Forgery Detection Using Statistical Features

Saba Mushtaq, Ajaz Hussain Mir
Department Of Electronics and Communication Engineering
National Institute Of Technology, Srinagar India-190006
sab.mushtaq@gmail.com , ahmir@rediffmail.com

***Abstract*— Digital images are present everywhere on magazine covers, in newspapers, in courtrooms as evidences, and all over the Internet signifying one of the major ways for communication nowadays. Easy availability of image editing tools has made it very simple to tamper the digital images thus putting the authenticity of these images under suspicion. There are a number of type of forgeries that can be carried out on digital images most common being the copy-move and splicing forgeries. This paper proposes a new method for image copy-move and splicing detection based on statistical features of the digital image. Copy- move involves copying of a region in an image and pasting it somewhere in the same image to hide any important detail and Splicing involves merging of two or more images to form a composite image that is significantly different from the original image. The proposed approach calculates grey level run length matrix (GLRLM) texture features for the forged images and original images. Support vector machine is used for classification. Results show that the proposed algorithm is very effective in detection of forgery.**

Keywords*— digital image forgery, copy-move, splicing, image texture, SVM.

I. INTRODUCTION

From time to time images have been generally accepted as evidence of events of the depicted happenings. Because of dominance of computer in field of education, business and other field, acceptance of digital image as authorized document has become frequent .The ease of use and accessibility of software tools[1] and low-cost hardware, makes it very simple to forge digital images leaving almost no trace of being subjected to any tampering . As such we cannot take the authenticity and integrity of digital images for granted [2].

Digital forensics field has developed significantly to combat the problem of image forgeries in many domains like legal services, medical images, forensics, intelligence and sports [3, 4]. Forgery detection intends to verify the authenticity of images [5]. For authentication of images several methods have been developed. Broadly they can be classified as Active authentication and Passive authentication. The classification is based on the fact whether the original image is available or not.

Active authentication is concerned with data hiding where some code is embedded into the image at the time of generation. Verifying this code authenticates the originality of image. Active authentication methods are further classified into two types digital watermarking and digital signatures [6, 7, 8]. Digital water marks are embedded into the images at the time of image acquisition and digital signatures embed some secondary information, usually extracted from image, at the acquisition end into the image. The main drawback of these approaches remains that they are to be inserted into the images at the time of recording using special equipments.

Passive authentication also called image forensics is the process of authenticating images with no requirement of prior information just the image itself [9, 10]. Passive techniques are based on the assumption that even though tampering may not leave any visual trace but they are likely to alter the underlying statistics. It is these inconsistencies that are used to detect the tampering. Exhaustive research survey has been carried out in this field of passive image forensics [11, 12]. Passive techniques have the advantage that they do not require prior information about the image, they just need the tampered image that requires to be verified for authenticity. In this paper we focus on copy-move and e image splicing passive techniques. The remainder of paper is organized as section II contains related work .Section III presents introduction to the proposed method, section IV Algorithm and implementation, section V results and comparison and finally conclusion.

II. RELATED WORK

Image splicing forgery technique involves composition or merging of two or more images changing the original image significantly to produce a forged image. In case images with differing background are merged then it becomes very difficult to make the borders and boundaries indiscernible. Figure 1 below shows an example of image splicing.

Fig 1 : Spliced image(two images merged to form a single image)

The presence of abrupt changes between different regions that are combined and their backgrounds, provide valuable traces to detect splicing in the image under consideration. Ng and Chang [13] suggested an image-splicing detection method based on the use of bi-coherence magnitude features and phase features. Detection accuracy of 70% was obtained.

Ng and Tsui [14] and Ng T.T. [15] developed a method that uses linear geometric invariants from the single image and thus extracted the CRF signature features from surfaces linear in image irradiance. In [15] authors developed an edge-profile based method for extraction of CRF signature from a single image. In the proposed method the reliable extraction depends on the fact that edges should be straight and wide.

Wang et al. [16] developed a splicing detection method for color images based on gray level co-occurrence matrix (GLCM). GLCM of the threshold edge image of image chroma is used. Zhao et al. [17] developed a method based on chroma space. Gray level run length texture feature is used. Four gray level run-length run-number (RLRN) vectors along different directions obtained from de-correlated chroma channels were used as unique features for detection of image splicing and for classification SVM was employed as classifier..

Method based on run length is proposed in [18] to detect splicing. Edge gradient matrix of an image is computed, and approximate run length is calculated along the edge gradient direction. Some features are constructed from the histogram of the approximate run length. To further improve the detection accuracy, the approximate run length is applied on the error image and the reconstructed images based on DWT to obtain more features. SVM is employed to classify the authentic and spliced images.

Subtle inconsistencies in the color of the illumination of images are exploited in [19]. The technique is applicable to images containing two or more people and requires no expert interaction for the tampering decision. Texture and edge based features are extracted from illuminant estimators which are then provided to a machine-learning approach for automatic decision-making. SVM is used for classification and detection rates of 86% on a dataset consisting of 200 images and 83% on 50 images collected from the Internet was achieved.

Another detection scheme based on blur as a clue is proposed in [20]. This method expose the presence of splicing by evaluating inconsistencies in motion blur even under space-variant blurring situations.

The methods discussed above have a few limitations such as the detection methods fail when measures such as blur are used to conceal the sharp edges disturbances after splicing. The requirement of edges to be wide for reliable extraction is also a limitation. Moreover minor and localized tampering may go undetected.

Copy-move is another popular and common photo tampering technique because of the ease with which it can be carried out [21]. It involves copying of some region in an image and moving the same to some other region in the same image. Since the copied region belong to the same image therefore the dynamic range and color remains compatible with the rest of the image[22]. An example of copy-move forgery is shown in figure2:

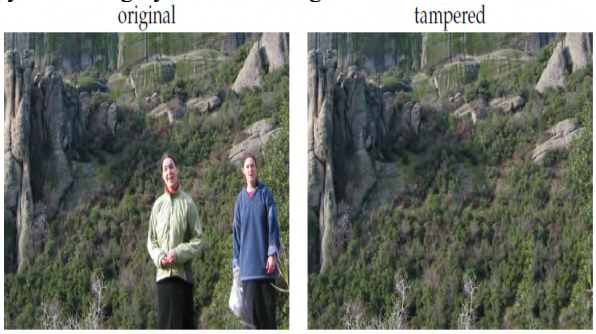

Fig 2: Copy- move forgery

The original image is forged to obtain the tampered image the two persons have been masked by copying a region from the same image and pasting it over the two people.

Among the initial attempts Fredrich[23] proposed methods to detect copy-move forgery. Discrete cosine transform (DCT) of the overlapping blocks are used and their lexicographical representation is taken to avoid the computational burden. Block matching algorithm was employed for best balance between performance and complexity.

Huang et al. [24] worked on enhancing the work done by Fridrich et al. [23] in terms of the processing speed. The algorithm is straightforward, simple, and has the capability of detecting duplicated regions with very good sensitivity and accuracy in spite of the post-processing operations. However there is no mention of robustness of the algorithm against geometric transformations.

Popescu and Farid [25] suggested a method using principal component analysis (PCA) for the overlapping square blocks. The computational cost and the number of computations required are considerably reduced $O(N_tN \log N)$, where N_t is the dimensionality of the truncated PCA representation and N the number of image pixels. However accuracy reduces for small block sizes and low JPEG qualities.

To combat computational complexity Langille and Gong[26] proposed use of k-dimensional tree which uses a method which searches for blocks with similar intensity patterns using matching techniques. The resulting algorithm has a complexity of O(NbNs).

Sutthiwan et al. [27] presented a method for passive-blind color image forgery detection which is a combination of image features extracted from image luminance by applying a rake – transform and from image chroma by using edge statistics. The technique results in almost 99% of accuracy.

Xunyu and Siwei [28] presented a technique that uses region duplication by means of estimating the transform between

matched SIFT key points that is invariant to distortions that occurs due to image feature matching. The algorithm results in average detection accuracy of 99.08% but the method has one limitation duplication in smaller region is hard to detect as key points available are very few.

Kakar and Sudha [29] developed a new technique based on transform-invariant features which detecting copy-paste forgeries but requires some post processing based on the MPEG-7 image signature tools. Feature matching that uses the inherent constraints in matched feature pairs so as to improve the detection of cloned regions is used which results in a feature matching accuracy of more than 90%.

All methods discussed above that are able to detect and localize copy move forgery and cloned regions in an image are expensive, computationally complex and require human interpretation of the results. Also some techniques more often fails to detect the forgery if size of the tampered area is relatively small compared to image dimensions.

III. PROPOSED METHOD

Forgery changes the underlying statistics of image which may be invisible to human vision. Our model uses the texture of image. In an image a region has constant texture if a set of local statistics or other local properties of picture function are constant, slowly varying or approximately periodic [33]. This concept is used to check if an image has been tampered.

The motivation to use run length texture features is due to the enormous application it has found in medical imaging [34, 35], steganalysis [36] and forgery detection [16,37,38] . Although texture has been used but we have tried to explore run length matrix features which have not been explored yet. The concept of run length was proposed by Gallow [39]. GLRLM is a pattern of grey level pixels in a particular direction from reference pixel. It is a way of searching the image across a particular direction for runs of collinear pixels having same gray level values. A run is adjacent pixel having same gray level values. GLRLM is characterized by intensity of run, length of run and direction of run from a reference pixel. It is based on computing the grey level of various lengths.

The Gray Level Run Length matrix is constructed as follows

$$GLRLM(\theta) = (p (i,j) \mid \theta)$$

p (i, j) is the number of times there is a run of length j having gray level i in direction θ where total intensity levels in image is n. There are four Run Length Matrix that can be computed for 4 directions of run (0°, 45°, 90°, 135°). The Figure 3 shows the sub image with 4 gray levels for constructing the GLRLM.

1	2	3	4
1	3	4	4
3	2	2	2
4	1	4	1

Fig. 3 : Matrix of image

Figure 4 shows that the GLRLM in the direction of 0^0 of the sub image. In addition to 0^0 directions GLRLM can be calculated in all four directions.

Gray Levels	Run Length(j)			
	1	2	3	4
1	4	0	0	0
2	1	0	1	0
3	3	0	0	0
4	3	1	0	0

Fig. 4. GLRLM Of Image

For each matrix in a particular direction following seven GLRLM features viz SRE, LRE, GLN, RLN, RP, LGLRE, HGLRE are obtained. These features were suggested by Gallow[36] and defined as follows in table I.

TABLE I. Gray level run length matrix features

S.NO.	Features	Formulae
1	Short Run Emphasis(SRE)	$\frac{1}{n}\sum_{(i,j)}\frac{P(i,j)}{j^2}$
2	Long Run Emphasis(LRE)	$\frac{1}{n}\sum_{(i,j)} j^2\, p(i,j)$
3	Grey Level Non-uniformity(GLN)	$\frac{1}{n}\sum_{i}\left(\sum_{j} p(i,j)\right)^2$
4	Run Length Non-Uniformity	$\frac{1}{n}\sum_{j}\left(\sum_{i} p(i,j)\right)^2$
5	Run Percentage(RP)	$\sum_{i,j}\frac{n}{p(i,j)\,j}$
6	Low Grey level Run Emphasis(LGLRE)	$\frac{1}{n}\sum_{i,j}\frac{p(i,j)}{i^2}$
7	High Grey Level Run Emphasis(HGLRE)	$\frac{1}{n}\sum_{i,j} i^2\, p(i,j)$

IV. IMPLEMENTATION

This section presents implementation of the proposed method

A. Database

We have used two databases one is the CASIA TIDE v1.0[40] database. This dataset contains 800 authentic and 925 spliced color images of size 384x256 pixels with JPEG format. This database is used for detection of forged images where splicing is carried out. The other database is CoMoFoD database[41]. It contains 260 image sets, 200 images in small image category (512x512), and 60 images in large image category (3000x2000). It is used for copy-

move forgery. We have used only 200 images in small image category.

B. Classifier

SVM is used as classifier. SVM is commonly used for machine learning. RBF kernel function being the reasonable first choice is used. All experiments are based on same database and classifier. SVM being a two class recognition system is suitable for forgery detection as it has to classify a test image into either authentic class or forged class. Experimentation is carried out using SVMlight.

C. Algorithm

The proposed method is carried out in two steps one involves the training of the SVM classifier The block diagram is shown below.

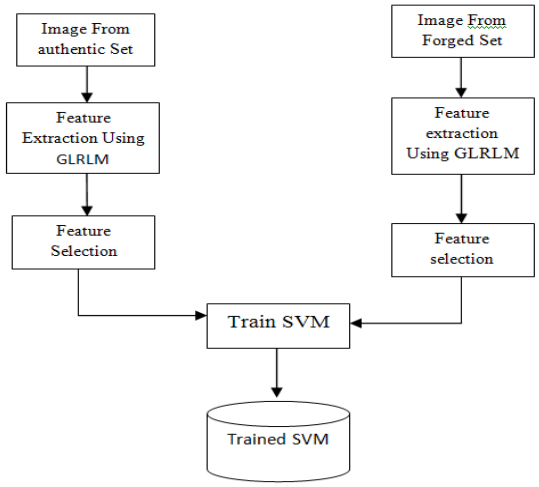

Figure 5 : Block diagram for training the SVM Classifier.

Second is the testing step. Here a test image is given as input to the classifier which based on its knowledge classifies it as original or forged as shown below.

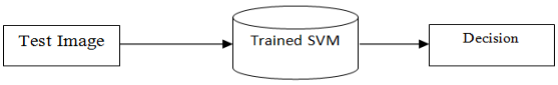

Figure 6 : Verifying the authenticity of image.

The algorithm can be summed up as follows

1. For the training phase images are chosen from authentic set and the forged set.
2. For each image GLRLM is calculated in three directions (0^0, 45^0 and 90^0). For each calculate gray level matrix 7 GLRLM features (given in Table I) are calculated. The features vector for each image is set of 7x3 features . Feature vector for authentic set and forged set is formed.
3. Features vectors thus obtained are used to train SVM classifier.
4. The trained SVM classifier trained for two class problem is used to verify a given test image for authenticity. Test images are chosen randomly from the database.
5. Results for the two databases are calculated as given in next section.

V. RESULTS AND DISCUSSION

To evaluate performance of proposed scheme, training samples are randomly selected from whole image data set. Using the SVM classifier we assigned the training images with random inputs 1 and -1 to fake and original images. We have calculated true positive (TP) which refers that a forged image is detected as fake and true negative (TN) which refers to that the authentic image is detected as original as shown in confusion matrix given below in table II . The average of the two gives the accuracy of the model.

TABLE II Confusion Matrix

Actual	Predicted Spliced	Predicted Authentic
Spliced	TP	FN
Authentic	FP	TN

For the two data bases the results obtained are shown in table III and table IV.

TABLE III. Classification accuracy using SVM on CASIA database.

Database	Training images	Testing images	TP	TN	Accuracy
Authentic	250	125	-	82.45%	**80.71%**
Spliced	250	125	78.98%	-	

TABLE IV. Classification accuracy using SVM on CoMoFoD database

Database	Training images	Testing images	TP	TN	Accuracy
Authentic	150	50	-	82.0%	**82.5%**
Spliced	100	40	83.0%	-	

The ROC Curve between true positive and false positive is shown in figure 7 below. False positive refer to the authentic image which are wrongly classified as forged. The two curves are for the two databases with the upper curve for database CoMoFoD and lower one for CASIA database. It can be concluded from the experimental results and ROC curve that the proposed model gives a good performance.

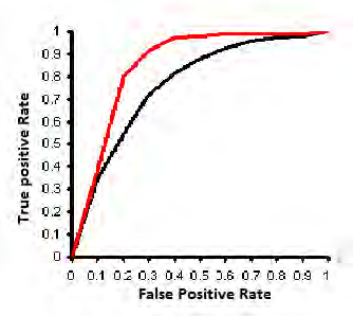

Fig 7 ROC curve for the two databases

It was found that with CASIA dataset the accuracy of 80.71 % was obtained and with CoMoFoD accuracy of 82.5% was obtained. A comparision of the proposed techniques with the start of art techniques is given below.

TABLE V : Comparison of start of art copy-move forgery techniques

Method	Extracted Feature	Classifier	Detection Accuracy
Proposed Algorithm	GLRLM (0.45,90)	SVM	**82.5%**
Popescu & Farid [25]	PCA of overlapping block	Lexographical sorting	50% for small block size 100% for 16x16 block size
Lin et al. [30]	Average intensity of image blocks.	Radix sort followed by shift vector calculation	98%
Sutthiwan et al.[27]	Image luminance using RAKE model & image chroma using edge statistics	SVM	99%
Xunyu & Siwei [28]	Matched SIFT Keypoints	K-mean Clustring	99.08%
Muhammad et al. [32]	Dyadic wavelet transform	Thresholding Classification	98.34%
Zhao & Guo[31]	DCT & SVD	Lexographical sorting of blocks and frequency thresholding.	96.1 %

TABLE VI: Comparison of start of art splicing detection methods

Method	Extracted Feature	Classifier	Detection Accuracy
Proposed algorithm	GLRLM (0.45,90)	SVM	80.7%
Ng et al.[13]	Higher order bi-coherence features	SVM	70%
Fu et al. [42]	Hilbert-Huang Transform & wavelet decomposition based features.	SVM	80.15%
Chen et al. [43]	Moments of wavelet characteristics & 2D phase congruency.	SVM	82.32%
Zhang et al. [44]	moment features from multi size block features(MBDCT) & Image quality Metrics	SVM	87.10%
Zhen Hua et al. [45]	Edge sharpness measure and visual saliency	SVM	96.33%
Fang et al. [46]	sharpness in color edges	LDA	90%
Zhao et al.[17]	Grey level run length number vectors	SVM	94.7%

From the above given table of comparison we conclude that the proposed method offers a good performance on the basis of detection accuracy. In this paper we have used texture features of the image to detect forgeries. Even though the forgery may be invisible to human eye but the changes caused to the underlying statistics as a result of combining two different images provide an evidence to detect tampering. As there are no accepted benchmarks for tampering detection, results of our method are illustrated by examples as usual available in the literature.

VI. CONCLUSION

Image forensics is the latest and hot field of research because of the dominance of the digital images in court rooms, on magazine covers, in scientific journals and almost everywhere. It has becomes important to establish their authenticity because of the ease with which they can be tampered using various easily available image tampering software and tools. Among various image forgery techniques splicing and copy-move are the most common forgery types which are very easy to carry. In this paper we have proposed a digital image forgery detection technique based on statistical texture features. The experimental result prove that the proposed GLRLM features taken for various images using CASIA DATABASE and CoMoFoD database and using SVM classifier have demonstrated the effectiveness of the algorithm and is applicable to images of unknown origin. In our future work we will attempt to apply other texture properties for the problem of splicing, copy-move and other forgery types.

REFERENCES

[1] Guangjie Liu, Junwen Wang, Shiguo Lian and Zhiquan Wang, A passive image authentication scheme for detecting region-duplication forgery with rotation, Journal of Network and Computer Applications, Volume 34, Issue 5, September 2011, Pages 1557-1565.

[2] Sebe Nicu, Liu.Yuncai,Zhuang, Yueting, Huang, ThomasS., Blind Passive Media Forensics: Motivation and Opportunity, Multimedia Content Analysis and Mining, vol. 4577, Springer, Berlin/Heidelberg, 2007, pp. 57–59.

[3] Mahdian, Babak; Saic, Stanislav, "Blind methods for detecting image fakery," Security Technology, 2008. ICCST 2008. 42nd Annual IEEE International Carnahan Conference on , vol., no., pp.280,286, 13-16 Oct. 2008.

[4] Shivakumar, B.L., Baboo, S.S.: 'Detecting copy-move forgery in digital images: a survey and analysis of current methods', Global J. Comput. Sci. Technol., 2010, 10, pp. 61–65.

[5] Gajanan K. Birajdar, Vijay H. Mankar, Digital image forgery detection using passive techniques: A survey, Digital Investigation, Volume 10, Issue 3, October 2013, Pages 226-245.

[6] S.Katzenbeisser and F.A.P. Petitcols, Information Techniques For Stenography And Digital Watermarking. Norwood,MA : Artec House, 2000.

[7] I.J.Cox, M.L.Miller and J.A.Bloom, Digital watermarking San Fransisco, CA: Morgan Kaufmann, 2002.

[8] Zhen Zhang; Yuan Ren; Xi-Jian Ping; Zhi-Yong He; Shan-Zhong Zhang, "A survey on passive-blind image forgery by doctor method detection," Machine Learning and Cybernetics, 2008 International Conference on , vol.6, no., pp.3463,3467, 12-15 July 2008.

[9] Zhou, Z., Zhang, X.: 'Image splicing detection based on image quality and analysis of variance'. 2010 Second Int. Conf. on Education Technology and Computer (ICETC), 2001, vol. 4, pp. V4-242–V4-246

[10] Ng T-T, Chang S-F, Lin C-Y, Sun Q. Passive-blind image forensics. In: Multimedia security technologies for digital rights. USA: Elsevier; 2006.

[11] Luo Weiqi, Qu Zhenhua, Pan Feng, Huang Jiwu , A survey of passive technology for digital image forensics, Front Comput Sci China (2007) pp 166–79.

[12] Tian Tsong Ng, Shih-Fu Chang , A model for image splicing., Proceedings of IEEE International conference on image processing (ICIP) 2004 pp. 1169–1172.

[13] Tian Tsong Ng, Mao-Pei Tsui, Camera response function signature for digital forensics - part I: theory and data selection.Proceedings of workshop on information forensics and security 2009 pp.156–160..

[14] Tian Tsong Ng ,Camera response function signature for digital forensics – part II: signature extraction., proceedings of workshop on information forensics and security 2009. pp. 161–165.

[15] 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.

[16] 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.

[17] Zhongwei He , Wei Sun , Wei Lu ,Hongtao Lu c , Digital image splicing detection based on approximate run length, Pattern Recognition Letters 32 (2011) pp 1591–1597.

[18] 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.

[19] Rao, Rajagopalan, Seetharaman , Harnessing Motion Blur to Unveil Splicing , IEEE Transactions on Information Forensics and Security 9(4) (2014) pp. 583-595.

[20] E. Ardizzone, A. Bruno, G. Mazzola, Copy-move forgery detection via texture description, in: MiFor'10 – Proceedings of the 2010 ACM Workshop on Multimedia in Forensics, Security and Intelligence, Co-located with ACM Multimedia 2010, 2010, pp. 59–64.

[21] S. Bravo-Solorio, A.K. Nandi, Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics, Signal Proc. 91 (8) (2011) 1759–1770.

[22] Fridrich J, Soukal D, Lukas J. Detection of copy-move forgery in digital images. In: Proc. of digital forensic research workshop 2003. p. 55–61.

[23] Y. Huang, W. Lu, W. Sun, D. Long, Improved DCT-based detection of copy-move forgery in images, Forensic Sci. Int. 3 (2011) 178–184.

[24] Popescu A, Farid H. Exposing digital forgeries by detecting duplicated image regions. Technical Report TR2004-515. Department of Computer Science, Dartmouth College; 2004

[25] Langille A, Gong M. An efficient match-based duplication detection algorithm. In: Proc. of the 3rd Canadian conference on computer and robot vision 2006. p. 64.

[26] Sutthiwan P, Shi YQ, Wei S, Tian-Tsong N. Rake transform and edge statistics for image forgery detection. In: Proc. IEEE International conference on multimedia and Expo (ICME) 2010. p. 1463–8.

[27] Xunyu P, Siwei L. Region duplication detection using image feature matching. IEEE Trans Inf Forensics Security 2011;5(4):857–67.

[28] Kakar P, Sudha N. Exposing postprocessed copy-paste forgeries through transform-invariant features. IEEE Trans Inf Forensics Security 2012; 7(3):1018–28.

[29] Lin, H., Wang, C., Kao, Y (2009) Fast copy-move forgery detection in WSEAS Transactions on Signal processing, 5(5), p 188-97

[30] Zhao Jie , Jichang Guo(2013). Passive forensics for copy-move image forgery using a method based on DCT and SVD in Forensic Science International 233 : 158–66

[31] Muhammad Ghulam, Muhammad Hussain , George Bebis (2012) . Passive copy move image forgery detection using undecimated dyadic wavelet transform, Digital Investigation 9 : 49–57.

[32] Sklansky, J., "Image Segmentation and Feature Extraction," Systems, Man and Cybernetics, IEEE Transactions on , vol.8, no.4, pp.237,247, April 1978.

[33] Mir AH.; Hanmandlu, M.; Tandon, S.N., "Texture analysis of CT images," Engineering in Medicine and Biology Magazine, IEEE , vol.14, no.6, pp.781,786, Nov/Dec 1995.

[34] S. G. Mougiakakou , I. K. Valavanis ,A. N. , K. S. Nikita, Differential diagnosis of CT focal liver lesions using texture features, feature selection and ensemble driven classifiers, Artificial Intelligence in Medicine (2007) 41, pp. 25—37

[35] Shi, Y.Q., Chen, C., Xuan, G.: Steganalysis versus splicing detection. In Int. Workshop on Digital Watermarking (IWDW07). (December 2007).

[36] J. Dong, W. Wang, T. Tan and Y. Q. Shi, Run-length and edge statistics based approach for image splicing detection, Lecture Notes in Comp. Sci. Vol. 5450, 2009, pp 76-87.

[37] Gharibi, F. ,RavanJamjah, J. ; Akhlaghian, F. ; Azami, B.Z. ; Alirezaie, J., Robust detection of copy-move forgery using texture features, 19th Iranian Conf. Electrical Engg. (ICEE), 2011 pp. 1-4

[38] M. M. Galloway,"Texture analysis using gray level run lengths", Computer Graphics Image Process., Vol. 4, pp. 172–179, June 1975.

[39] Credits for the use of the CASIA Image Tempering Detection Evaluation Database (CAISA TIDE) V1.0 are given to the National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Science, Corel Image Database and the photographers. http://forensics.idealtest.org".

[40] Tralic D., Zupancic I., Grgic S., Grgic M., "CoMoFoD - New Database for Copy-Move Forgery Detection", in Proc. 55th International Symposium ELMAR-2013, pp. 49-54, September 2013

[41] Fu Dongdong, Shi YunQ, Su Wei, Detection of image splicing based on Hilbert- Huang transform and moments of characteristic functions with wavelet decomposition, In: Proc. of Int. workshop on digital watermarking , 177–187.

[42] Chen,Wen Shi ,Yun Quing Su Wei., Image splicing detection using 2-d phase congruency and statistical moments of characteristic function, SPIE conference on security, steganography, and watermarking of multimedia contents.

[43] Zhen Zhang; Jiquan Kang; Yuan Ren, "An Effective Algorithm of Image SplicingDetection," International Conference on Computer Science and Software Engineering, 2008, pp.1035-1039

[44] Qu Zhenhua,Qiu Guoping, Huang Jiwu, Detect digital image splicing with visual cues, Proceedings of international workshop on information hiding, pp. 247–261.

[45] Zhen Fang; Shuozhong Wang; Xinpeng Zhang, "Image Splicing Detection Using Camera Characteristic Inconsistency," Multimedia Information Networking and Security, 2009. MINES '09. International Conference on , vol.1, no., pp.20,24, 18-20 Nov. 2009.