cons are discussed in Section 1. The proposed work is described with a flow diagram in Section 2, the results of the proposed work are presented in Section 3. Finally, conclusions are given from the experience of experimentation along with future directions in Section 4.

2. Proposed work

Manipulations in intensities or luminance components are easy to identify by the human eye, so attackers concentrate on manipulating the chrominance components. In the proposed work, the suspected RGB image is converted into YCbCr. The chrominance components are given to SPT to obtain various orientations. From each orientation, GLCM features are extracted for further simplification of the process. These extracted features are concatenated side by side of a single suspected image for making a feature set. These feature sets are given to Optimized Support Vector Machine for training. After training, a feature set of a suspected image is given to OSVM [14,15] Classifier to classify whether the suspected image is authentic or forged. If the image is classified as authentic, then no further process is continued. If the image is classified into forged, then the identification of the forged area process will start. In the first step of localization [16,17], the original suspected image was converted into grey, and was divided into overlapping blocks. GLCM features are extracted from each overlapping block. This block feature set end is the appended block number for further reference, then a matrix using all block feature sets is made. This matrix is sorted using lexicographical sorting. The similarity is observed using distance metrics among sorted rows, and similar blocks are marked as copy–move forged. False matches are removed using the windowing method and morphological operators. Various steps of the proposed CMFD can be observed in Fig. 2.

2.1. SPT

Analysing the suspected image in various orientations is necessary as attackers take care to show an image as the original image, so the chrominance component is given to SPT and collected a required number of orientations from SPT. Three significant constraints must be satisfied by filters for angular and radial decompositions, so the SPT has the possibility of rotated orientation bands and free from aliasing in subbands [18]. The constraints are mentioned here.

- For recursive nature the condition is

$$|L_1(w/2)|^2 = |L_1(w/2)|^2[|L_1(w)|^2 + |B(w)|^2]$$

- For flat response in system it should follow

$$|H_0(w)|^2 + |L_0(w)|^2[|L_1(w)|^2 + |B(w)|^2] = 1$$

- For preventing aliasing in subbands, the condition is

$$L_1(w) = 0 \quad for \quad |w| > \pi/2$$

Here H_0 and L_0 represent highpass and lowpass filters, respectively, on scale zero of SPT. Subbands in k-orientations ($2\pi/k$) can get using directional operators ($B_k(w)$). L_1 is the scaled version of L_0; using a directional operator, one can get k-oriented subbands. The SPT source code is available at http://www.cns.nyu.edu/~eero/steerpyr/.

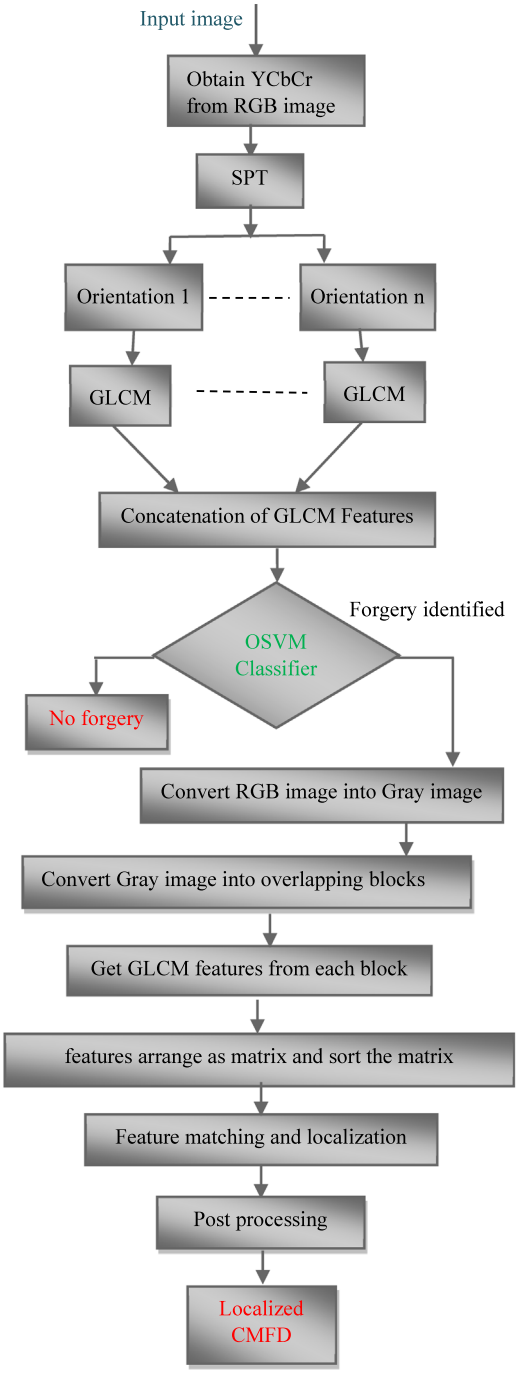


Fig. 2. Flow diagram of proposed algorithm.

2.2. GLCM

GLCM is a texture feature extractor in images using second-order statistical methods [19,20]. Initially, it calculates the co-occurrence matrix, from it measures various features such as contrast, entropy, energy, homogeneity, variance, and correlation. Among all these features, four essential features are considered for this work: contrast, correlation, energy, and homogeneity.

$$Contrast = \sum_{i,j=0}^{N-1} \left(P_y\,(i-j)\,\hat{}\,2\right)$$

$$Entropy = \sum_{i,j=0}^{N-1} \left(\frac{P_y}{1+(i-j)\,\hat{}\,2}\right)$$

$$Energy = \sum_{i,j=0}^{N-1} (P_y)\,\hat{}\,2$$

$$Correlation = \frac{\sum_{i,j=0}^{N-1} \left(P_y\,(i-\mu)\,(j-\mu)\right)}{\sigma^2}$$

These extracted features of all orientations of a single image are concatenated into a row. The entire training dataset image features are set like this and made a matrix. This matrix and another label matrix are used to train the Optimized Support Vector Machine. The command 'fitcsvm' in MATLAB has the flexibility to optimize hyperparameters automatically.

Once the training is finished, the suspected image's orientations are obtained using SPT. GLCM features will be extracted from these orientations. All these orientation features are concatenated and set as a single row and given to 'predict' to verify authenticity. The classifier classifies the suspected image into either an authentic or copy–move forged image. If the classifier result is authentic, the process is stopped there; otherwise, the localization process will be carried out on the forged image.

2.3. Localization of forgery

Initially, the suspected image of M*N is converted into a Greyscale image of the same size. The grey image is segmented into overlapping blocks with the size of S*S. The selected square block size 'S' must be less than the size of the forged region. If it is higher than the forged region, the detection probability is very minor. If the grey image of M*N is converted into overlapping blocks of each block size S*S, then the number of overlapping blocks is (M-S + 1) * (N-S + 1). From each block, GLCM features are extracted using the GLCM feature extraction procedure. Each block's features are arranged as a row and are numbered each block feature at the end of the respective row for easy identification. A matrix 'M' is formed using these rows, and this matrix is sorted using lexicographical sorting.

As feature matrix (M) is sorted so similar rows (similar blocks) will set near, for verifying similarity among all blocks no need of verifying similarity among all rows because verifying similarity among similar rows is sufficient. Each row starting from the first row compared to the next 'R' rows, and the sorted matrix is marked as M_s. While calculating similarity among rows, the distance between overlapping blocks is also considered, and it must be greater than overlapping block size 'S'. A distance threshold is considered 'T_d', which must be greater than or equal to overlapping block size 'S'. For verifying similarity among blocks, the similarity threshold is considered 'T_s', which must be significantly less. The similarity and distance among blocks are measured using Euclidean

Table 1
Block size versus number of blocks.

Dataset/Overlapping block size (S)	S = 8	S = 12	S = 15	S = 18
CASIA dataset (384 × 256)	93 873	91 385	89 540	87 713
CoMoFoD dataset (512 × 512)	255 025	251 001	248 004	245 025

distance. The parameters T_s, T_d and S are determined by continuous repeating procedure on mentioned datasets. The matching procedure in feature matrix M starts from the first row, if row 'α' is compared with row 'β', then distance D (α, β) is Euclidean distance between features of these two rows. As each row of M_s is marked with overlapping block details, the distance between two blocks is easily measured using the Euclidean distance metric. Apart from overlapping block details, the remaining features are used to measure the similarity between them.

All matched rows (blocks) will be stored in a separate set (ϕ) for marking results. Initially, an image (I_m) of size equal to suspected image size M*N is formed with zero values. The proposed algorithm marks the matched blocks on I_m with white patches of size overlapping block size (S*S) in respective locations using matched overlapping blocks details. In the process of identifying similar regions, there is a possibility of false matches occurring. Also, these false matches are removed using morphological operators like erosion and dilation on I_m. Here morphological erosion is performed first, and then morphological dilation operation is performed; in both dilation and erosion, the structuring element of the same size is considered.

3. Results and discussions

This section provides complete details of experimentation setup and results in analysis. For testing the proposed methodology, the images are considered from CoMoFoD, CASIA Datasets, and other forged images created by authors. Most of the CASIA dataset images have the exact size of 384 × 256, but very few vary. The CASIA images considered for evaluation of the proposed method are of the same size 384 × 256. All the images in the CoMoFoD dataset are of 512 × 512 size. The authenticated images for creating forged images by authors are taken from CASIA Dataset with size 384 × 256.

The whole experimentation was carried out on MATLAB 2018 version in a personal laptop with AMD A9 processor with 3.10 GHz speed and 8 GB RAM, 64-bit Windows 10 operating system. In the experimentation, the first step is to train OSVM. Before training the training-dataset needs to be extracted and arranged in proper order. Initially, the training images/suspected images are converted to YCbCr for obtaining chrominance channels. In two chrominance channels, the chrominance blue (Cb) channel is used for further analysis. From Cb, different orientations are obtained using SPT. Here, the number of scales is only one, and the number of orientations is five. Every training image/suspected image will have one low-frequency component band and five-band passed frequency bands. GLCM features are extracted from these six bands and formed a row for a single image that means this feature row contains concatenated features of all orientations. The rows of all training images are arranged to form a matrix to give 'fitcsvm'. 'Fitcsvm' is a command in MATLAB used to train SVM. The command supports Sequential Minimal Optimization (SMO) and various kernel functions with simple command parameter variations. Once the training is finished, similar to training, the suspected image GLCM features are also extracted. These features are given to the command 'predict'. This command classifies the given suspected image features either into authentic image class or copy–move forged image class. If the classified class is authentic, the process is ended, and the result is displayed as the given image is an authentic image. If the classified class is a copy–move forged image class, then locating the forged region starts, that is localization process starts.

In the Localization process, the overlapping block size S value is varied from 8 to 18. The total number of blocks obtained after dividing the suspected image with various S values is provided in Table 1. From each overlapping block, GLCM features are obtained, and matrix M is formed. The sorted matrix M_s is obtained by lexicographical sorting of the matrix M. The number of rows in matrices M and M_s is equal to the total number of overlapping blocks given in Table 1. The overlapping block size should be less than the forged area. As the forged area is not known here, overlapping block size is varied. The threshold of similarity T_s value is varied between 0.1 to 1.5, and the threshold of distance T_d is 40.

If the suspected image is given to the OSVM classifier, the optimized binary classifier results in an image with its class heading. This proposed CMFD classifier is tested with various kinds of images such as images with texture, images with animals, images with birds, and images of human beings.

3.1. Performance measures

The proposed method performance is measured with different evaluation metrics such as True Positive Rate (TPR), True Negative Rate (TNR), False Positive Rate (FPR), False Negative Rate (FNR).

$$TPR = (True\ Positive)/(True\ Positive + False\ Negative)$$

$$FNR = (False\ Negative)/(False\ Negative + True\ Positive)$$

$$TNR = (True\ Negative)/(False\ Positive + True\ Negative)$$

$$FPR = (False\ Positive)/(False\ Positive + True\ Negative)$$

The number of tampered images detected as tampered is True Positive (TP), and the number of tampered images mistakenly detected as authentic is False Negative (FN), the number of authentic images mistakenly detected as tampered images is False Positive (FP), and the number of authentic images detected as authentic is True Negative (TN).

The evaluation of the proposed method is done in various conditions. The proposed method tested for plain CMF

Table 2
Performance measures of proposed GLCM+OSVM algorithm (Stage 1 performance)

Type of attack	Attack quantity	Proposed method				GLCM+SVM [19]		DSM+ELM [13]		GLCM+ONBC [21]	
		TPR%	TNR%	FPR%	FNR%	TPR%	FNR%	TPR%	FNR%	TPR%	FNR%
No attack	–	99	99	1	1	98	2	99	1	98	2
Rotated angle	3	94	92	8	6	93	7	93	7	94	6
	5	85	84	16	15	85	15	84	16	86	14
	10	81	81	19	19	78	22	79	21	80	20
	45	71	72	28	29	73	27	72	28	75	25
Scale	85	78	83	17	22	77	23	78	22	76	24
	90	82	83	17	18	85	15	85	15	80	80
	95	86	87	13	14	86	14	86	14	82	18
	105	87	86	14	13	87	13	86	14	86	14
Brightness variation	85	84	83	17	16	80	20	81	19	79	21
	90	88	89	11	12	84	16	86	14	81	19
	95	89	89	11	11	85	15	88	12	83	17
	105	90	91	9	10	88	12	88	12	86	14
JPEG quantization	90	92	92	8	8	98	2	96	4	98	2
	80	90	90	10	10	98	2	94	6	98	2
	70	88	88	12	12	89	11	89	11	90	10
	60	82	82	18	18	78	22	79	21	78	22

Table 3
CMF localization results on plain CMF images.

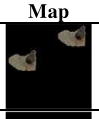
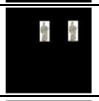
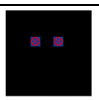
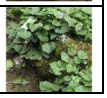
S No	Forged Images	Binary Map	Region Map	Authentic Image
1				
2				
3				
4				
5				
6				
7				

Table 4
CMF localization results on post processing attacked images.

Attack Type	Forged Images	White Patch Map	Region Map	Authentic Image
Rotation 10°				
Rotation 45°				
Scale 95%				
Scale 105%				
Bright 90%				
JPEG Q-90				

images as well as post-processing attacks underwent images. The post-processed image is obtained by varying brightness or Scale or Rotation or JPEG Quantization in the forged image. The proposed method performance measures up to classification (stage 1) and is presented in Table 2.

The proposed CMFD algorithm shows the best results if the suspected image is unattached by any post-processing methods. The proposed method is also tested on suspected images which have even undergone some post-processing attacks, and the results show robustness over existing methods [13,19,21].

If the suspected image is classified into CMF, then the localization process is carried out on the suspected image. In this forgery localization, the initial detected result is a binary mapped image with suspected image size. Later the contents of copied and pasted regions are also mapped on a binary map. The results of copy–move forgery localization on images without any post processing attacks are presented in Table 3. The results of copy–move forgery localization on images with post processing attacks such as brightness variation or Scale change or Rotation of an angle or JPEG Quantization are presented in Table 4.

In Tables 3 and 4, a binary map is presented, it represents forged locations in white colour, and authentic regions remain in the black. In the region map image, the white regions in the binary map are replaced by regions in the suspected image. Here, the forged image can be compared with the authentic image. The main drawback in classification type

CMFD [19,21] is the localization of the forged location. It is addressed in the proposed algorithm.

4. Conclusions

A two-step forgery detection method is proposed in this paper. In step one, the proposed method classifies the given suspected image into an authentic or forged image. Step two is an optional step carried out on the suspected image classified as forged and used to locate the forged regions. In step two, the alleged image is converted into overlapping blocks. From each block, GLCM features are extracted, and matrix M is formed. The matrix M_s is obtained from M. The proper similarity threshold value and distance threshold value can locate the forged region using M_s. CoMoFoD, and CASIA Datasets are used to evaluate the proposed method's performance. The proposed method's performance shows robustness even if the forged image undergoes post-processing attacks like JPEG compression, scaling, and rotation. In comparison with state-of-the-art, OSVM is superior over ONBC, ELM and SVM. The future idea is to modify the proposed algorithm to test whether image is either authentic or computer-generated image.

CRediT authorship contribution statement

S B G Tilak Babu: Methodology, Software, Validation, Formal analysis, Investigation, Writing – original draft. **Ch Srinivasa Rao:** Conceptualization, Resources, Writing – review & editing, Supervision, Project administration.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] W.D. Ferreira, C.B.R. Ferreira, G. da Cruz Júnior, F. Soares, A review of digital image forensics, Comput. Electr. Eng. 85 (2020) 106685, http://dx.doi.org/10.1016/j.compeleceng.2020.106685.

[2] R. Thakur, R. Rohilla, Recent advances in digital image manipulation detection techniques: A brief review, Forensic Sci. Int. 312 (2020) 110311, http://dx.doi.org/10.1016/j.forsciint.2020.110311.

[3] Y. Rao, J. Ni, H. Xie, Multi-semantic CRF-based attention model for image forgery detection and localization, Signal Process. (2021) 108051, http://dx.doi.org/10.1016/j.sigpro.2021.108051.

[4] J. Ouyang, Y. Liu, M. Liao, Robust copy-move forgery detection method using pyramid model and Zernike moments, Multimedia Tools Appl. 78 (8) (2019) 10207–10225, http://dx.doi.org/10.1007/s11042-018-6605-1.

[5] G. Ramu, S.B.G.T. Babu, Image forgery detection for high resolution images using SIFT and RANSAC algorithm, in: 2017 2nd International Conference on Communication and Electronics Systems (ICCES), Vol. 2018-Janua, 2017, pp. 850–854, http://dx.doi.org/10.1109/CESYS.2017.8321205.

[6] J. Fridrich, D. Soukal, J. Lukáš, Detection of copy-move forgery in digital images, in: Digital Forensic Forensic Research Workshop, 2003.

[7] A.C. Popescu, H. Farid, Exposing Digital Forgeries By Detecting Duplicated Image Regions, Technology Report TR2004-515, Department Computer Science, Dartmouth College, 2004.

[8] B. Soni, P.K. Das, D.M. Thounaojam, Geometric transformation invariant block based copy-move forgery detection using fast and efficient hybrid local features, J. Inf. Secur. Appl. 45 (2019) 44–51, http://dx.doi.org/10.1016/j.jisa.2019.01.007.

[9] S. Wenchang, Z. Fei, Q. Bo, L. Bin, Improving image copy-move forgery detection with particle swarm optimization techniques, China Commun. 13 (1) (2016) 139–149, http://dx.doi.org/10.1109/CC.2016.7405711.

[10] B. Chen, M. Yu, Q. Su, L. Li, Fractional quaternion cosine transform and its application in color image copy-move forgery detection, Multimedia Tools Appl. 78 (7) (2019) 8057–8073, http://dx.doi.org/10.1007/s11042-018-6595-z.

[11] B. Chen, M. Yu, Q. Su, H.J. Shim, Y.-Q. Shi, Fractional quaternion Zernike moments for robust color image copy-move forgery detection, IEEE Access 6 (c) (2018) 56637–56646, http://dx.doi.org/10.1109/ACCESS.2018.2871952.

[12] T. Mahmood, Z. Mehmood, M. Shah, T. Saba, A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform, J. Vis. Commun. Image Represent. 53 (2018) 202–214, http://dx.doi.org/10.1016/j.jvcir.2018.03.015.

[13] S. Dua, J. Singh, H. Parthasarathy, Detection and localization of forgery using statistics of DCT and Fourier components, Signal Process., Image Commun. 82 (January) (2020) 115778, http://dx.doi.org/10.1016/j.image.2020.115778.

[14] T.M. Huang, V. Kecman, I. Kopriva, Iterative single data algorithm for kernel machines from huge data sets: Theory and performance, in: Kernel Based Algorithms for Mining Huge Data Sets, Vol. 17, Springer-Verlag, Berlin/Heidelberg, 2006, pp. 61–95, no. May 2005.

[15] M.Y. Cho, T.T. Hoang, Feature selection and parameters optimization of SVM using particle swarm optimization for fault classification in power distribution systems, Comput. Intell. Neurosci. 2017 (2017) 1–9, http://dx.doi.org/10.1155/2017/4135465.

[16] C. Srinivasa Rao, S.B.G. Tilak Babu, Image authentication using local binary pattern on the low frequency components, in: Lecture Notes in Electrical Engineering, Vol. 372, Springer Verlag, 2016, pp. 529–537.

[17] S.B.G.T. Babu, Ch.S. Rao, Texture and steerability based image authentication, in: 2016 11th International Conference on Industrial and Information Systems (ICIIS), Vol. 2018-Janua, 2016, pp. 154–159, http://dx.doi.org/10.1109/ICIINFS.2016.8262925.

[18] E.P. Simoncelli, W.T. Freeman, Steerable pyramid: a flexible architecture for multi-scale derivative computation, in: IEEE International Conference on Image Processing, Vol. 3, 1995, pp. 444–447, http://dx.doi.org/10.1109/icip.1995.537667.

[19] G. Suresh, C. Srinivasa Rao, Copy move forgery detection using GLCM based statistical features, Int. J. Cybern. Inform. 5 (4) (2016) 165–171, http://dx.doi.org/10.5121/ijci.2016.5419.

[20] M. Hall-Beyer, GLCM texture: A tutorial v. 3.0 2017, Arts Res. Publ. (2017–03) (2017) 75, http://dx.doi.org/10.11575/PRISM/33280.

[21] S.B.G.T. Babu, C.S. Rao, Statistical features based optimized technique for copy move forgery detection, in: 2020 11th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2020, 2020, http://dx.doi.org/10.1109/ICCCNT49239.2020.9225426.