Image Forgery Identification using Convolution Neural Network

N. Hema Rajini

Abstract--- In recent days, an important problem in image forensic is to determine whether a specific image is authenticated or non-authenticated. It is a crucial process where the images are considered as major evidence to alter decision in various scenarios like court laws. For performing those forensic investigation, different technical devices and algorithms has been introduced in the present world. Copy move and splicing are the commonly employed approaches for passive image forgery. This paper develops a model for detecting splicing and copy-move forgery concurrently on the similar dataset of CASIA v1.0 as well as CASIA v2.0. At the beginning, a doubtful image is considered for processing and the feature extraction process takes place using block discrete cosine transform (BDCT) and enhanced threshold approach. The presented model will decide the presence of manipulated image among the provided images. When the image is found to be manipulated, convolution neural network (CNN) is employed for classifying the image into splicing or copy-move forgery. Furthermore, Zernike Moment (ZM) polar is employed for locating the replicaportions in the image. The simulation outcome ensures the effective performance of the presented method over the existing ones.

Keywords--- Image Forensic, Copy Move, CNN, Splicing, Zernike Moment.

I. INTRODUCTION

Digital crime along with regularly developing software techniques is exponentially raising the rate which exceedssuspiciousactions. In some cases, digital images or videos are unquestionableproof of a crime or the confirmation of a maliciousact. Using the information from the digital image, the multimedia forensic agencies intends to develop effective approaches for supporting clue investigation and also offer a basis to make decision regarding a crime. Multimedia forensics [1] defines the upcoming technical devices which operate in the non-existence of watermark or signature placed in the image. Generally, in contrast to digital watermarking, forensic indicates the passive work due to the fact that it formulates an investigation of a digital document by the presence of digital data itself. These methods fundamentally enable the client to verify whether the specific data has been tampered with [2] or the usage of capturing devices. Particularly, the concentration on the process of the recognition of acquisition devices, two things should be considered: initially, we have to recognize the device model that created the image, for example, scanner, camera, etc; second it to identify the particular kind of the product that captured the particular data. Another important forensic concept is the identification of tampered images, i.e. evaluating the authentication of the digital image.

Data integrity is a basic criterion in various applications, it is also obvious that the invention of digital images and easiness of image processing in the present days makes it authentication. A sample is shown in Fig. 1 where the digital image is modified and the crucial meaning of the image is interpreted which influences the court decision. In addition, it is fascinating that the images are given as an important proof to manipulate the information of what actually happened.

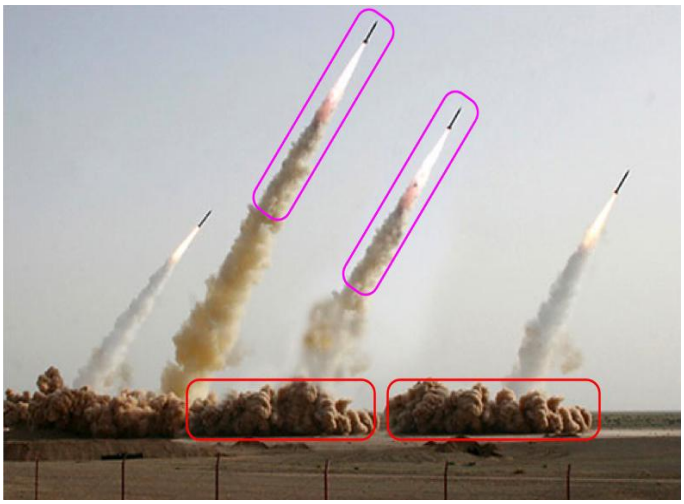


Fig. 1: Illustration of image tampering. The feigned image (on the right) interprets 4 missiles are launched from Iran, but actually it is 3

In the present digital world, “seeing is no more believing”. A massive amount of content is transmitted in the digital way particularly in the outward appearance of images or videos. Hence, itproduces the major flow of data carrier and the sources will undergo manipulation in an easier way. This paper focuses on image forgeries which are considered as a crucial task.

Manuscript receivedJune 10, 2019.

N. HemaRajini, Department of Computer Science and Engineering, AlagappaChettiar Government College of Engineering and Technology, Karaikudi, Tamilnadu, India. (e-mail: auhemasmith@yahoo.co.in)

The image processing software like Adobe Photoshop is readily accessible and it makes the modification of images easier resulting to more consequences, since the tampered images are used as proof in the court judgment to take false decision by providing false information as a portion of evidences. So, the problem of authentication of images is considered seriously. The available digital image forgery recognition methods are categorized intointrusive/non-blind and non-intrusive/blind [3] as provided in Fig.2.

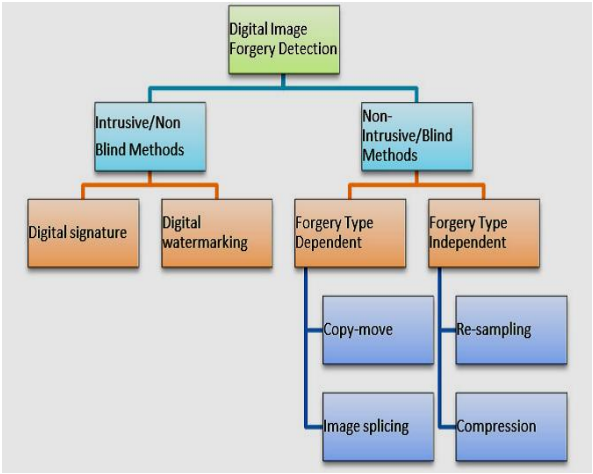


Fig.2: Classification of image forgery detection approaches

Intrusive or non-blind approaches need digital data to be inserted to the input image once it is created. Few instances are watermarking, digital signatures, etc. At the same time, non-intrusive or blind approach does not need any inserted data. An image is considered as forged in case of tampering the input image by the use of different transformation typesnamely rotation, scaling, resizing, etc.

Two widely using tampering methods are copy-move and splicing. In the first type, a part of the image is replicated and placed in other portions to hide the unnecessarypart inside the same image [4]. In the splicing type, the tampered image contains two sources and retains major part of the one image [4]. Passive forensic approaches satisfy the process with no extra detail excluding the image, hence, offering benefits over active methods like watermarking and signature approaches. So, many research works are carried out in the development of blind authentication approaches. The forged images leave some clue that can be utilized for locating the manipulated parts.

This paper devises a new detection model which is employed to identify the type of forgery whether it is copy move or splicing. The paper's contribution is given here

- The presented approach involves the process of handling both splicing and copy-move forgery concurrently where the previous methodologies have focused on any one of the type. Based on it, existing methods make use of the dataset focusing on splicing or copy-move. Here, we present a novel approach that detects the splicing and also copy-move on the identical dataset CASIA v1.0.
- For identifying the forgeries, color space characteristics of the image is assumed and employed Markov features for extracting the features from various color spaces by the use of enhanced threshold approach.
- An enhanced threshold approach is devised to decrease the feature vector dimensions while comparing with available approaches.
- To detect copy-move, PatchMatchmethod is employed to match the features. It is accurate for nearest-neighbor for searching an image and the computation time is also minimized.

The upcoming portions of the paper are arranged here: Existing works are briefed in Section 2. Proposed model is explained in Section 3. Result validation takes place in Section 4. The presented model is concluded in Section 5.

II. RELATED WORKS

Few recent methods that are build for detection of image forgery has been discussed here. The major focus of copy-move forgery is to search the same area exist in input images, whereas finding the inconsistency feature in splicing detection. Even though, there are many studies exist, highly they resolve one of the two issues that are splicing or copy-move forgery in a given image. But, some techniques that solve the two forgeries are presented in the following review. It is a difficult thing to construct a method to solve both the methods in image forensics.

2.1 Splicing forgery recognition

An illustration of splicing is shown in Fig. 3. When compared to identification of copy-move forgery, splicing is a difficult task to work with. Illustrating an image via splicing is a challenging one. With images feature, the basic idea of different splicing detection methods is to search the inconsistency area. For manipulating a forged image, the area is always compressed double times, blurred and re-sampled in splicing. This is the reason to motivate the researchers to construct various methods to image splicing detection. Few built methods are described as follows which are recently proposed.

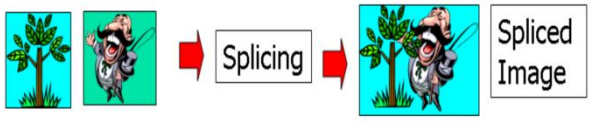


Fig. 3: Sample splicing process

A method has been projected [5] which depends on noise discrepancies among spliced and actual image. Primarily, at pixel level over different scales, noise level function is estimated and examined. The area which is not present in the noise level is called as suspicious region and tampering existence in spliced segments are denoted through noise inconsistent level. For detection of multiple spliced objects, this method works well. Depending on discrete cosine transform (DCT) and improved local binary pattern (LBP), [6] projected a methodology.The chrominanceimage element is segmented into non-overlapping blocks. For entire blocks, the enhanced LBP is computed and it is changed into frequency domain employing 2D-DCT. For the entire blocks, to search the standard deviation, additionally, the frequency coefficients are computed using k-nearest neighbor that are employed as classification features.

A natural image model is projected by [7] that draw out geometric characteristics function moments through BDCTadjacent differences of image as 1-D signal in addition to the dependency among adjacent nodes over particular directions might developed as Markov model. For classification, support vector machine (SVM) classifier assumed the parameters as discriminative features. To derive edge images, a method had been projected [8] in that gray level co-occurrence matrix (GLCM) is assumed over particular direction and for classification, the drawn edge image acts as a discriminating feature. For forgery detection, a method had been projected through [9] in that the moment of characteristic functionandHilbert-Huang transformof wavelet transformare employed. For classification of spliced image, SVM is employed as a classifier and attained 85.86%accuracy.

A method had been projected [10], in that gray level run-length featuresandchroma channel are employed. With the four various directions from de-correlated chroma channel, gray level run-length is employed to derive the features. Depending on the derived features, SVM is employed for classification. Employing inconsistency of illuminant color, a method had been projected [11] for image splicing detection. Primarily, images are segmented into overlapping zones and then employing the classifier, the calculated illuminant is chosen for subsequent procedure. The variation among referenceandestimated one is estimated additionally. The block is assumed as spliced block, if the variance rate is higher when compared to predefined threshold.

2.2 Copy-move forgery detection

An illustration to understand copy move is given in Fig. 4. The detectionmethod of copy-move forgery undergoes classification into Keypoint basedandBlock based methods. For image matching, keypointsandinterest points are detected whereas block based methods employs blind search over image. Each detection technique employs a trivial channel that depends on the three main phases:

- Feature Extraction: For every pixel of interest, this is the fundamental step of any identification method where a relative feature is stored that demonstrates the nature of the image in its adjacent pixel.
- Matching: For forged regions detection, the every pixel top matching is drawn out after deriving appropriate features.
- Post-processing: It is performed to distinguish the top match over entire detected matched pair and to decrease the false alarm rate.

(a) Input

(b) Target

(c) Output

Fig. 4: Illustration for copy move method

Over every pixel, the above operations can be implied otherwise for few chosen keypoints that are not distributed to produce dense offset field. Keypoint dependent techniques are assumed speedier when compared to those techniques that depend on dense matching, since it performed over a little pixel set relatively. By employing SIFT features, [12] projected an initial method that tackle the various distortions types autonomously. Through RANSAC method [13], they assume statistical distortions. Alternate technique had been projected [14], in that numerous duplicate areas are taken care through hierarchical agglomerative clusteringorJ-linkage. The keypointsare categorized by employing local descriptors that are well-acclaimed such as DAISY, SURF,LBP, few local features. Even though the keypoint based methods are fast when compared to dense field, however, there exists a lack in accuracy. While copy-move links works only with smooth areas, the dense field work well especially, as it is difficult in smooth area to distinguish forgery. The research gap present in [15] inspires us to focus over the methods of dense field.

Complexity is the issue with dense field method. For the methods like post-processing,feature extraction and matching, each and every pixel is subjected to general three phase processes. Therefore, it is a major focus to feature extraction and it is easy to enhance the matching procedure speed. For the feature length minimization, various researchers build some methods to resolve this issue. To reduce the feature length and to derive the features, DCT is employed.

For feature extraction, [16] employed DWT and the model exhibits good outcomes but there exist a lack in rotation and rescaling. For minimizing the length of the feature, SVD is used [17] and PCA is used. They gained good results; however, while the operations like scaling and rotations are implied over the image, the performance gets minimized.

Considerable effort has been taken to avoid these issues with feature that deal with scaling and rotation efficacy. In this paper, well-suited features are provided by Circular harmonic transform (CHT) that is rotation invariant. To extractfeatures, Zernike moment (ZM) is employed that depend to CHT family. For forgery detection, to feature extraction, polar cosineandsine are employed [18].

a technique that merge ZM-polar (Zernike moment) and block discrete cosine transform (BDCT) as motivated by the works in the above section. Over copy-move forgery and splicing, this paper offers detection of forgery-based image. The major contribution of the projected method is the primary detection of the given image is illustrated or not. When the detection of image illustration is done, employing a convolutional neural network(CNN), we examine the existence of splicing forgery or copy-move. When copy-move is found, then additional processing is carried out for finding forged areas. Therefore, there exists a two-step procedure for forged image detection:

- Forgery detection by using CNN.
- Forgery Classification of (Copy-move or splicing).

III. PROPOSED MODEL

The overall process involved in the proposed modelis illustrated in Fig. 5. For image forgery detection, we project

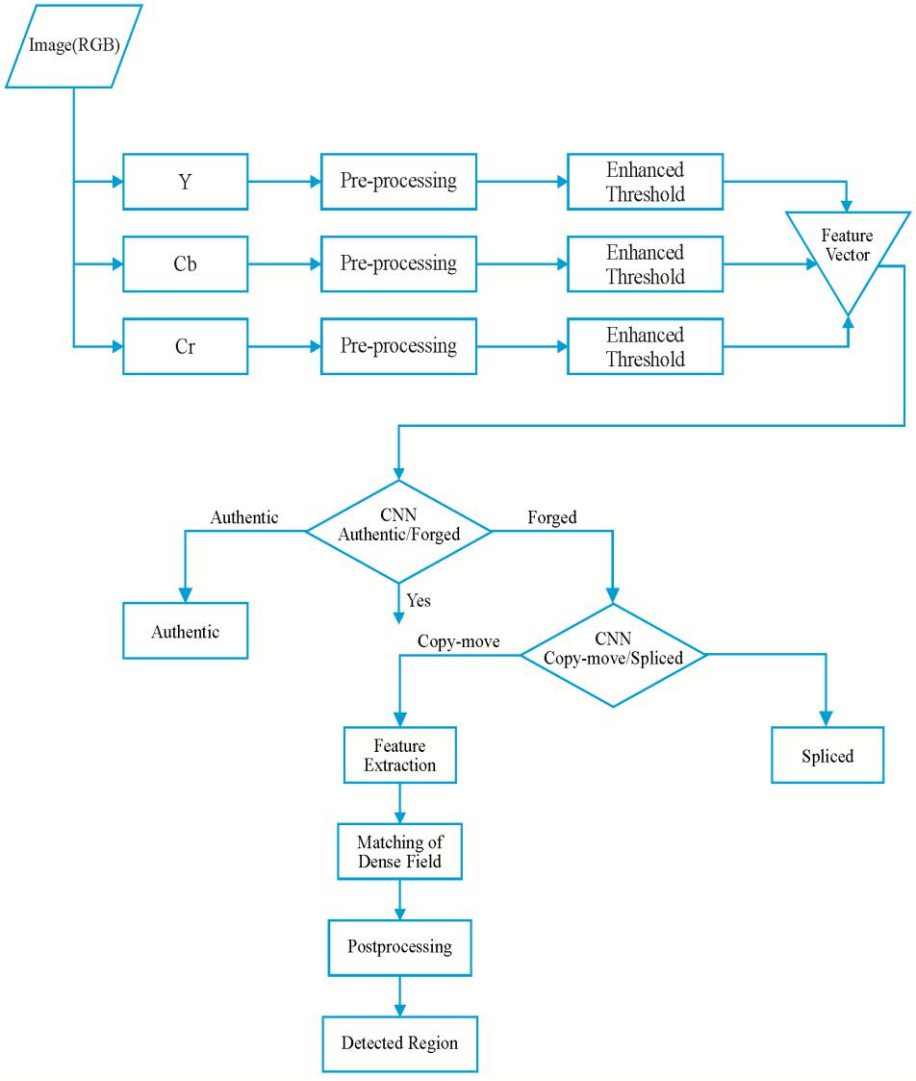


Fig. 5: Overall process of the proposed model

3.1 Detection of forgery using CNN

We will aim at decision making process in this section over an input image, either it is illustrated or not. We imply color image chrominance element, in spite of assuming image luminance part for extracting splicing artifacts. In detail, feature extraction and chrominance space in chroma space is demonstrated.

Chroma space

We employed YCbCrcolor model image format that is a color space family like RGB.

In this, Cr and Cb demonstrates Chroma channel or chrominance component, whereas luminance component is demonstrated through Y in this color model. Cr and Cb are the chrominance components that are known as red-difference and blue-difference correspondingly. In contrast to Cr or Cb, Y element stores high image contents. For extracting features, the luminance element of color image splicing detection method has high concern when compared to chrominance component. But, by using many splicing artifacts, we examined that chroma channel stores. Therefore, image chrominance element might be employed, to store splicing artifacts. To the authentic image in fig. 6, the bird region is spliced. It is noted that details of image mask in splicing is initiated in Y element through bird contour observation in Y. When comparing with other object in image, the bird's contour looks sharper. Therefore, the edges that get affected through splicing can be detected simply.

In Fig. 7, to derive the color image features, we projected a method in Chroma space depending on advanced threshold method. To minimize the effect of image content diversity that is caused, in the initial phase, a pre-processing step is performed such as image de-correlation and block discrete.cosine transform (BDCT) which is non-overlapping. For detection of forgery, to derive the discriminative feature in the subsequent phase, improved method of threshold is implied in matrix of image intensity. Over three chrominance component channels like Cr, Y, Cb, these are implied. For classification, the resultant features from Cr, Y and Cb are assumed as discriminative features. To improve gamma value and C, we implied RBF kernel and CNN; in that k-fold cross validation is employed.

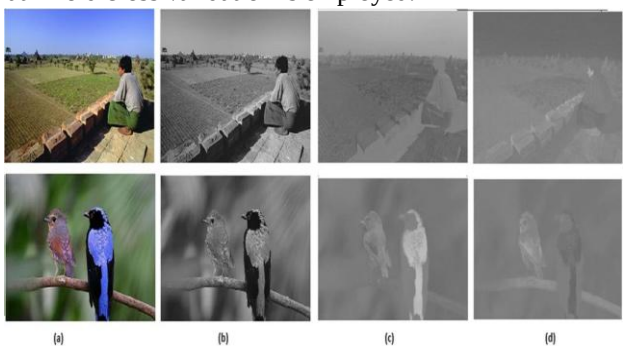


Fig. 6: Color model (a) RGB,(b) Y-channel, (c) Cb-channel, (d) Cr-channel

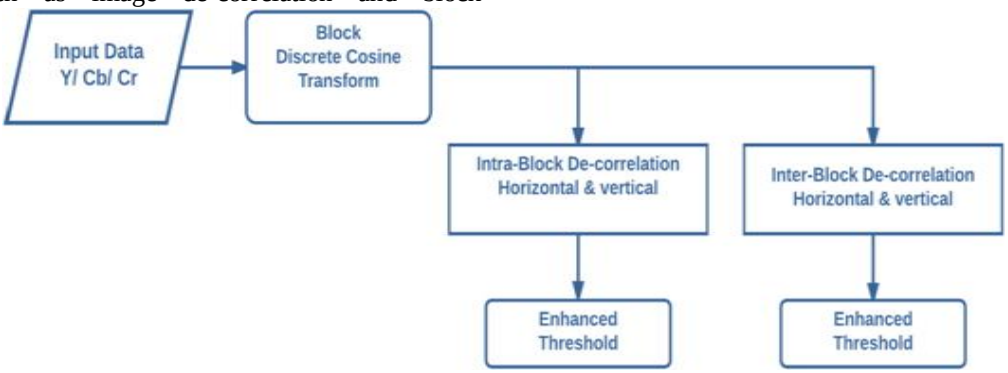


Fig. 7: Preprocessing model

Image pre-processing

It is complex to distinguish the apprehensive part of an image in detection of image forgery.So, we implicate pre-processing steps like image de-correlation and BDCT. Over source image, it includes 8×8 block-wise of non-overlapping transformation; S refers to the DCT block coefficient. The non overlapping BDCT that is N × N is shown in Fig. 7. In vertical and horizontal direction, the image de-correlation is estimated after DCT coefficient rounding to adjacent integer rate as below:

$$D_{intra}^{h} = S(i,j) - S(i+1,j) \quad (1)$$

$$D_{intra}^{v} = S(i,j) - S(i,j+1) \quad (2)$$

In vertical and horizontal direction, at the position (i,j) S (i,j) demonstrates the value of intensity, D_{intra}^{h} , D_{intra}^{v} , D_{inter}^{h} ,D_{inter}^{v} denotes inter-block de-correlated and de-correlated image.

Enhanced threshold method

Here, image splicing influence the actual image pixel correlation and procedure of Markov random to correlation characterization, and we project an improved threshold technique depending on the procedure of Markov random for extracting the features. The subsequent stated visited through the procedure in process of Markov chain is demonstrated through the current process state. This means X_t+1doesn't based on X_0 or X_t−1 but based on X_t. The matrix of One-step transition probability is described as:

$$P[X(t+1) = x_t + 1 \mid X(1) = x_1, X(2) = x_2, \ldots, X(t) = x_t]$$
$$= P[X(t+1) = x_t + 1 \mid X(t) = x_t] \quad (3)$$

At time t+1 and t, X(t+1) and X(t) are the states correspondingly and state transition is X(t+1) from X(t). At time t and state x, current Markov chain state and Markov chain probability would be at time t+1 in state y described through state transition probability (P_{xy}) or one step transition probability and it can be demonstrated through:

$$P_{xy} = P[X(t+1) = x \mid X(t) = y] \quad (4)$$

The local feature count is very large in transform domain. Hence, there exist process requirements that delete the variation in de-correlation rates.

The rate $Tr_x^b(u,v)$ is truncated and is described as

$$Tr_x^b(u,v) = Thr\left(abs(D_x^b(u,v))\right), \quad (5)$$

And,

$$Thr(A) = \begin{cases} A, & if\ |A| \leq T \\ sign(A)T, & otherwise \end{cases} \quad (6)$$

When the element rate in de-correlation matrix $Tr_x^b(u,v)$

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

is> T or <−T, then it will be replaced with T or -T correspondingly.Within the range of [(−T, −T + 2...T + 2, T)] as a subsequent phase to pre-processing, threshold T is demonstrated. This also aids in reducing the feature vectors dimension when comparing with existing standard method. The feature matrix elements linked with improved threshold procedure implied to Tr_{intra}^{h} are demonstrated through,

$$p\left(T_n^b(u+1,v)|T_m^b(u,v)\right) = \sum_{u=1,}^{S_u-2}\sum_{v=1}^{S_v-1}\delta\left(T_{m,m-1}^b(u,v), T_{n,n-1}^b(u+1,v)\right) * \emptyset_{intra} - 1 \quad (7)$$

$$p\left(T_n^b(u,v+1)|T_m^b(u,v)\right) = \sum_{u=1,}^{S_u-1}\sum_{v=1}^{S_v-2}\delta\left(T_{m,m-1}^b(u,v), T_{n,n-1}^b(u,v+1)\right) * \emptyset_{inter} - 1 \quad (8)$$

And, δ function in the (7) and (8) is demonstrated as,

$$\delta(A=m,B=n) = \begin{cases} 1 & if A = m and B = n \\ 0 & otherwise \end{cases} \quad (9)$$

Therefore, we store a sum of 4 (T+1)×(T+1) features through implying improved threshold procedure shown above,. We store high Markov characteristics, through (11) and (12) to inter-block Tr_{inter}^{v} to assume inter-block correlation through 8×8 BDCT.

$$p\left(T_n^b(u+8,v)|T_m^b(u,v)\right) = \sum_{u=1,}^{S_u-16}\sum_{v=1}^{S_v-8}\delta\left(T_{m,m-1}^b(u,v), T_{n,n-1}^b(u+8,v)\right) * \emptyset_{inter} - 1 \quad (10)$$

$$p\left(T_n^b(u,v+8)|T_m^b(u,v)\right) = \sum_{u=1,}^{S_u-8}\sum_{v=1}^{S_v-16}\delta\left(T_{m,m-1}^b(u,v), T_{n,n-1}^b(u,v+8)\right) * \emptyset_{inter} - 1 \quad (11)$$

With the extracted features from above equations, these features are merged to create a feature vector that is assumed for splicing detection in discriminative feature. Separately, from Cb, Y and Cr channel, 2 × 4×(T+1)×(T+1) features are derived. That is for splicing detection to construct a discriminative feature vector, sum of 3×2 × 4×(T+1)×(T+1) features are extracted.

3.2 Feature extraction for copy-move forgery

We have assumed features depending on Circular Harmonic Transform (CHT) that have variant features.Over a consequent space, let us assume a scalar image I(x, y), where (x, y)∈R^2 and I (ρ, θ) refers the polar coordinates illustration with ρ ∈ [0, ∞] and θ ∈ [0,2π]. For examining the CHT coefficients, the common function can be expressed through

$$F_I(n,m) = \int_0^{2\pi}\int_0^{\infty} I(\rho,\theta)\, k_{n,m}^{*}(\rho,\theta)\rho d\rho d\theta \quad (12)$$

Where

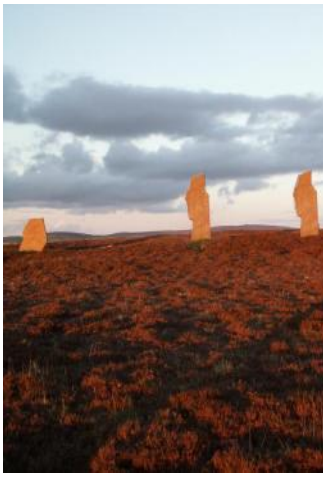
$$K_{n,m}(\rho,\theta) = R_{m,n}(\rho)\frac{1}{\sqrt{2\pi}}e^{jm\theta} \quad (13)$$

It denotes that the common function $K_{n,m}(\rho,\theta)$ refers the product of a radial profile$R_{m,n}(\rho)$ and circular harmonic.

IV. EXPERIMENTAL VALIDATION& TESTING RESULTS

This section discusses the validation of the presented model and a comparison the some of the recently presented models. For experimental analysis, CASIA v1.0 and CASIA v2.0 [19] tampered image detection evaluation dataset is employed for investigating the performance of the presented model. CASIA v1.0 holds 800 authentic and 921 spliced color images of sizes 384×256 and, each image is in JPEG form with no post-processing. Fig. 8 depicts the sample authentic, spliced and copy-moved images from CASIA v1.0. In addition, CASIA v2.0 holds large size dataset with various size images and difficult operation or post-processing among edges is employed. It comprises of 7491 authentic and 5123 tampered color images with various sizes of 240×160 to 900×600 pixels. When compared with the first dataset, it has original image with various Q values of JPEG images. The authenticated images are gathered from Corel image dataset. The tampered images are generated as follows:

- Portions of images are cropped and pasted arbitrarily
- The portions of copied image regions undergo processing under various functions such as resizing, rotation or other distortions and then being pasted to produce the tampered image.
- Once the portions are cropped and pasted, post-processing operation will takes place to complete the process of generating tampered images.
- Various sizes of tampered portions are taken.




Life's Noodle
Shop & Grill

Fig. 8: Sample test images

A detailed experimentation takes place on the image dataset CASIA v1.0 and CASIA v2.0 [19]. As the image dataset CASIA v2.0 contains many authenticated images compared to forged ones, hence, to maintain the tradeoff among the authenticated and forged ones, a set of 5123 images are arbitrarily selected from the existing 7413 authenticated images and identical image count is chosen from forged type. At the end, to evaluate the results of the proposed method, a total of 80% of the images are used to train and rest of the 20% are used to test the model. The above procedure is iterated over 50 times to determine the performance measures of the presented approach. Fig. 9 shows the input images and the corresponding segmented portions.

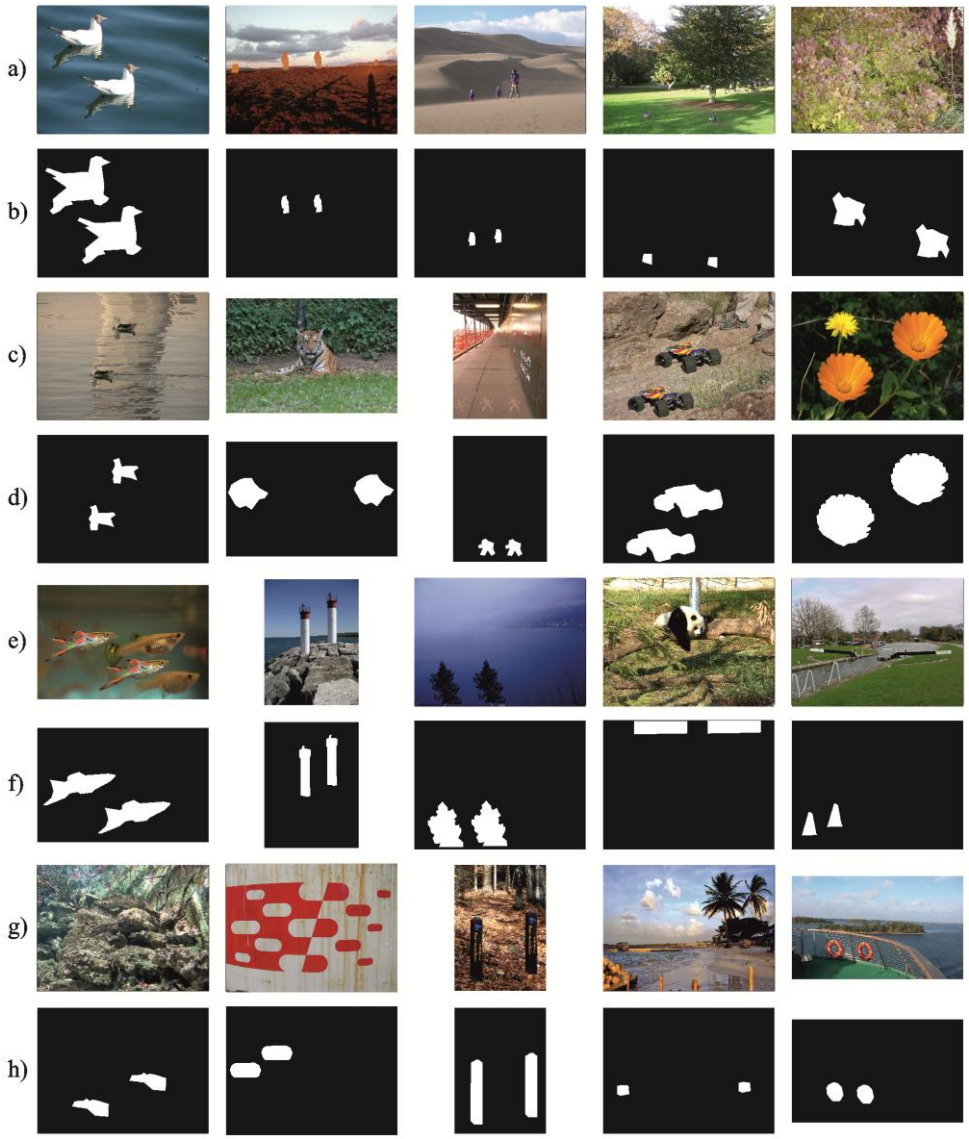


Fig. 9: Input image and its segmented portions

Table 1 provides the obtained results of the presented model interms of three evaluation parameters namely true positive rate (TPR), true negative rate (TNR) and accuracy. The evaluation parameters are equated as follows:

$$TPR = \frac{TP}{TP+FN} * 100 \quad (14)$$

$$TNR = \frac{TP}{FP+TN} * 100 \quad (15)$$

$$ACCURACY = \frac{TP+TN}{TP+FN+FP+TN} * 100 \quad (16)$$

where, TP is the number of authenticated images that are properly identified, TN is the number of spliced images that are properly identified, FP is the number of authenticated images that are wrongly identified and FN is the number of spliced images that are wrongly identified.

Table 1 shows the detection results of the copy-move forgery type. Fig. 10 shows the comparative results attained by the presented and compared methods interms of TPR, TNR and accuracy. From the table, it is evident that the presented model exhibits maximum results with a maximum TPR of 98.91, TNR of 99.16 and accuracy of 99.03. The recently presented SVM based model shows better results than the compared methods with a TPR of 97.18, TNR of 97.34 and accuracy of 97.26.

Table 1: Detection performance of copy-move forgery

Methods	TPR	TNR	Accuracy
[20]	93.27	94.30	93.78
SRM [21]	94.32	95.12	94.72
He et al. [22]	94.98	95.10	95.04
SPAM [23]	96.35	96.22	96.20
SVM [24]	97.18	97.34	97.26
Proposed	98.91	99.16	99.03

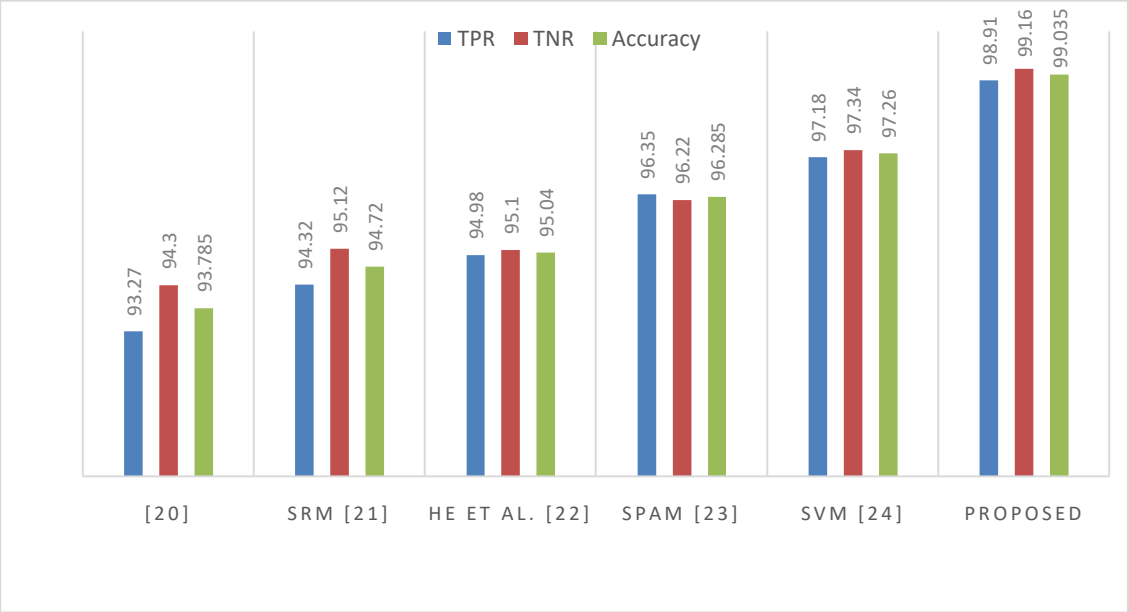


Fig. 10: Comparison of proposed with existing models on copy-move forgery images

Similarly, Table 2 shows the detection rate of the Spliced forgery type. Fig. 11 illustrates the comparison of various approaches interms of TPR, TNR and accuracy. From the table, it is noticeable that the CNN based model shows superior results with the highest TPR of 98.98, TNR of 99.24 and accuracy of 99.11. The recently presented SVM based model shows better results than the compared methods with a TPR of 97.59, TNR of 97.98 and accuracy of 97.78.

Table 2: Detection performance of Splicing forgery

Methods	TPR	TNR	Accuracy
[20]	94.56	95.37	94.96
SRM [21]	95.38	96.35	95.86
He et al. [22]	94.56	95.90	95.23
SPAM [23]	97.36	96.89	97.12
SVM [24]	97.59	97.98	97.78
Proposed	98.98	99.24	99.11

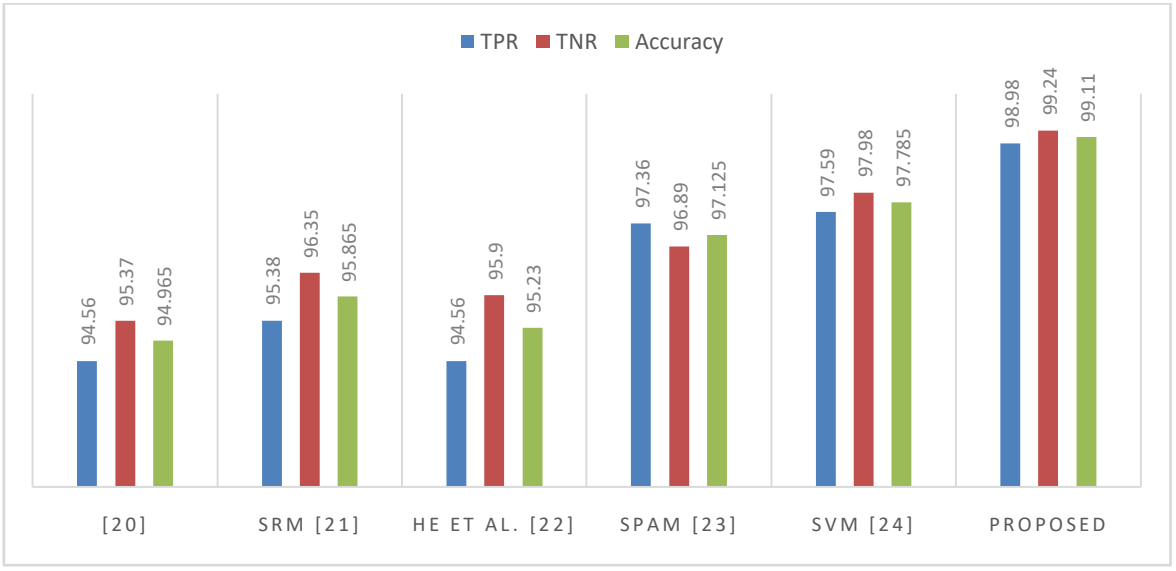


Fig. 11: Comparison of proposed with existing models on spliced images

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

V. CONCLUSION

This paper has presented a novel image forgery identification method which dealt with splicing and copy-move forgeries concurrently. At the initial stage, the transformation of the input image to YCbCr channels takes place. Next, BDCT and image de-correlation takes place as the pre-processing step. Once the filtered features are integrated, the model will be trained using good and forged images. Then, CNN is employed for classifying an image as spliced type or copy-move type. The simulation values depict the better performance of the presented model. For the copy move images, CNN accurately classifies with an accuracy of 99.03 whereas a maximum accuracy of 99.11 is attained for the spliced images. As a part of future scope, the proposed model will be implemented on a difficult dataset to validate the betterment of the projected model.

REFERENCES

1. S. Lyu and H. Farid, “How realistic is photorealistic?” IEEE Transactions on Signal Processing, vol. 53, no. 2, pp. 845–850, 2005.
2. H. Farid, “A survey of image forgery detection,” IEEE Signal Processing Magazine, vol. 2, no. 26, pp. 16–25, 2009.
3. Muhammad, Najah, Muhammad Hussain, Ghulam Muhammad, and George Bebis, "Copy-move forgery detection using dyadic wavelet transform.", In Proceedings of IEEE Eighth International Conference on Computer Graphics, Imaging and Visualization (CGIV-2011), pp. 103-108, 2011.
4. J. Granty Regina Elwin, T. S. Aditya, and S. Madhu Shankar, “Survey on passive methods of image tampering detection,” in Proceedings of the International Conference on Communication and Computational Intelligence (INCOCCI ’10), pp. 431–436, December 2010.
5. Pun C-M, Bo L, Yuan X-C (2016) Multi-scale noise estimation for image splicing forgery detection. J Vis Commun Image Represent 38:195–206
6. 20. Hakimi F (2015) Image-splicing forgery detection based on improved lbp and k-nearest neighbors algorithm. Electron Inf Plan, 3
7. Shi Y, Chen C, Chen W (2007) A natural image model approach to splicing detection. In: Proceedings of the 9th workshop on Multimedia & security, pp 51–62. ACM
8. Wang W, Dong J, Tan T (2009) Effective image splicing detection based on image chroma. Image Processing (ICIP), 2009 16th IEEE International Conference on, pp 1257–1260. IEEE
9. Li X, Jing T, Li X (2010) Image splicing detection based on moment features and hilbert-huang transform. In: 2010 IEEE international conference on information theory and information security (ICITIS), pp 1127–1130. IEEE
10. Zhao X, Li J, Li S, Wang S (2011) Detecting digital image splicing in chroma spaces. Digital Watermarking 6526:12–22
11. Wu X, Fang Z (2011) Image splicing detection using illuminant color inconsistency. In: 2011 3rd international conference on multimedia information networking and security (MINES), pp 600–603. IEEE
12. Pan X, Lyu S (2010) Region duplication detection using image feature matching. IEEE Trans Inf Forensics Secur 5(4):857–867
13. Fischler MA, Bolles RC (1981) Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography. Commun ACM 24(6):381–395
14. Amerini I, Ballan L, Caldelli R, Bimbo AD, Serra G (2011) A sift-based forensic method for copy–move attack detection and transformation recovery. IEEE Trans Inf Forensics Secur 6(3):1099–1110
15. Christlein V, Riess C, Jordan J, Riess C, Angelopoulou E (2012) An evaluation of popular copy-move forgery detection approaches. IEEE Trans Inf Forensics Secur 7(6):1841–1854
16. Muhammad G, Hussain M, Bebis G (2012) Passive copy move image forgery detection using undecimated dyadic wavelet transform. Digit Investig 9(1):49–57
17. Zhao J, Zhao W (2013) Passive forensics for region duplication image forgery based on harris feature points and local binary patterns. Math ProblEng 2013:12
18. Li Y (2013) Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching. Forensic SciInt 224(1):59–67
19. Dong J, Wang W, Tan T (2013) Casia image tampering detection evaluation database. In: Signal and information processing (ChinaSIP), 2013 IEEE China Summit & International Conference on, pp 422– 426. IEEE
20. Zhang Q, Wei L, Weng J (2016) Joint image splicing detection in dct and contourlet transform domain. J Vis Commun Image Represent 40:449–458
21. Qiu X, Li H, Luo W, Huang J (2014) A universal image forensic strategy based on steganalytic model. In: Proceedings of the 2nd ACM workshop on Information hiding and multimedia security, pages 165–170. ACM
22. He Z, Wei L, Sun W, Huang J (2012) Digital image splicing detection based on markov features in dct and dwt domain. Pattern Recogn 45(12):4292–4299
23. Pevny T, Bas P, Fridrich J (2010) Steganalysis by subtractive pixel adjacency matrix. IEEE Trans Inf Forensics Secur 5(2):215–224
24. ChoudharyShyam Prakash1 · Avinash Kumar1 · Sushila Maheshkar1 · VikasMaheshkar, "An integrated method of copy-move and splicing for image forgery detection", Multimed Tools Appl, 2018