International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8, Issue-1, May 2019

Copy-Move Forgery Detection System Through Fused Color and Texture Features using Firefly Algorithm

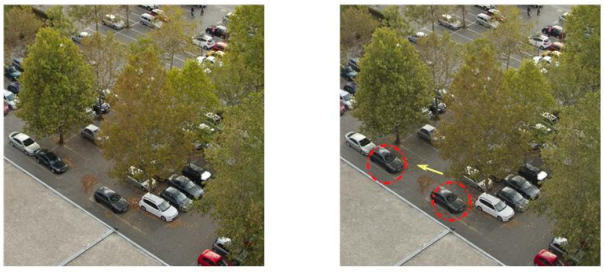
Gulivindala Suresh, Chanamallu Srinivasa Rao

Abstract: ***Copy-Move Forgery Detection (CMFD) is an established process to detect copy-move tampered regions in digital images. Several CMFD algorithms based on image transform, color and texture features are available in the literature. Detection of the tampered regions depends on the superiority of the feature vector. Hence, an efficient passive approach is proposed in which color and texture features are fused to form an improved feature vector. Firefly Algorithm (FA) is explored to obtain the nonlinear relationship between color and texture features. These Optimal Weighted Color and Texture Features (OWCTF) are used for detection of forged images and later localization is performed to detect the tampered regions in the forged image. The detection performance of the proposed method is evaluated on CASIA and CoMoFoD databases and the classification accuracy of 95.5% and 97% is achieved respectively. Similarly, performance evaluation of localization phase is also carried out. Simulation results demonstrate that the proposed method overtakes some of the existing methods in terms of detection and localization results. It is witnessed that proposed method is capable to detect and localize the tampered regions in the presence of signal processing attacks.***

Index Terms: ***color features, copy-move forgery, Firefly algorithm, texture features, localization.***

I. INTRODUCTION

Due to the advancement in digital technology, multimedia content distribution became easy. With the widespread of sophisticated image editing tools, modification or tampering of digital images can be done easily and can be uploaded onto social media networks. This made the reliability of digital images questionable. The trustworthiness of the images plays a critical role in judicial, medical and news media applications. Therefore, there is a very much need of identifying such tampered or forged images. Generally, image forgery detection can be categorized into two ways [1]: i. Active and ii. Passive. In Active approach, a known piece of information such as watermark or signature is embedded into the digital image. Signature is extracted to show the authenticity of the image. Any deviation in the retrieved signature indicates the possibility of tampering. Major limitation of this approach is signature embedding in real time before their distribution in digital networks. Passive approach relies on underlying statistical properties of the image to detect the tampered regions. Usually, the images are counterfeited by means of splicing or copy-move; splicing process uses two images to form the third image called as spliced image, whereas in copy-move forgery duplicated regions are created within the same image as shown in Fig. 1. Passive approach of CMFD involves detection and localization of CMF. Several works on CMF detection and localization are available in the literature; firstly, CMF detection techniques are reviewed and followed by localization techniques. Weber Law Descriptors (WLD) are explored by [2] on chrominance components for CMFD. Robust texture features are built from WLDs at different scales. The method is experimented for different types of copied regions.



a. Original Image b. Forged Image

Fig. 1: Illustration of Copy-Move Forgery

A CMFD method [3] in which LBP is applied on the sub bands obtained from Curvelet transform at different scales and orientations. Final histogram is formed from the fusion of normalized LBP histograms and this act as feature vector. This method is evaluated on CASIA database and achieved an accuracy of 93.4%. Steerable Pyramid Transform (SPT) and LBP are used by [4] for CMFD. LBP is applied on the sub bands obtained from SPT at different scales and orientations. Another work with SPT-LBP is proposed by [5] and here, feature selection methods are explored to reduce the dimensionality of the feature vector.

Revised Manuscript Received on 30 May 2019.

***** Correspondence Author

Gulivindala Suresh*, Department of ECE, GMR Institute of Technology, Rajam, AP, India.

Department of ECE, JNTUK University College of Engineering, Kakinada, AP, India.

Chanamallu Srinivasa Rao, 3Department of ECE, JNTUK University College of Engineering, Vizianagaram, AP, India.

The method is evaluated with the features from different Chroma components. Multi-scale LBP is explored with Multi-scale WLD by [6] for CMFD. Robust texture features are developed with WLD and LBP at different scales and this method has been evaluated on CASIA database.

Gabor wavelets and Local Phase Quantization (LPQ) are used by [7] for forgery detection. LPQ is applied on sub bands obtained from Gabor wavelets at different scales and orientations. Authors in [8] explored Discrete Cosine Transform (DCT), LBP, Curvelet and Gabor for feature extraction. These features are trained with Hidden Markov Model (HMM) and Support Vector Machine (SVM) to classify the forged images from the original images. A CMFD method [9] is proposed by Saurabh Agarwal and Satish Chand with entropy filter and local phase quantization (LPQ) on different color channels but it works with a large feature size of 2048. Mangat and Kaur in [10] used SIFT and Kernel Principal Component Analysis (KPCA) for CMFD. They have investigated SVM and Neural networks for classification. LBP texture features are used by [11] and these features are fed to Extreme Learning Machine (ELM) for classification. In [12], image features are extracted in Undecimated DWT domain and Markov model is used for classification. Authors in [13], explored DCT and two-scale LBP for feature extraction. This method is image-format independent approach which can detect different type of tampered images. SVM and neural networks are used for classification. An integrated system is being developed by [14] for CMFD and splicing detection. This method constructed features from DCT and enhanced threshold method. Various localization techniques are reviewed here; the earliest work of CMFD [15] used Discrete Cosine Transform (DCT) for feature extraction and various matching algorithms such as exact match, robust match are used for block matching. Later, Principal Component Analysis (PCA) based CMFD was developed by [16] which had better sensitivity to additive noise and JPEG compression. In some cases, copied regions will endure rotation and scaling operations before pasting, therefore a scheme was established using Fourier Mellin Transform (FMT) [17] to detect the rotated and scaled versions of the copied regions. The work contributed by [19] provides resilience against rotation and flipping due to rotation invariant features from Local Binary Pattern (LBP). Geometric invariant features from Radon transform are obtained in [20] to detect duplicate regions in the presence of noise, compression and blurring. The limitation of this method is its time complexity to build the features from large images. Lee [21] developed a method based on the features from Gabor magnitude and is robust against compression, blurring, brightness but for rotation and scaling to some extent. A method based on DCT was developed by [22] and authors has investigated the influence of number of blocks and forged area size on performance accuracy. An improved method based on DCT [23] was developed in which Kernel Principal Component Analysis (KPCA) is utilized for dimensionality reduction and is robust against various attacks. Authors in [24] established a method based on DWT and DCT for feature reduction. Similarity matching of the blocks is performed using correlation coefficients and the method achieved low false detection rate. Stationary Wavelet Transform (SWT) is explored by [25] and DCT for feature reduction. This method has a low feature vector and is resilience against signal processing attacks.

Several block-based methods concentrate on improving the features to detect the duplicate regions with high accuracy and with low computational complexity in the presence of various signal processing attacks. Methods based on texture features lack in capturing the color content of the image. This work investigates detection and localization of Copy-Move Forgery (CMF) with color and texture combination. Traditionally, in methods [26] and [27], color and texture features are merely concatenated to form a feature vector, but in the proposed method FA is adopted to obtain the nonlinear relationship among color and texture features to define an improved CTF vector. The main contributions of this work are: i. Color and Texture Features (CTF) are combined to frame a new and improved feature set to detect copy move forgeries, ii. Firefly optimization algorithm (FA), a metaheuristic approach, is explored to obtain optimal weights to fuse CTF vector and iii. CTF vector is used to localize the forged regions of different sizes and shape. Proposed method is novel and it is explored for the detection of duplicated regions. The remaining paper is organized as follows. Preliminaries of color, texture and FA are detailed in Section II. Section III presents the OWCTF detection and localization method. Section IV discusses experimentation and results. Sections V gives the concluding remarks.

II. PRELIMINARIES

This section describes the feature extraction from color moments and GLCM. The working of Firefly algorithm is detailed in this section.

A. Color features

Color is a powerful descriptor. Color moments are used to differentiate images based on their features of color. [28] defined three central moments mean M_c, standard deviation σ_c, skewness S_c for color image. We included the fourth moment kurtosis K_c to capture the image details effectively. These four moments are calculated for each channel of RGB color image as given in Equations 1-4, to obtain a set of 12 features for the image.

$$M_c = \frac{1}{N}\sum_n^N P_{nc} \quad (1)$$

$$\sigma_c = \sqrt{\left(\frac{1}{N}\sum_n^N (P_{nc} - M_c)^2\right)} \quad (2)$$

$$S_c = \frac{\left(\frac{1}{N}\sum_n^N (P_{nc} - M_c)^3\right)}{\sigma_c^3} \quad (3)$$

$$K_c = \frac{\left(\frac{1}{N}\sum_n^N (P_{nc} - M_c)^4\right)}{\sigma_c^4} \quad (4)$$

Where c indicates one of the three color channels i.e R, G, B and n ranges from 1 to N the number of pixels available in the image. P_{nc} is the pixel intensity of the n^{th} pixel in c^{th} channel.

B. Texture features

GLCM is a good old technique to extract texture features and recently, it is used for forgery detection [29] application. In this work, GLCM is explored to extract the texture features which provides a statistical measure on the occurrence of specific combinations of pixel intensities in a gray image. Six textural features [30] measure the nature of texture in terms of uniformity, non-uniformity, contrast, correlation, degree of change and homogeneity. These six features along with 12 color features form a feature vector for each image during the detection phase. In the case of localization, as it is a block-based approach, 12 color features on every block of color image and 6 GLCM textural features are computed on each block of gray image to form a vector of 18 features.

C. Firefly algorithm

Nature inspired algorithms are in use to solve global optimization problems. Firefly Algorithm (FA) proposed by Yang [31], is one of the bio-inspired Optimization Algorithms (OA), to address NP hard problems. FA works on the light flashing behaviour of the fireflies. FA is one among the OA, where a global solution is obtained through random movements of the fireflies towards brighter one. In the proposed method, FA is adopted to obtain the optimal weights between color and texture features by considering the detection accuracy as an objective function.

D. Support Vector Machine

SVMs are effectively useful in classification and regression problems. Vapnik introduced standard SVM [32] which works with statistical learning philosophy to separate trained data into classes. Consider a two-class problem, in which training data group $T = \{(r_1, s_1), (r_2, s_2), \dots \dots (r_k, s_k)\}$, $r_i \in \mathbb{R}^d$ where r is the data points of length k and $s \in \{-1, 1\}$ defines the class label of the various data points respectively. The objective of the SVM is to discover a hyper-plane that provides the least distance between any data point. Optimal hyper-plane can be achieved by minimizing the below objective function

$$\left\{\frac{1}{2}|w|^2 + C\sum_{i=1}^k \varepsilon_i\right\}, \varepsilon_i \geq 0 \quad (5)$$

Subject to $s_i(w^T r_i + b) \geq 1 - \varepsilon_i,\ i = 1, 2, \dots \dots k \quad (6)$

Where, w is a normal vector, C is trade-off margin width and misclassifications, ε_i is a slack variable allows data points to slip off the margin but penalizes them. Linear SVM takes the form in Eq.6. In some cases, data is not linearly separable, then kernel function is used to transform data into a different space to perform the linear separation. Various kernel functions are available for this purpose, but Radial Basis Function (RBF) mostly used as kernel function for SVM due to its accurate and reliable performance. Hence, RBF has been explored in this work.

III. PROPOSED SYSTEM FOR CMFD

A novel CMFD method is proposed using Optimal Weighted Color and Texture Features (OWCTF) through FA. Proposed system consists of two steps: i. Detection of copy-move tampered images and ii. Localizing tampered regions in the detected forged images. In the proposed system, CTF are extracted and a feature vector is constructed for each image in the database. In classification problem, classification accuracy depends on the feature set and it increases when the features are more distinguishable and significant. Hence, color and texture features are fused with optimal weights to increase the classification accuracy. To achieve this, Firefly Algorithm is explored with accuracy as the objective function to obtain optimal weights for CTF vector. These OWCTF are used to train the Support Vector Machine (SVM) and a cross-validation with 10-Fold is adopted to detect the forged images. The localization process is followed to localize the tampered regions in the detected CMF images.

A. Proposed OWCTF detection method

The proposed OWCTF detection method detects the forged images from the given database which consists of original and tampered images. In the proposed system, CTF are extracted and a feature vector is constructed for each image in the database. Color moments are extracted on each color channel to yield 12 moments as described in Section 3.1. Six texture features are obtained using GLCM on the gray image as explained in Section 3.2. Each image is represented by a vector of 18 CTF features. FA is explored to provide optimal weights for CTF by considering accuracy as objective function. FA evaluates the objective function for accuracy, in each case SVM with k-fold cross-validation is used to train and test the images to determine the accuracy. This process is repeated until all the firelfies in all generations are exhausted or attained the optimal solution. The pseudo code for the proposed OWCTF detection method is detailed below in Algorithm 2.

***Algorithm 2**: Proposed OWCTF detection method*

Input: Image database
Output: Detection of forged images
To obtain CTF
for *k=1:DS* *# DS is number of images in the database*

calculate color moments
calculate texture features
CTF(k)=cat(CM,TF) # Assign 12 color moments and 6 texture features
end for *k;*
 # To obtain OWCTF and detection
Define Objective Function $f(w)$,
$w = (w_1, w_2 \dots \dots w_{18})^T$
 # accuracy Acc *as a function of weights*
Initialize population of fireflies $w_i = (1,2, \dots \dots n)$
Initialize light absorption coefficient γ, α
while *(iter < MaxIter)*
for *i=1:n # all n fireflies*
for *j=1:n # all n fireflies*
With the present population (weights)
Using k-fold cross-validation
Obtain Accuracy of SVM Classifier
if ($Acc_i < Acc_j$),
Move firefly i *towards ;*
end if;
Vary β *with distance* r *through* $e^{\gamma r_{ij}^2}$
Evaluate new solutions and update weights
end for *j*;
end for *i*;
Sort Acc *and find the present global best solution*
end while
Store Acc, *optimal weights* w *and forged images index*
Proceed for localization

B. Proposed OWCTF localization method

In CMFD, localizing the duplicated regions is an important task. To achieve this, given image is partitioned into overlapping blocks of uniform size and feature vector is constructed for each block. The features are optimal weighted obtained through FA. Euclidean distance measure is used to calculate the similarity between the blocks and the blocks with high similarity are identified as potential regions of forgery. Morphological opening and closing are performed to avoid false matches to improve the detection accuracy.
Algorithm steps of the CTF method:
Step 1: Image partitioning
Partition the given image of size ($M \times N$) into overlapping blocks of uniform size Bs. Number of overlapping blocks are $(M - Bs + 1) \times (N - Bs + 1)$.
Step 2: Feature extraction
Compute 4 color features for every block of each color channel, resulting in 12 features. Compute 6 texture features on each block of the gray image. Finally, an array of $(M - Bs + 1) \times (N - Bs + 1) \times 18$ features are built for the entire image. These features are weighted according to the optimal weights w obtained through FA.
Step 3: Sort Features
Duplicated regions have similar features and to identify the similar regions entire feature array is to be verified. In order to reduce complexity, feature array is lexicographically sorted. Thus, feature vectors of duplicated regions come closer and available sequentially.
Step 4: Block matching
Similarity is measured between the feature vectors of the image blocks using Euclidean distance as given in Eq.7.

$$Sim = \sqrt{(\sum_b^R (F_b - F_{b+1})^2)} \quad (7)$$

Where F_b and F_{b+1} are the feature vectors of b^{th} block and $(b+1)^{th}$ blocks respectively.
Similarity Sim is measured for all the feature vectors within the range R.

$$Sim(i,\beta) = \min\{Sim(i,i+1), \dots Sim(i,i+R)\} \quad (8)$$

The feature vectors of overlapping blocks have high similarity. In order to mitigate this, the similarity between the corresponding blocks is controlled by a similarity threshold T_{sim} and physical distance by a distance threshold T_{dist}. From Eq.8, if $Sim(i,\beta)$ is less than T_{sim} and physical distance more than T_{dist}, then it is identified as a potential block of forgery and indices of the respective blocks are maintained in an array ψ.
Step 5: Post-Processing
The array ψ contains matched pairs and duplicated regions can be exposed by marking the regions in red color on the given image. This can be compared with ground truth and false alarms can be eliminated by morphological open and close operations. Final detection can be taken into account to calculate performance metrics.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

This section provides experimentation details and performance analysis of the OWCTF method quantitatively and qualitatively. Robustness of the method and its comparison with other existing methods are also discussed. Two rounds of experimentation are carried to validate the proposed OWCTF system, i. Round #1 to detect the forged images using optimal weighted CTF and ii. Round # 2 to localize the forged regions in the detected forged images using optimal weighted CTF.

A. Database

Experimentation is carried on benchmark databases viz., CoMoFoD [33] and CASIA [34]. CoMoFoD database consists of 10,000 images of size 512x512 in .png format which are original, forged and post-processed images. CASIA Tampered Image Detection Evaluation Database consists of images with size 384×256 pixels in JPEG format.

B. Performance Metrics

In the case of detection, the following parameters are calculated to evaluate the performance of the classifier.
True Positive (TP) – Forged
Images predicted as Forged

True Negative (TN) – Original Images predicted as Original
False Positive (FP) – Original Images predicted as Forged
False Negative (FN) – Forged Images predicted as Original
With the above parameters, the below performance metrics are computed with the below equations 9, 10 and 11.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \times 100 \quad (9)$$

$$Sensitivity = \frac{TP}{TP+FN} \times 100 \quad (10)$$

$$Specificity = \frac{TN}{TN+FP} \times 100 \quad (11)$$

In the case of localization, performance is measured at the pixel level using the parameters True Detection Rate (TDR) and False detection rate (FDR) as defined in Equations 12 and 13. In this experimental setup, values of T_{sim}, T_{dist} and R are considered as 0.01, 50 and 20 respectively.

$$TDR = \frac{|C \cap \widehat{DC}| + |F \cap \widehat{DF}|}{|C| + |F|} \quad (12)$$

$$FDR = \frac{|\widehat{DC} - C| + |\widehat{DF} - F|}{|\widehat{DC}| + |\widehat{DF}|} \quad (13)$$

Where C, F, $\widehat{DC}$, $\widehat{DF}$ are copied, forged, detected copied and detected forged regions respectively.

C. Round #1 OWCTF Detection results

FA parameters

FA is used to obtain weights for the color and texture features to form a optimal combination of color and texture feature vector. List of parameters and their initial values of Firefly are provided here. Maximum iterations: 50, Population: 20, Light absorption coefficient γ=1, Mutation coefficient α=0.1, Attraction coefficient β_o=10, Lower bound=0.0001 and Upper bound=50.

Detection performance

The effectiveness of the proposed method is assessed on CoMoFoD and CASIA datasets. In the proposed method, SVM [32] classifier with RBF kernel is used for classification of authentic and forged images. Texture feature vector obtained from genuine image is labelled as +1 (positive), and CMF image as -1 (negative) label. SVM is a supervisory learning algorithm consists of train and test phases. In our experiments, feature vectors are randomly split into two sets as training and testing sets. SVM is modeled using the training set to define optimal hyperplane and the model is tested for classification using testing set. In order to reduce this effect, 10-fold Cross Validation (CV) is considered where the images in dataset are split into 10 independent parts. In each CV test case, 9/10 of authentic and forged images are used for training the classifier and the rest 1/10 images are used for SVM classification. Average value of classifier performance for 10-fold CV tests is considered as the final result and is shown in Table 1.

Table 1. Classification performance of OWCTF detection method

Database	TP	TN	FP	FN	Accuracy	Sensitivity	Specificity
CoMoFoD	95	96	4	5	95.5	95	96
CASIA	97	97	3	3	97	97	97

Detection performance against post-processing attacks

Following are the post-processing attacks that are performed on the forged images which are available in CoMoFoD database.

1. Brightness Change (BC): Change in intensity level with lower and upper bounds [(0.01, 0.95), (0.01, 0.9), (0.01, 0.8)]
2. Contrast Adjustments (CA): Contrast is varied with three different lower and upper bounds [(0.01, 0.95), (0.01, 0.9), (0.01, 0.8)]
3. Color Reduction (CR): Quantization is performed per each color channel as [32, 64, 128]
4. Noise Adding (NA): Additive White Gaussian Noise with mean, μ = 0, variance σ^2 = [0.009, 0.005, 0.0005]
5. Image Blurring (IB): Image is blurred with spatial averaging filter using [3x3, 5x5, 7x7] masks
6. JPEG compression (JC): Images are compressed at different quality factors (Q) [20, 30, 40, 50, 60, 70, 80, 90, 100] The proposed method is evaluated by considering 50 forged images under each post-processing attack category, so that 1200 forged and processed images are tested. Performance of the proposed OWCTF detection method against the above mentioned attacks in terms of accuracy, sensitivity and specificity are shown in Fig. 2-4.

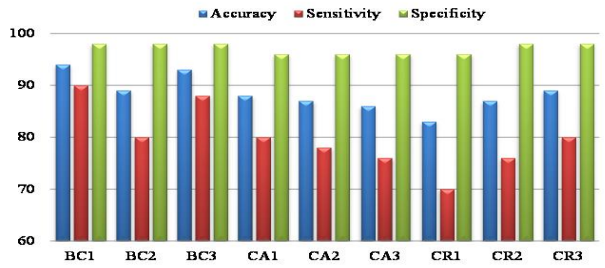


Fig. 2: Detection performance against BC, CA and CR attacks

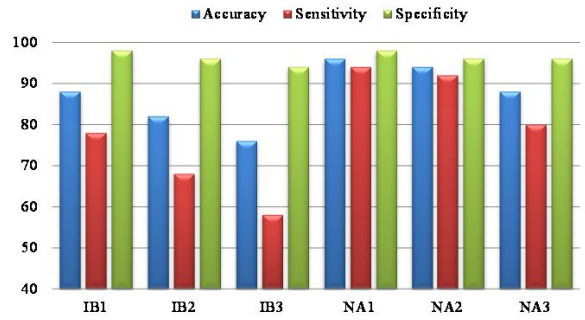


Fig. 3: Detection performance against IB and NA attacks

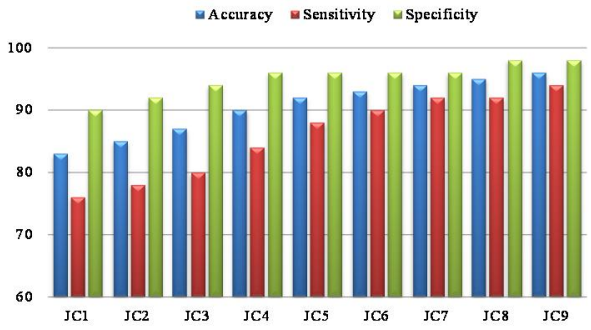


Fig. 4: Detection performance against JPEG compression

Comparative Analysis

The proposed method's accuracy is compared with other existing methods viz., WLD [2], Curvelet-LBP [3], SPT-LBP [5], WLD-LBP [6], LBP [11] and BDCT [14]. All these methods works with textural component in combination with an image transform for effective feature extraction and evaluated on CASIA v 1.0 dataset. The comparative analysis is shown in Fig. 5 and it is evident that the proposed method outperforms other existing methods with regard to accuracy.

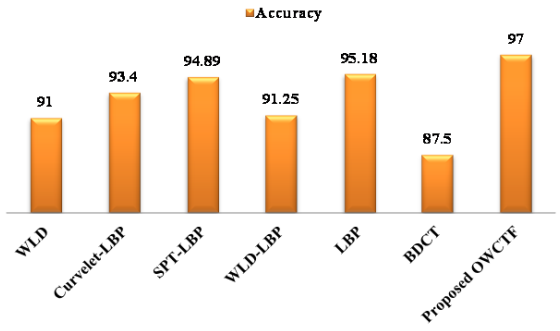


Fig. 5: Comparative analysis of the proposed method

D. **Round #2 OWCTF Localization results**

Quantitative and qualitative analysis

The forged images that are identified through OWCTF detection method are used in localization phase to localize the tampered regions. CoMoFoD dataset is used as it contains ground truths, forty forged images without any attack are considered and forged regions are localized using the CTF method. These regions are compared with ground truths and average detection rates are calculated. As well, the proposed localization method is able to detect multiple forged regions. Table 2 illustrates the average CDR and FDR for images without attack and images with multiple forged regions.

Table 2. Detection results of OWCTF localization method

Forged Image Description	TDR	FDR
Without attack	0.9721	0.0816
Multiple Forged regions	0.9519	0.1201

OWCTF method is also able to detect forged regions of different shape and size. These results are presented visually in Fig. 6. CMFD can be achieved through individual features viz., texture using GLCM (GLCM6) and color moments (Color). Detection rates achieved through these features are given in Table 3. A novel combination of color and texture features enhanced the detection rate and reduced the false detection rate.

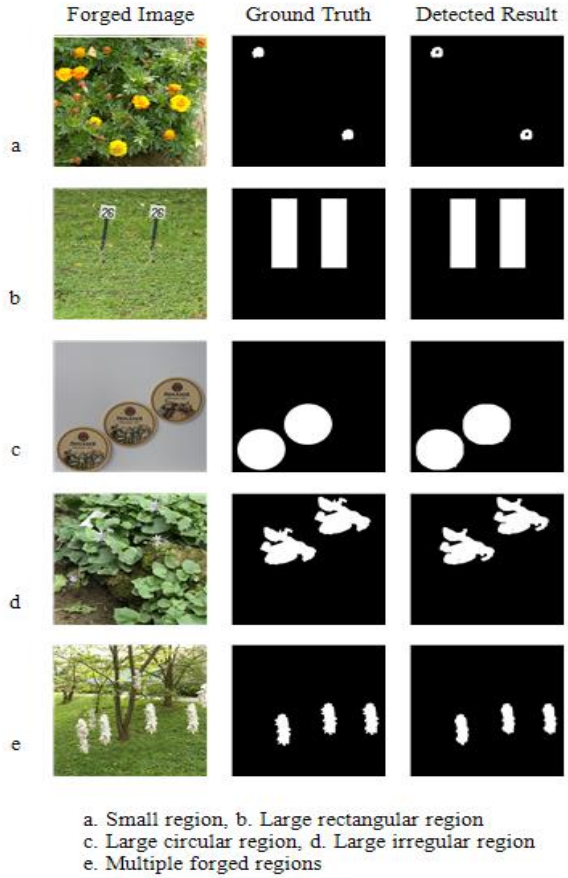


Fig. 6: Detection results (Qualitative) of CTF method

Table 3. Significance of the features

Description	TDR	FDR
GLCM6	0.7934	0.8006
Color	0.9721	0.3073
Color+GLCM6	0.9721	0.0816

Robustness analysis

Robustness of the proposed method is evaluated on forged images with different post-processing operations. An investigation is carried on forged images from CoMoFoD database which consists of forged regions of different sizes and shapes with post-processed attacks viz., Brightness Change (BC), Color Reduction (CR), Image Blurring (IB) and Contrast Adjustment (CA) for robustness analysis. In BC attack, the forged image brightness levels are varied in three categories by defining the lower and upper limits as [0.01,0.95], [0.01,0.9] and [0.01,0.8]. In CR attack, color levels of the forged images are quantized to either 32, 64 or 128 levels. IB attack uses three filter masks such as 3x3, 5x5 and 7x7 to blur the forged images. In CA attack, contrast levels of the image are varied in three categories through the lower and upper limits as [0.01,0.95], [0.01,0.9] and [0.01,0.8]. In each attack case,

30 images are considered for analysis and the results are tabulated in Table 4.

Table 4. Robustness analysis

Attack Description		TDR	FDR
Brightness change	[0.01,0.95]	0.9845	0.0400
	[0.01,0.9]	0.9800	0.0412
	[0.01,0.8]	0.9735	0.0850
Color reduction	32	0.9564	0.0723
	64	0.9792	0.0564
	128	0.9853	0.0400
Blurring	3x3	0.9500	0.0436
	5x5	0.8945	0.1012
	7x7	0.8124	0.1830
Contrast Adjustment	[0.01,0.95]	0.9348	0.0719
	[0.01,0.9]	0.9300	0.0840
	[0.01,0.8]	0.9235	0.0875

Robustness of the method against brightness change and color reduction attacks is very high and it can withstand only blurring with 3x3 filter mask. TDR is decreased and false matches are increased for other blurring filters.

Comparative analysis

Performance of the CTF method is compared with existing methods PCA [16], FMT [17], LBP [19], DCT [22], DCT-KPCA [23], DWT-DCT [24] and SWT-DCT [25] in terms of TDR and FDR. Post-processing attacks such as brightness change, color reduction and blurring are considered for comparative analysis. Fig. 7 & 8 illustrate the superiority of proposed OWCTF method over other methods for brightness change attack. It is evident that TDR is increased and FDR is reduced for higher changes in brightness level; these TDR and FDR values validates the superiority of the proposed method over other existing methods.TDR is low and FDR is high when color quantization has used only 32 levels. Proposed method performs better in the presence of color reduction attack and is evident from the Fig. 9 & 10.

More amount of blurring on the forged images results in poor localization and it can be seen in Fig. 11 & 12. Proposed method performs well for blurring attack in terms of TDR but FDR is not better over all the existing methods.

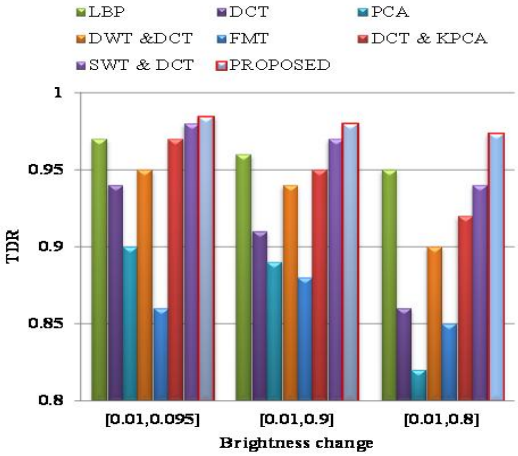


Fig. 7: TDR for brightness change

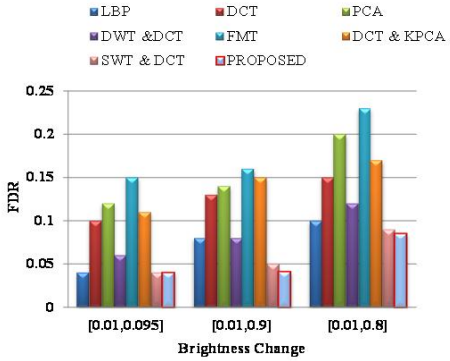


Fig. 8: FDR for brightness change

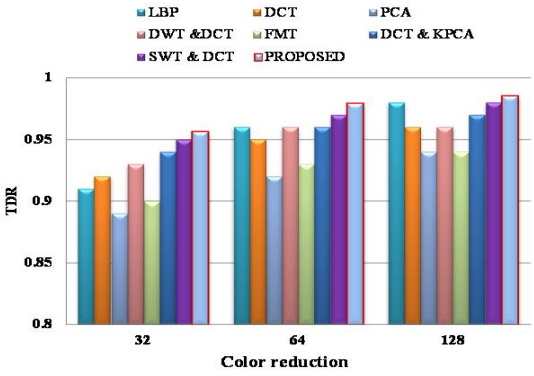


Fig. 9: TDR for Color reduction

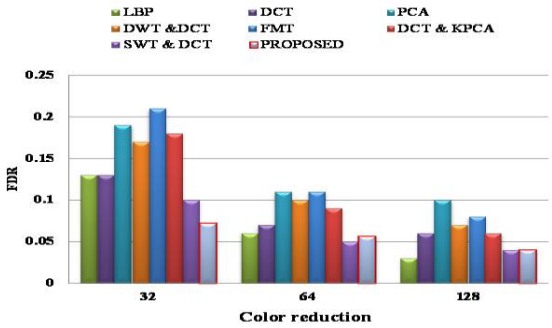


Fig. 10: FDR for Color Reduction

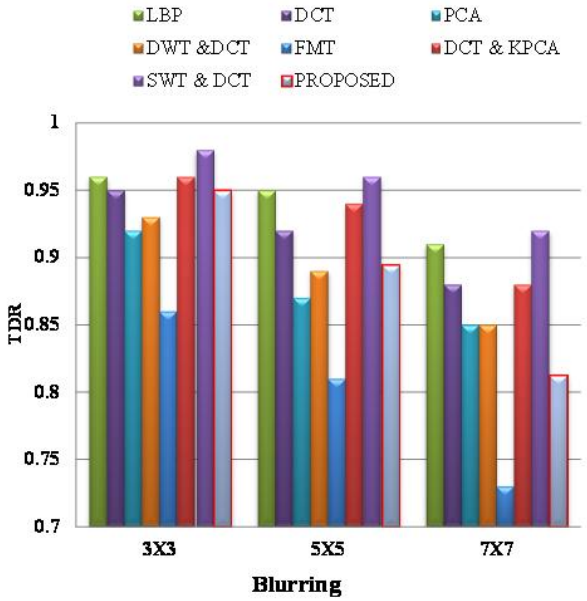


Fig. 11: TDR for Blurring attack

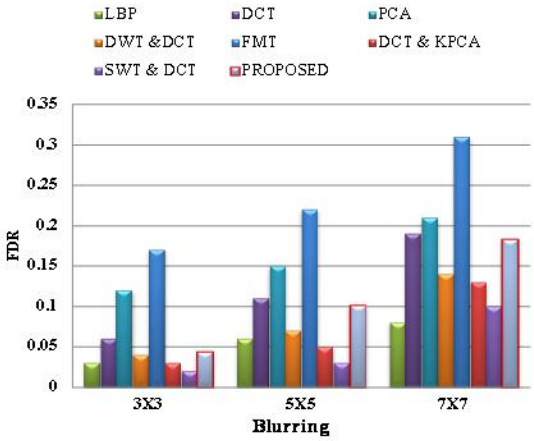


Fig. 12: FDR for Blurring attack

V. CONCLUSIONS

An efficient passive block based approach to detect and localize CMF in digital images is proposed. Firefly Algorithm (FA) is explored to obtain optimal weights for color and texture features. These Optimal Weighted Color and Texture Features (OWCTF) are used for detection of forged images and later localization is performed to detect the tampered regions in the forged image. Classification performance of OWCTF method is evaluated on CASIA and CoMoFoD databases and the detection accuracy of 95.5% and 97% is achieved respectively. Comparative analysis of the OWCTF detection method surpasses other established methods based on texture features. Simulation results demonstrate that the proposed localization method outperforms some of the existing methods in terms of TDR and FDR. It is validated that proposed method is capable in detecting and localizing the tampered regions in the presence of signal processing attacks.

REFERENCES

1. H. Farid, "Image Forgery Detection," *IEEE Signal Process. Mag.*, no. March, pp. 16–25, 2009.
2. M. Hussain, G. Muhammad, S. Q. Saleh, A. M. Mirza, and G. Bebis, "Copy-Move Image Forgery Detection Using Multi-Resolution Weber Descriptors," in *Eigth International Conference on Signal Image Technology and Internet Based Systems*, 2012, pp. 395–401.
3. B. G. Al-Hammadi M.H., Muhammad G., Hussain M., "Curvelet Transform and Local Texture," in *In: Bebis G. et al. (eds) Advances in Visual Computing. ISVC 2013. Lecture Notes in Computer Science*, 2013, vol. 8034, pp. 503–512.
4. G. Muhammad, M. H. Al-Hammadi, M. Hussain, A. M. Mirza, and G. Bebis, "Copy move image forgery detection method using steerable pyramid transform and texture descriptor," in *IEEE EuroCon 2013*, 2013, no. July, pp. 1586–1592.
5. G. Muhammad, M. H. Al-Hammadi, M. Hussain, and G. Bebis, "Image forgery detection using steerable pyramid transform and local binary pattern," *Mach. Vis. Appl.*, vol. 25, no. 4, pp. 985–995, 2014.
6. M. Hussain, S. Qasem, G. Bebis, G. Muhammad, H. Aboalsamh, and H. Mathkour, "Evaluation of Image Forgery Detection Using Multi-Scale Weber Local Descriptors," *Int. J. Artif. Intell. Tools*, vol. 24, no. 04, p. 1540016, 2015.
7. M. M. Isaac and M. Wilscy, "Image Forgery Detection Based on Gabor Wavelets and Local Phase Quantization," in *Procedia Computer Science*, 2015, vol. 58, pp. 76–83.
8. M. F. Hashmir and A. G. Keskar, "Image Forgery Detection and Classification using HMM and SVM Classifier," *Int. J. Secur. its Appl.*, vol. 9, no. 4, pp. 125–140, 2015.
9. [9] Saurabh.Agarwal.;Satish.Chand, "Image Forgery Detection using Multi Scale Entropy Filter and Local Phase Quantization," *Int. J. Image, Graph. Signal Process.*, vol. 8, no. 10, pp. 78–85, 2015.
10. S. S. Mangat and H. Kaur, "Improved copy-move forgery detection in image by feature extraction with KPCA and adaptive method," in *Proceedings on 2016 2nd International Conference on Next Generation Computing Technologies, NGCT 2016*, 2016, no. October, pp. 694–703.
11. M. Alhussein, "Image tampering detection based on local texture descriptor and extreme learning machine," *Proc. - 2016 UKSim-AMSS 18th Int. Conf. Comput. Model. Simulation, UKSim 2016*, pp. 196–199, 2016.
12. S. Agarwal and S. Chand, "Image forgery detection using Markov features in undecimated wavelet transform," in *2016 9th International Conference on Contemporary Computing, IC3 2016*, 2016, pp. 1–6.
13. M. L. Wu, C. S. Fahn, and Y. F. Chen, "Image-format-independent tampered image detection based on overlapping concurrent directional patterns and neural networks," *Appl. Intell.*, vol. 47, no. 2, pp. 347–361, 2017.
14. C. S. Prakash, A. Kumar, S. Maheshkar, and V. Maheshkar, "An integrated method of copy-move and splicing for image forgery detection," *Multimedia Tools and Applications*, pp. 1–25, 2018.
15. J. Fridrich, D. Soukal, and J. Lukáš, "Detection of Copy-Move Forgery in Digital Images," in *Digital Forensic Forensic Research Workshop*, 2003, pp. 19–23.
16. A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," *Dept. Comput. Sci., Dartmouth Coll. Tech. Rep. TR2004-515*, no. 2000, pp. 1–11, 2004.
17. S. Bayram, H. T. Sencar;, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in *IEEE Acoustics, Speech and Signal Processing*, 2009, pp. 1053–1056.
18. L. Li, S. Li, Hancheng Zhu, S.-C. Chu, J. F. Roddick, and J.-S. Pan, "An efficient scheme for detecting copy-move forged images by local binary patterns," *J. Inf. Hiding Multimed. Signal Process.*, vol. 4, no. 1, pp. 46–56, 2013.
19. Y. Lei, L. Zheng, and J. Huang, "Geometric Invariant Features in the Radon Transform Domain for Near-Duplicate Image Detection," *Pattern Recognit.*, vol. 47, no. 11, pp. 3630–3640, 2014.
20. J.-C. C. Lee, "Copy-move image forgery detection based on Gabor magnitude," *J. Vis. Commun. Image Represent.*, vol. 31, pp. 320–334, 2015.
21. M. H. Alkawaz, G. Sulong, T. Saba, and A. Rehman, "Detection of copy-move image forgery based on discrete cosine transform," *Neural Comput. Appl.*, pp. 183–192, 2016.
22. T. Mahmood, T. Nawaz, A. Irtaza, R. Ashraf, M. Shah, and M. T. Mahmood, "Copy-Move Forgery Detection Technique for Forensic Analysis in Digital Images," *Math. Probl. Eng.*, vol. 2016, p. Article ID 8713202, 2016.

23. K. Hayat and T. Qazi, "Forgery detection in digital images via discrete wavelet and discrete cosine transforms," *Comput. Electr. Eng.*, vol. 62, pp. 448–458, 2017.
24. T. Mahmood, Z. Mehmood, M. Shah, and 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.*, vol. 53, no. March, pp. 202–214, 2018.
25. P. Liu, J. M. Guo, K. Chamnongthai, and H. Prasetyo, "Fusion of color histogram and LBP-based features for texture image retrieval and classification," *Inf. Sci. (Ny).*, vol. 390, pp. 95–111, 2017.
26. L. Z. Weifang Xie; Shengxiang Zhang, Shuwan Pang, "Ore Classification Based on Color and Texture Feature Fusion," 2017, vol. 25, pp. 496–501.
27. [27] M. Stricker and M. Orengo, "Similarity of Color Images," in *SPIE conference on storage and retrieval for Image and Video databases*, 1995, pp. 381–392.
28. X. Shen, Z. Shi, and H. Chen, "Splicing image forgery detection using textural features based on the grey level co-occurrence matrices," *IET Image Process.*, vol. 11, no. 1, pp. 44–53, 2017.
29. G. Suresh and C. Srinivasa Rao, "Localization of Copy-Move Forgery in Digital Images through Differential Excitation Texture Features," *Int. J. Intell. Eng. Syst.*, vol. 12, no. 2, pp. 42–52, 2019.
30. X. Yang and L. Press, *Nature-Inspired Metaheuristic Algorithms Second Edition*, Second. Luniver Press, 2010.
31. V. N. Vapnik, *The Nature of Statistical Learning Theory*, vol. 8, no. 6. 2000.
32. D. Tralic, I. Zupancic, S. Grgic, and M. Grgic, "CoMoFoD - New Database for Copy-Move Forgery Detection," *Proc. 55th Int. Symp. ELMAR-2013*, no. September, pp. 49–54, 2013.
33. "CASIA Tampered Image Detection Evaluation Database," *http://forensics.idealtest.org*, 2010. [Online]. Available: http://forensics.idealtest.org.

AUTHORS PROFILE

Gulivindala Suresh is a research scholar in the Department of ECE at JNTUK University College of Engineering, AP, India. He obtained his M.Tech from Biju Patnaik University of Technology, Orissa, India. He obtained his B.Tech from JNTU, AP, India. His research interests are Digital Image Processing and VLSI. He is a member of IETE. Presently, he is working as Assistant Professor in the Department of ECE, GMR Institute of Technology, Rajam, AP, INDIA.

Chanamallu Srinivasa Rao is currently working as Professor in the Department of ECE, JNTUK University College of Engineering, Vizianagaram, AP, India. He obtained his Ph.D. in Digital Image Processing area from University College of Engineering, JNTUK, Kakinada, AP, India. He received his M. Tech degree from the same institute. He published 50 research papers in international journals and conferences. His research interests are Digital Speech/Image and Video Processing, Communication Engineering and Evolutionary Algorithms. He is a Member of CSI. Dr Rao is a Fellow of IETE.