



Texture based Image Splicing Forgery Recognition using a Passive Approach

Asif Hassan^{1*}, V K Sharma¹

¹Department. of ECE,
Bhagwant University, Ajmer, INDIA

*Corresponding Author

DOI: <https://doi.org/10.30880/ijie.2021.13.04.010>

Received 5 August 2020; Accepted 4 March 2021; Available online 30 April 2021

Abstract: With the growing usage of the internet in daily life along with the usage of dominant picture editing software tools in creating forged pictures effortlessly, make us lose trust in the authenticity of the images. For more than a decade, extensive research is going on in the Image forensic area that aims at restoring trustworthiness in images by bringing various tampering detection techniques. In the proposed method, identification of image splicing technique is introduced which depends on the picture texture analysis which characterizes the picture areas by the content of the texture. In this method, an image is characterized by the regions of their texture content. The experimental outcomes describe that the proposed method is effective to identify spliced picture forgery with an accuracy of 79.5%.

Keywords: Copy move forgery, gray level co-occurrence matrix, image splicing forgery, texture segmentation

1. Introduction

In today's era, it is too simple to share access and process data in the form of images. Traditionally we had self-assurance in the authenticity of images, however, with the rapid growth of digital technology in terms of robust algorithms like Photoshop and advanced cell phone applications for modifying digital images, the question of its authenticity is raised. Practically, digital images are found in media networks, technical journals, governmental campaigns, courtrooms etc. Sometimes it is too tough to identify reliable and manipulated images. In general image forgery is the process of altering the originality of digital images which is not visible to the human eye.

Nowadays government and private organizations are concerned with paperless work like e-government services which requires the data to be stored in digital format. Unfortunately, several data like documents and images are all vulnerable to manipulations, which make challenging to secure authentic data. This gives rise to an interest among the researchers to develop image forensics methods towards identifying authentic digital pictures.

Image Forgery detection can be classified into *Active Forgery* detection and *Passive Forgery* detection. In Active forgery detection, watermarking and digital signature which is embedded into the image is confirmed during detection to identify the authenticity, but this technique has limitations because they require human involvement or special cameras. To overcome these limitations, various passive authentication methods are used.

A passive method does not require previous data about the images, and this method takes assistance from specific noticeable differences that forgeries can bring into the image. In the passive approach detection of forged images is done without the knowledge of the original image. The evidence or traces left on the image during image manipulations are used for the detection of forgery. The amount of forgery and position of forgery in the image can also be determined with a passive approach.

Two subtypes of Image forgery are Image Splicing and Copy-move forgery. The process of creating an amalgamated image by cutting a few picture areas and pasting them to different pictures is called Image Splicing.

Compared to Copy-move forgery, image splicing is difficult to identify because in the Image Splicing technique dissimilar objects are included along with the dissimilar texture and in Copy-move Forgery, it is simple to identify because of the same objects along with similar texture in the same picture.

Figure 1(c) represents a spliced picture that shows John Kerry and Jane Fonda at an anti-war. In the period of the American presidential election campaign in 2004, this picture was forged by combining two original pictures. Figure 1(a) and Figure 1(b) represents the actual image [1]. The Image Splicing technique is extensively used for forgery of image, which contains particular adverse public impacts.



Fig 1 - An example of Spliced image forgery

Digital image forgery detection techniques are classified as Pixel-based image forgery detection, Format-based image forgery detection, and Camera-based image forgery detection, Physical environment-based image forgery detection and Geometry-based Image forgery detection.

The pixel-based method emphasizes the pixels of an image. These methods are commonly classified as copy-move, Image splicing and image re-sampling. The most common image manipulation technique is Image splicing.

The format-based method is based on image formats, in which JPEG format is desirable. For image forgery detection, Statistical correlation is introduced by precise lossy compression patterns. These methods are classified as JPEG quantization, Double JPEG and JPEG blocking. It is very difficult to identify image forgery if the images are compressed. But these methods can identify image forgery even if the images are compressed.

In *the Camera-based method*, when an image is acquired from a digital camera, the image is sent to the memory through the camera sensor. It undergoes various processing stages like quantization, gamma correction, colour correlation, white adjusting, filtering, and JPEG compression. These processing steps from acquiring the image to saving the image in the memory may depend upon the camera model and camera antiques. These methods classified as chromatic aberration, colour filter array, and camera response and sensor noise.

The physical environment-based method depends on three-dimensional relations between physical object, illumination and the camera. This method is based on the illumination under which an image is captured. Illumination is a very significant factor for capturing an image. Distinctions in illumination in an image can be used as proof for forgery. These techniques are classified as light direction (2-D), light direction (3-D) and light environment.

The geometry-based method is based on the projection of the camera focus onto the image, hence object in the world and their location will be relative to the camera. Geometry-based methods are classified as principle point and metric measurement.

Image Segmentation is used to identify particular entities and also to separate foreground content from background content. Dividing an image into a smaller number of similar regions highlights essential features. It makes the analysis of the image easier. Image segmentation approaches can be categorized as a region-based method and edge-based method. Image textures, grey values, colour values and structural features are the only option to derive information from an Image. Texture based analysis is used from the beginning of digital image processing. Single texture features are not suitable for texture segmentation because of different viewing conditions, illumination conditions and shadows. Hence image segmentation analyses are carried out using couples of texture features.

The other sections of this paper are arranged as below: In section-2, Image texture, Section-3, Related Work of Image Forgery detection techniques, section-4, a summary of Proposed Method, section-5 Experimental Results and section-6 conclusion.

2. Image Texture

A texture is a group of texture components or “*texels*” that are present in some patterns in an image. Image Texture gives information about the arrangement of intensities or colour in the spatial domain. Segmentation of an image can be done by using image texture. Image texture detects different textured and non-textured regions in an image to categories or segment different texture regions in an image and to extract boundaries amongst the texture regions. It is a very challenging concept to characterize the Image Texture. Modelling the texture as a two-dimensional gray level

distinction is used for the identification of specific textures in an image. The illumination of pairs of pixels is calculated as the amount of contrast and consistency. Figure 2 represents segmented into different texture regions.

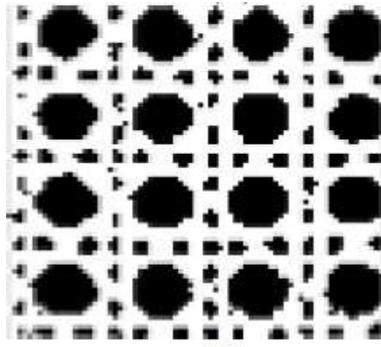


Fig 2 - Example of Image texture Segmentation

Image texture analysis methods are classified as Structural method, statistical method, model-based method and transform method.

The structural method characterizes texture by its primitive which is known as micro-texture and also by spatial arrangements which are known as macro-texture of those primitives. To describe image texture, the primitives must be defined. The chosen primitive and its probability to be positioned at a specific location in an image is the function of location or the primitives near that location. The structural approach provides a good figurative description of an image but, this method is more suitable for the synthesis of the image than an analysis of the image. The abstract descriptions cannot be properly defined for natural textures because of the inconsistency in both micro-texture and macro-texture. Mathematical morphology is one of the tools for structural texture analysis.

The statistical method is used to characterize the texture indirectly by non-deterministic properties of the gray levels of an image. The information provided by the pairs of pixels achieves more discrimination rates than the transform-based approach and structural approach. The textures in gray images distinguish only if they differ in second-order moments. The co-occurrence matrix is the most popular second-order statistical feature for texture analysis. For texture classification, the approach based on co-occurrence matrices has good performance than the transform-based method.

The model-based method uses fractal and stochastic models. This method represents an image texture by using an image model and a stochastic model. The image is analyzed by estimating and using the parameters of the model. The major problem of this method arises in the computational complexity of the estimation of stochastic model parameters. For modelling natural textures, a fractal model is more useful. It can be used for texture analysis but it is not appropriate for the identification of local image structures and it lacks location selectivity.

The transform method is used to characterise an image in a space whose co-ordinate system is closely related to the characteristics of a texture such as frequency or size. The performance of methods based on the Fourier transform is very poor due to the absence of spatial localisation. For better spatial localization, Gabor filters can be used but, practically they are less useful because in natural textures generally there is no single filter resolution that can localise a spatial structure. Wavelet transform has many advantages compared to Gabor transform. Wavelet transform allows the representation of textures at the most suitable scale by changing the spatial resolution. There is a wide range of choices for the wavelet function, so the wavelets best suited for texture analysis in a specific application can be chosen. The wavelet transform is best suited for texture segmentation. The major issue with wavelet transform is that it is not translation-invariant

3. Related Work

To identify the introduction of the higher-order un-natural correlations as a signal by the process of forgery, Farid [2] gives one technique that depended on bi-spectral analysis and is developed for identifying human-speech splicing. For the identification of image splicing, Chang and Ng [3] presented one technique that depends on the usage of bi-coherence phase and magnitude characters and obtained the 70% of identification accuracy. Abrupt splicing leads to discontinuity which is identified by other techniques which have been introduced by a few authors and are done by using bi-coherence [4].

Tsui and Ng [5] and Ng T.T. [6] implemented one technique that utilizes “linear geometric invariants by picture and therefore generated the characters of CRF signature by planes linear in picture irradiance. Generation of CRF signature by picture, the authors implemented a technique depended on the edge profile. Here reliable generation is done depending on the reality that is the edges must be broad and straight. Threshold edge picture GLCM is used. For identification of splicing for colour pictures Wang et al.[7], introduced a technique by using a gray level co-occurrence matrix (GLCM).

Xuefang et al.[8], introduced a technique that generates characters and a statistical model which utilizes the characteristic operations moments upon the use of wavelets to identify the spliced area and this is also done by Hilbert–

Huang transform (HHT). For the identification of passive splicing, this technic provides maximum accuracy. The method which measures four vectors with four directions which are provided by de-correlated chroma channels and the technique was implemented by Zhao et al. [9], which utilizes the gray level, run length, texture character and chroma space and above are used as an identical character for the division Support Vector Machines (SVM) and identification of picture splicing was established.

By using photometric consistency of lights, Liu et al. [10], implemented a technique in which the value of Shadow Matte is utilized to calculate colour features of shadows by utilizing photometric consistency. Detection method proposed by Xuemin et al. [11], Image Splicing Identification technique utilizes illuminant colour inconsistency. Based on blocks content light colour is decided for every block, provided the picture is classified as overlapping blocks. Variation among the reference and predicted light colour is calculated. For division purpose threshold is utilized and the block is considered as a forged block when the variation is more than a threshold.

To identifying splicing, the Run length-dependent technique is proposed by Zhongwei et al. [12]. The computation of run length is in the direction of the edge gradient. For a provided picture, an edge gradient dependent matrix is measured. By the histogram of the approximate run length, characters are formed. Therefore to increase the identification accuracy, run length is used upon the reconstructed and error pictures which are provided by the implementing Discrete Wavelet Transform (DWT) to get several characters. To divide the spliced and authentic pictures SVM is used. In Zhongwei et al. [13], Markov feature dependent technique is introduced. The co-efficient of Discrete Cosine Transform (DCT) is measured by utilizing Markov characters correlation of inter-block and intra-block between the blocks.

SVM is implemented as a classifier and SVM-RFE is utilized to minimize the character complexity and dimension, de Carvalho et al. [14] introduced a technique for the identification of inconsistencies in colour picture illumination. The technique is suitable for a picture that consists of more than two or more people. From illuminant estimators Edge dependent and texture characters are generated, which are given to the approach of machine-learning. This method does not need professional collaboration and systematizes the method of making the decision. For identification and division, SVM is utilized at rates of 86% on a set of information containing 200 pictures and 83% on 50 pictures counted by the Internet. Rao et al. [15], introduces a detection method that is dependent on blur. By calculating inconsistencies this approach shows the splicing by evaluating inconsistencies in space-variant blurring situations and also in motion blur.

Chi Man Pun et al. [16] suggested a technique based on noise inconsistencies amongst the spliced image and original image to detect the forged images. Initially, the image is alienated into multiple-scale pixels. The noise level function is calculated for every single scale and examined the portion. If the portion is lower than the level of the noise, then it is considered a dubious region. Finally, the pixel clusters of a dubious region are treated as the region that is spliced. The spliced area's variable noise concentrations show the presence of forgery. The multi-scale investigation produced the outcomes. This method is appropriate to identify the splicing of numerous objects.

D Vaishnavi et al. [17] suggested a technique that works to identify the image splicing which is based on digital watermarking. Spliced image is formed when two images are combined. An image is considered as a forged image if the watermarking which will be retrieved from the image indicates the existence of certain noise. This technique is an active forgery detection method.

Using Support Vector Machine (SVM) and Hidden Markov Models (HMM) classifiers, M F Hashmi et al. [18] suggested the tampering identification techniques. In this method, digital images are characterized by their feature vector. DCT, Local Binary Patterns (LBP), multi-scale directional transform and linear filters, extract the image attributes used for texture analysis. The system performance is improved when the images are tested using HMM as well as SVM models and the outcomes got by this method obtained respectable accuracy.

A Agarwal et al. [19] proposed a method using entropy filter and Local Phase Quantization (LPQ) that works on passive forgery recognition technique. When the images are spliced then it interrupts the fundamental information that will be noticed through this technique. The entropy filter gives uncertainty in the pixels in the nearby region. Hence Entropy filter highlights the edge of the manipulated image. The LPQ operator provides the phase statistics gives the statistic quantities of the image. Initially, the image is transformed from the RGB colour domain to YCbCr. Then the Cb and Cr constituents are obtained. Cb, as well as Cr constituents, are filtered using an Entropy filter. The feature matrix can be identified by assessing the image histogram by applying the LPQ operator to the filtered image. Finally, the image is classified as a forged or original image using an SVM classifier. Columbia, CASIA v1.0, v2.0 datasets are used by the author to evaluate forgery in an image. This technique is strong enough for the forgery of Copy-move and image splicing.

Zenan Shi et al. [20] suggested an original blind tampering identification technique based on Run Length Matrix on Fuzzy LBP (RLM-FLBP). Initially, the gradient sequence of every pixel is calculated by using an edge gradient matrix for an image and then measured in all directions. Using each pixel's gradient direction, the fuzzy histogram, grade of variation the total histogram are calculated.

Then the three instants distinguishing function of histograms are estimated and these are known as histogram characteristics that help identify image splicing The Fuzzy run length increases the topographies of variation calculating histogram to differentiate the forged and original image.

The method discussed above has three main drawbacks. Small and classical tampering may be unidentified. For a reliable generation, it needs the wide necessity of wide edges. Blur identification technique is failed when calculation and are needed to mask the sharp edges ailments after image splicing.

The proposed technique depends on the picture texture analysis which characterizes the picture areas by the content of the texture. Some intuitive qualities have been explained by terms like hard, soft, bumpy and silky as an operation of the spatial difference in pixel intensities and these are calculated by texture analysis. A difference in the values of intensity or the levels of gray represents the roughness or bumpiness. Some applications of texture analysis are automated inspection and remote sensing. These are more useful when entities in a picture are categorized by their texture instead of image intensity. Processing of the medical picture and the detection of texture boundaries is called texture segmentation.

4. Proposed Method and discussion

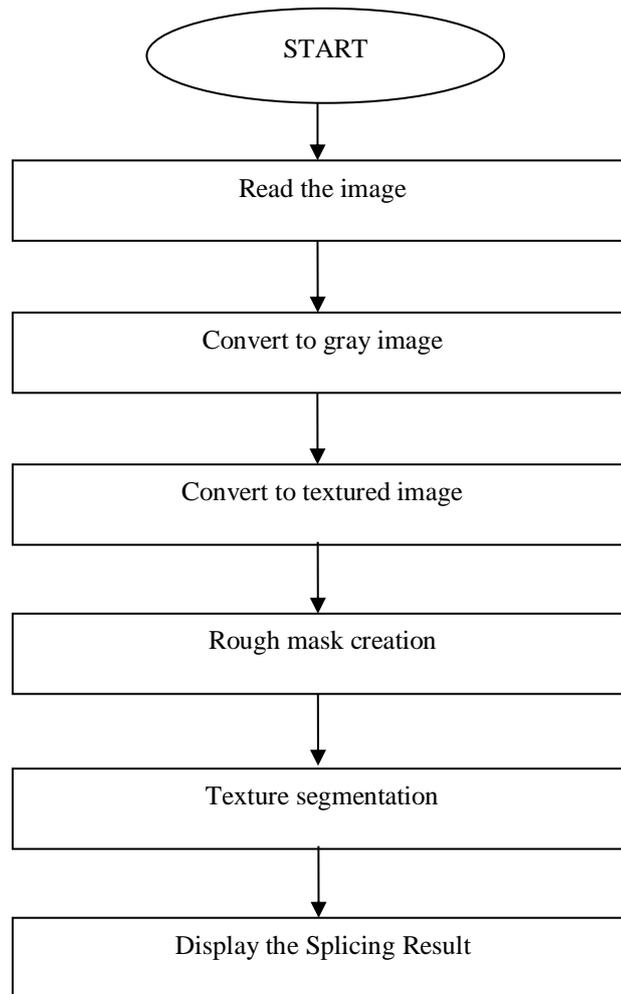


Fig 3 - Flow chart of the process

The flow chart of the proposed system is shown in Figure 3. The Proposed method is explained in the following steps:

Read Picture

Read Image and convert the picture to grey from RGB. The *RGB to gray* function converts RGB pictures to grayscale (I) while keeping luminance by removing the saturation and hue message.

$$I = 0.2989 * R + 0.5870 * G + 0.1140 * B \quad (1)$$

Here, R refers to Red, G refers to Green and B refers to the Blue component of the RGB colour picture respectively. 'I' indicate the Luminance component of the equivalent RGB pixel value.

Texture Picture Creation

An entropy filter is used for the formation of the texture picture. Entropy value indicates the complexity present in neighbourhood pixels. Variation in gray level distribution can be detected by the Entropy filter. Entropy filter operation returns an array where every output pixel consisting of the 9-by-9 surrounding entropy value around the respective pixel input pictures ‘I.’ Statistical calculation of randomness is referred to as Entropy. Let the entropy filter image be ‘E’. To rescale the texture picture ‘E’, the `mat2gray` function is used. Therefore for double picture values are in the default range. The resulting image is ‘Eim.’

The classical entropy of a grayscale picture is measured by *Entropyfilt* operation. Statistical calculation of randomness refers to Entropy. Statistics are characterized by picture texture since it gives the message of the classical differentiability of pixels intensity value in a picture. The range of values in regions beside smooth texture is the least value around a pixel; in regions of rough texture, the range of values is larger. In the same way, the degree of inconsistency of pixel values in that region can be calculated using the standard deviation of pixels in the neighbourhood.

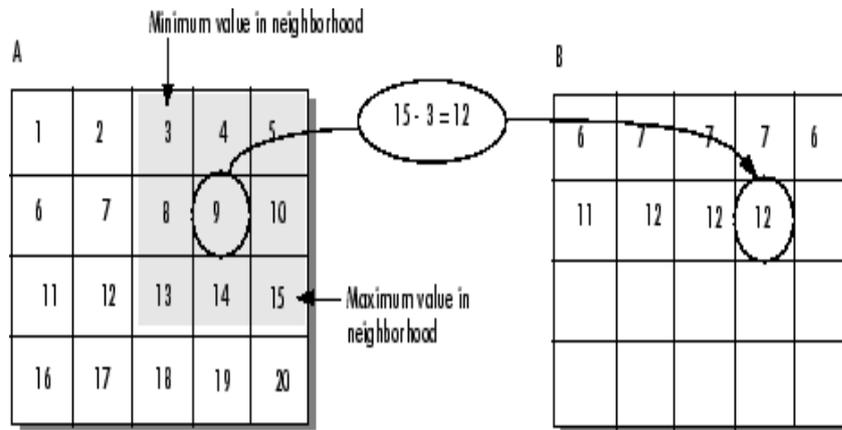


Fig 4 - Examining values of pixel in range filtered output picture

Surrounded pixel of interest defines the operation Entropy filter. It measures the surrounding statistic to estimate the pixel value of the output picture. This operation provides the values to the output Pixel and measures the surrounding entropy. The operation *entropyfilt* defines a 9-by-9 neighbourhood around the pixel of interest by default. An example is shown in Figure 4.

Formation of Rough Mask for the Bottom Texture

The intensity level of the object and the background pixels are clustered into two-dominant modes. Selecting threshold 0.8 is one way of separating the object from the background. This threshold value is selected randomly. Then any region (x, y) for which $f(x, y) \geq 0.8$ is called the object point, else the region is called as background point.

Hence, the threshold $g(x, y)$ is defined as

$$g(x, y) = \begin{cases} 1; & f(x, y) \geq 0.8 \\ 0; & f(x, y) < 0.8 \end{cases} \quad (2)$$

Let the resulting image be ‘BW₁.’ All pixels in the input picture are replaced by level 1(white) when the luminance is higher than 0.8 and other pixels are replaced with level 0 (black). An example of the resulting image is shown in Figure

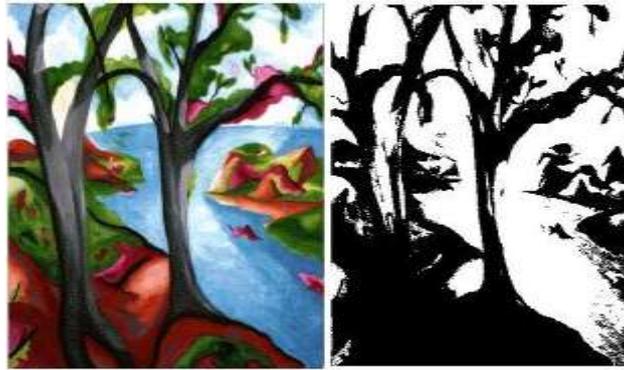


Fig. 5 - Illustration of the luminance image

If BW1 is compared with 'I', it is noticed that the bottom texture is almost entirely segmented and the top texture highly divided (several white objects). By using the function *bwareaopen* (BWao) the bottom texture can be generated. The function *BWao imclose* is used to close any other open holes in objects and for smoothing the corner lines. The function *closeBWao* is used to block up the holes in the objects.

Texture Segmentation

Top Texture segmentation using Rough Mask is used to compare the binary image rough mask to the real picture 'I'. Mask does not expand to the below end of the picture, there bottom texture mask is not perfect. Therefore, the function *roughMask* is used to segment the top texture. To measure the texture of the picture, *entropyfilt* is used. By using a rough mask top texture raw picture can be obtained by *Threshold E2im* using *graythresh* (BW2).

Area opening is the operation from a binary image (BW1), removes all known linked elements (components) instead of pixels P, generating other BW2 binary picture. Eight (8) is the avoidance connectivity for dual measurements, 26 for three dimensions, an `conndef(ndims(BW),'maximal')` for higher dimensions. Here P=2000 is used.



Fig 6 - illustration of area opening of an Image

If BW2 is compared with 'I', it is noticed that in BW2 two objects are divided. To obtain a mask for the top texture *bwareaopen* function is used as shown in the following equation.

$$BW2 = bwareaopen(BW1, P) \quad (3)$$

Segmentation Outcomes Display

The top and bottom textures are generated by using mask2 from 'I'. Then outline the boundary between the two textures and displayed as a result.

5. Experiments and Results

For the operation estimation, the proposed technique is tested on pictures that include 100 authentic and 100 spliced pictures with the resolution limit of 1200×900 pixels to 397×397 pixels. The tests were carried out on the MATLAB R2013a, RAM 2 GB and processor of 2.90 GHz.



Fig.6 a - STEP-1 Gray scaled Image



Fig.6 b - STEP-2 textured image creation



Fig.6 c - STEP-3 Rough Mask Image

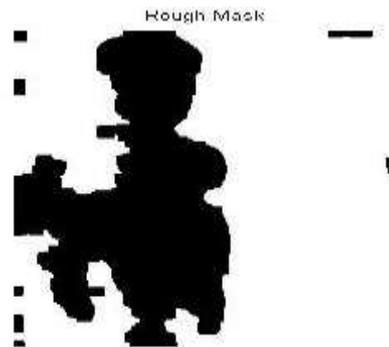


Fig.6 d - STEP-4 Texture Segmentation of an image



Fig. 6 e - STEP-5 Display the splicing result

To estimate the proposed method operation, the above-provided algorithm is followed. The proposed method is applied to our database which consists of both Spliced and original images. This database is created with a collection of 150 authentic and 150 spliced images from various internet sources. Figure 6 shows the Experimental outcomes generated by the Proposed Method.

True Negative (TN) and True Positive (TP) are measured where True Negative represents the authentic picture and is identified as real and True Positive represents the forged picture and is identified as real as represented in Table 1. Model accuracy is provided by the average of these two.

Table 1 - Accuracy of the proposed method

Image Type	Testing Images		
	Total Images	TP	TN
Authentic Image	150	-	81%
Spliced Images	150	78%	-

$$\text{The total accuracy} = \frac{TP+TN}{2} = \frac{78+81}{2} = 79.5\% \quad (4)$$

Out of 150 authentic images, 121 images are identified as authentic images and out of 150 spliced images, 117 images are identified as spliced images. The average of the TP and TN give the accuracy of the model of 79.5%. This technique provides good outcomes for both maximum resolution and uncompressed pictures, which represents its effectiveness.

6. Conclusion

Image forensics is a very popular research area due to the importance of digital pictures on magazine covers, in scientific journals and courtrooms and other areas. It is dominant to develop their identity since they can be tampered with by using several freely provided picture tampering tools and software. Depending on the characters of texture features of an image, here we introduced a digital picture forgery identification technique. The experimental outcomes describe that the proposed method is effective to identify spliced picture forgery. The identification accuracy is about 79.5%. Even though a major section of the spliced region is detected but some region of the spliced region is not detected. These two factors can be improved in future work.

Acknowledgement

I thank Dr. V K Sharma for his expertise and assistance throughout all aspects of my study and for his help in this research work. I give special thanks to my friend Er. Ghouse Ahamed Z for being there for me throughout this work.

References

- [1] El-Alfy, E. S. M., Qureshi, M. A.: 'Combining spatial and DCT based Markov features for enhanced blind detection of image splicing', *Formal Pattern Anal. Applications*, 2014, 18, (3), pp. 1–11
- [2] Hany Farid, *Detecting digital forgeries using bispectral analysis*, Technical Report, Massachusetts Institute of Technology 1999
- [3] Tian Tsong Ng, Shih-Fu Chang, A model for image splicing., *Proceedings of IEEE International conference on image processing (ICIP) 2004* pp. 1169–1172
- [4] Tian Tsong Ng, Shih-Fu Chang, Qibin Sun, Blind detection of photomontage using higher-order statistics, *proceedings of the International symposium on circuits and systems (ISCAS) 2004* pp. 688–691
- [5] Tian Tsong Ng, Mao-Pei Tsui, Camera response function signature for digital forensics - part I: theory and data selection. *Proceedings of the workshop on information forensics and security 2009* pp.156–160
- [6] Tian Tsong Ng, Camera response function signature for digital forensics – part II: signature extraction., *proceedings of the workshop on information forensics and security 2009*. pp. 161–165
- [7] Wei Wang; Jing Dong; Tieniu Tan, "Effective image splicing detection based on image chroma," *16th IEEE International Conference on Image Processing (ICIP)*, 2009, pp.1257-1260
- [8] Xuefang Li, Tao Jing, Xinghua Li, Image splicing detection based on moment features and Hilbert-Huang Transform, *IEEE International Conference on Information Theory and Information Security (ICITIS)*, pp.1127-1130
- [9] Zhao Xudong, Li Jianhua, Li Shenghong, Wang Shilin, Detecting digital image splicing in chroma spaces. *Proceedings of International workshop on digital watermarking 2010*. pp. 12–22
Qiguang Liu; Xiaochun Cao; Chao Deng; Xiaojie Guo, "Identifying Image Composites Through Shadow Consistency," *Information Forensics and Security, IEEE Transactions on*, vol.6, no.3, pp.1111,1122, Sept. 2011
- [10] Xuemin W., Zhen F., Image Splicing Detection Using Illuminant Color Inconsistency, *Int. Conf. Multimedia Inf. Networking and Security (MINES)*, 2011 pp. 600-603
- [11] Zhongwei He, Wei Sun, Wei Lu, Hongtao Lu, Digital image splicing detection based on approximate run length, *Pattern Recognition Letters*, Volume 32, Issue 12, 1 September 2011, Pages 1591-1597
- [12] Zhongwei H., Wei L., Wei S., Jiwu H., Digital image splicing detection based on Markov features in DCT and

- [13] DWT domain, *Pattern Recognition* 45 (2012) pp.4292–4299
- [14] de Carvalho, T.J.; Riess, C.; Angelopoulou, E.; Pedrini, H.; de Rezende Rocha, A, "Exposing Digital Image Forgeries by Illumination Color Classification," *Information Forensics and Security, IEEE Transactions on*, vol.8, no.7, pp.1182,1194
- [15] Rao, M.P.; Rajagopalan, AN.; Seetharaman, G., "Harnessing Motion Blur to Unveil Splicing," *Information Forensics and Security, IEEE Transactions on*, vol.9, no.4, pp.583,595, April 2014
- [16] Chi-Man Pun, Bo Liu, Xiao-Chen Yuan, "Multi-scale noise estimation for image splicing forgerydetection", *Journal of visual communication and image representation*, pp.195-206, 2016
- [17] D. Vaishnavi and T. Subashini, "Image Tamper Detection Based on Edge Image and Chaotic Arnold Map", *Indian Journal of Science and Technology*, vol. 8, no. 6, pp. 548–555, 2015
- [18] M. F. Hashmi and A. G. Keskar, "Image Forgery Authentication and Classification using Hybridization of HMM and SVM Classifier.," *International Journal of Security & Its Applications*, vol. 9, pp. 125-140, 2015
- [19] S. Agarwal and S. Chand, "Image Forgery Detection using Multi Scale Entropy Filter and Local Phase Quantization," pp. 752- 759, 2015
- [20] Zenan Shi, Xuanjing Shen, Haipeng Chen, Xiang Li, "Blind Detection of Image Splicing Based on Fuzzy Run-Length", *International Conference on Computer and Information Technology; Ubiquitous Computing and Communications Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, pp. 915-920, 2015