Tampered Region Detection on Digital Images by Efficient SVM Classifier

[1] Sreeletha S.H, [2]Geethu N Nadh,[3] Prof. (Dr.) M. Abdul Rahman
[1] Associate professor, [2] M.Tech Scholar, [3] Pro Vice Chancellor
[1]Department of Computer Science and Engineering,
[1]LBSITW, Poojappura, Trivandrum, Kerala, India

***Abstract*—Digital images have been used in a wide variety of applications such as military, law enforcement, reconnaissance, medical diagnosis and media. With the rapid development of image editing tools, it is easy to produce believable manipulated images. A malicious user may perform contrast enhancement as a retouching manipulation. Also contrast enhancement is used for creating composite image. So it is necessary to detect contrast enhancement manipulation in order to verify the originality and authenticity of the digital images. This contrast enhancement may be applied globally and locally on images. In the proposed system SVM (Support Vector Machine) classifier is used for image tampering region detection. SVM classifiers are used to classify the images as genuine or forged. First, develope a framework for the design of composite image forgery. This framework operates by identifying peak position similarities and gap position similarities from an images gray-scale histogram, then adding a SVM classifier to classify the image original or not. Two algorithms are proposed to detect the contrast enhancement involved manipulations are proposed. First, we focus on the detection of global contrast enhancement applied to the previously JPEG-compressed images, which are widespread in real applications. The histogram peak/gap artifacts are distinguished by identifying the zero-height gap fingerprints. Second, we propose to identify the composite image created by enforcing contrast adjustment on either one or both source regions. The positions of detected blockwise peak/gap bins are clustered for recognizing the contrast enhancement mappings applied to different source regions. The consistency between regional artifacts is checked for discovering the image forgeries and locating the composition boundary. We use this technique to identify image forgery more accurately than the previous methods.**

***Index Terms*— Image forgery, Contrast enhancement, Histogram, Composite image, SVM.**

I. INTRODUCTION

Digital images have been used in number of applications from law enforcement and military field to medical field and consumer photography. News media organizations routinely integrate digital images into their reporting. Governmental, judicial and military institutions rely on digital images to make critical policy and legal decisions. Digital images are considered as proofs against various crimes or evidences for various purposes. In the field of medicine, reports of patients are highly confidential and supposed to be authentic. They are proof for unhelthiness and claim of disease. With the wide spread availability of low-cost image editing softwares, it is easy to manipulate the digital images. So the integrity of image content can no longer be taken for granted. Image forgeries are widespread on the internet. To circumvent such a problem, digital forensic techniques have been proposed to blindly verify the integrity and authenticity of digital images. There are different types of image alterations, which can be broadly divided into two categories: 1) non-content-changing operations including resampling, compression, sharpening ltering, contrast enhancement and median ltering; 2) content- changing operations, i.e., splicing and composition.

When an attacker manipulates an image, contrast enhancement is used for avoiding traces left by the image forgery. Contrast is one of the factors of low or good quality images. An image can't be said good quality when it has very low contrast or too high contrast. Most of the contrast enhancement operations are pixel-value mapping operation which introduces some statistical traces that can be used to expose the cut-and-paste type image forgery. The prior contrast enhancement forensic algorithms work well under the assumption that the gray level histogram of an unaltered image exhibits a smooth contour. The histogram of an image is a plot of the gray levels values versus the number of pixels at that value. Contrast enhancement increases the local contrast in smaller regions while it preserves the global contrast. Global contrast enhancement techniques enhance the overall contrast of the image. Their dependencies on the global content of the image limit their ability to enhance local details. Users may also perform local contrast enhancement for creating a realistic composite image. Some of the contrast enhancement techniques are Contrast Stretching, Histogram equalization etc. Histogram equalization is widely used for contrast enhancement in a variety of applications. It works by flattening the histogram and stretching the dynamic range of the gray levels. The flat histogram will determine the contrast of the image. It increases the global contrast of image. Intensities can be better distributed on the histogram.

A malicious user may perform contrast enhancement as a retouching manipulation. In copy-move forgery, one region is copied from an image and pasted onto other region of same image. Another copy-move forgery through composition is copying and pasting areas from one or more images and pasting onto an image being forged. Copy-move forgery manipulates both, image statistics and image content as well. .So it is necessary to detect contrast enhancement manipulation in order to verify the originality and authenticity of the digital images. When an image is subjected to typical forgery, contrast is used by the attacker to avoid leaving visual clues after forging an image. Contrast enhancements improve the perceptibility of objects in the scene by enhancing the brightness difference between objects and their backgrounds. The contrast enhancement operations can be viewed as nonlinear pixel mappings which introduce artifacts into an images histogram. These mapping maps multiple unique input pixel

values to same output value, result in the addition of sudden peak values to an image histogram. The complex nature of most natural and man-made lighting environments rarely results in a real world scene consist of several distinct colors with no shading. Instead, a continuum of color values and illumination levels exist in real world scene. If the observational noise present in the image capture process is large, some pixels will incorrectly be observed as a slightly larger or lower pixel values than the correct. Detecting the traces left by contrast enhancement can be effective way of exposing cut-and-paste image forgery. Contrast enhancement will introduce sudden peaks and zeros in the histogram and therefore increases high frequency components in the histogram spectrum.

In order to detect the tampering region more accurately, Support Vector Machine (SVM) classifier is used. SVM is a super learning algorithm based on the concept of decision planes that define decision boundary. Machine learning concerned with the development of techniques and methods which enable the computer to learn and perform tasks and activities. A decision plane separates a set of objects into two classes. It is considered a good candidate for image classification because of its high generalization performance without the need to add a priori knowledge, even when the dimension of the input space is very high. All images lies on one side of hyperplane are belongs to class +1 and others to class-1. Using SVM training is relatively easy. It scales relatively well to high dimensional data. SVM classification technique is used for training and testing the input images. For classification, first extract the features from the test images blocks and these features are used to pass in an SVM to construct a training model, which will further classify the test images blocks given by the user. We can run that trained model on unknown test images to determine which classes each belongs. Training is the iterative process to build best classifier possible. It is the process of taking content that is known to belong to specified classes and creating a classifier on the basis of known content. The respective class of the content is already known. Testing is the process of running the classifier on unknown content to determine the class membership for the unknown content. It is the one-time process designed to run on unknown content. A main advantage of SVM classification is that SVM performs well on datasets that have many attributes, even when there are only a few cases that are available for the training process. Good separation is achieved by the hyper plane that has the largest distance to the nearest training data point of any class (functional margin), generally larger the margin lower the generalization error of the classifier.

.

II. RELATED WORK

A. Swaminathan, M. Wu, and K. J. R. Liu [2] proposed a method for the forensic analysis of digital camera images. The various traces that are left behind in a digital image when it goes through various processes are called intrinsic fingerprints. These fingerprints are used to identify the source and are used to establish the authenticity of the image. There are in-camera and postcamera fingerprints. The absence of in-camera fingerprints suggests that the test image is not a camera output and it is generated by other image production processes. The presence of new postcamera fingerprints suggests that the image has undergone some kind of postcamera processing. This work describes the image acquisition model in digital cameras. This paper also describes method to estimate the camera component parameters and also describe method to estimate the postcamera fingerprints of manipulated camera outputs. Any further postcamera processing is considered as a manipulation filter. Although this method can detect manipulation, this method fails to determine which specific type of manipulation was enforced.

M. C. Stamm and K. J. R. Liu [3] again proposed the method for detecting general forms globally and locally applied contrast enhancement. They also proposed a method for identifying the use of histogram equalization by searching for the identifying features of each operation's intrinsic fingerprint. The pixel value mappings leave behind statistical artifacts are visible in an image's histogram. By observing the common properties of the histogram of unaltered images, the model of an unaltered image's histogram is proposed. None of the original image's histograms contain sudden zeros or impulsive peak. We can identify the features of a pixel value mapping's intrinsic fingerprint using this model. Locally applied contrast enhancement operation detection can be used to identify cut-and-paste forgery. By measuring the strength of the high frequency components of an image's pixel value histogram, contrast enhancement operation can be detected. A composite image can be created by replacing a contiguous set of pixels in one image with a set of pixels corresponding to an object from a separate image. A manipulator may need to perform contrast enhancement on one of the source image so that the lighting conditions match across the composite image. The test image is segmented into blocks. Each block is tested for evidence of locally applied contrast enhancement. Here only pasted region has undergone contrast enhancement.

A method to reconstruct the gamma mapping via the recognition of the peak-gap fingerprints in the histograms is proposed in [5]. Gamma correction is a contrast enhancement operation. The peak-gap fingerprint patterns and the methodology of pattern matching are employed to achieve fast gamma estimation. The peak-gap characteristic which is unique to gamma mapping should be identified firstly. The peak-gap pattern for different gamma mappings can be precomputed. The amount of gamma correction is estimated by matching the peak-gap feature pattern extracted from test images to those precomputed ones.

M. C. Stamm and K. J. R.Liu [6] proposed a method for detecting image manipulation. The intrinsic fingerprints are the evidence of image manipulation and it can be used to determine which operations were used to modify an image. An iterative algorithm to estimate any contrast enhancement mapping used to alter the image is proposed here. Once the image modifications have been detected, the next task is to recover as much information as possible about the unaltered version of image and also the operation used to modify it. A probabilistic model is used to estimate contrast enhancement mapping used to modify the images as well as the histogram of the unaltered version of the image. This model identifies the histogram entries corresponding to enhancement artifacts. The pixel value histograms of the image are interpolatably connected. Once an image has been identified as contrast enhanced, an estimate of the contrast enhancement mapping used to modify the image as well as an estimate of the unaltered image's pixel value histogram can be jointly obtained through an iterative process. This iterative algorithm is capable of providing accurate estimates even when nonstandard forms of contrast enhancement are applied to an image.

M. C. Stamm and K. J. R. Liu [7] proposed a forensic method of exposing cut-and-paste image forgery through detecting contrast enhancement. This work is about the inter-channel correlation introduced by color image interpolation. It shows how a linear or nonlinear contrast enhancement can disturb this natural inter-channel dependency. In order to measure the correlation, a metric is constructed here. Using this metric we can distinguish the original and contrast enhanced images. In a composite image, the contrast between the background and the pasted region is not consistent with that of original image. Contrast enhancement operations introduce some statistical traces. So this method exposes cut-and-paste forgery by detecting contrast enhancement. A general contrast enhancement detection algorithm based on the observations in the histogram of the images is proposed. But there are some parameters need to be determined by users. It is not convenient in practice, as the parameters may vary with different forms of contrast enhancements. If the attacker removes the peak and gap artifacts in the histogram, this histogram based methods will fail to find out the contrast enhancement operations. This paper describes how the contrast enhancement can be disturb the inter-channel similarities of high frequency components of an image and what will happen to its high frequency components if it is enhanced.

A method is developed for detecting image forgery including removal, insertion, and replacement of objects [9]. Image, texture and pixel value based features are extracted and analyzed from the images. Then hash values are calculated for these features. An image can become a forgery based on the context in which it is used. The manipulation techniques include deletion of details, insertion of details, combining multiple images and false captioning. In the proposed method, SVM classifier is employed for forgery detection after calculating the hash values for extracted features. RSA key is set in training phase and the user is asked to enter the same key in testing phase to ensure that the user is an authorized person. The process consisting of two phases which are training phase and testing phase. A database is created and trained in the training phase with a number of images. The RSA key is set after training images in the database. When any user tries to run the application for checking the authenticity of query image, he has to enter the same key which was set during the training phase. Thus making sure that only authorized person can run the application. The images are converted into gray scale from rgb. Median filter is applied to remove noises present in the images. Image enhancement techniques are applied. It includes gray level contrast manipulation etc. The mean and standard deviation are calculated. Texture analysis can be used to find the texture boundaries. The hash values are calculated for the extracted features. SVM finds the vectors that define the separators giving the widest separation of classes. In this method accuracy of detecting forgery is enhanced by using SVM classifier.

III. PROPOSED WORK

Aim of this work is to develop a frame work for the detection of contrast enhancement operation on digital images. Contrast enhancement operation can be applied globally or locally. So it is necessary to detect contrast enhancement operation globally and locally.

Global Contrast Enhancement Detection

The previous algorithms work well under the assumptions that the grey level histogram of unaltered image shows smoothness while that of contrast enhanced images shows peak/gap artifacts. The gap bins with zero height always appear in enhanced images. We focus on the detection of isolated zero-height gap bins but not connected bins, which are rarely present in the middle of histograms. The zero- height gap bins are absent in compressed images since there is lack of a distinct pixel value mapping applied to all pixels. Therefore, the zero height gap features can be used to detect global contrast enhancement in both uncompressed and compressed images. The global contrast enhancement detection algorithm [8] counts the number of zero height gap bins in the histogram of the input image. Then it is compared with the decision threshold. Based on that contrast enhancement is detected. Figure.1 shows the definition of a zero-height gap bin at k. Figure.2 shows the original input and its grey scale histogram. Figure.3 shows contrast enhanced image and its grey scale histogram.

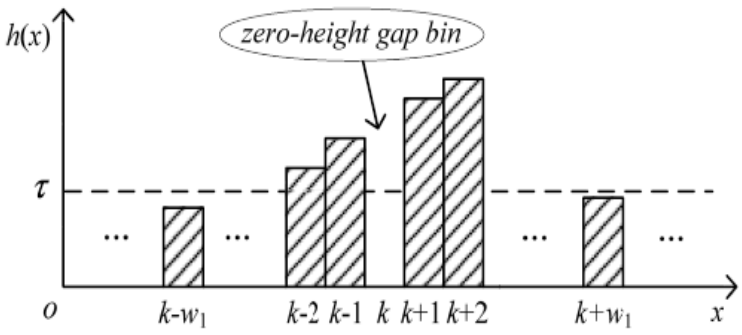

Fig. 1: Definition of a zero-height gap bin at k

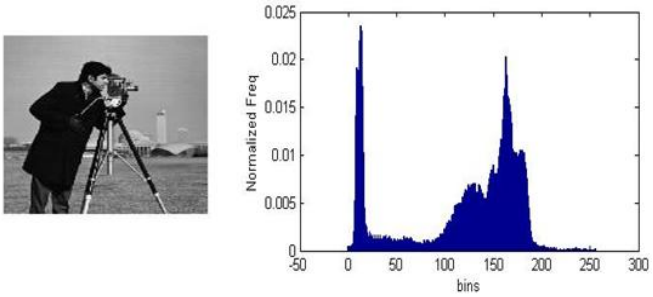

Fig. 2: Original input image and its corresponding histogram

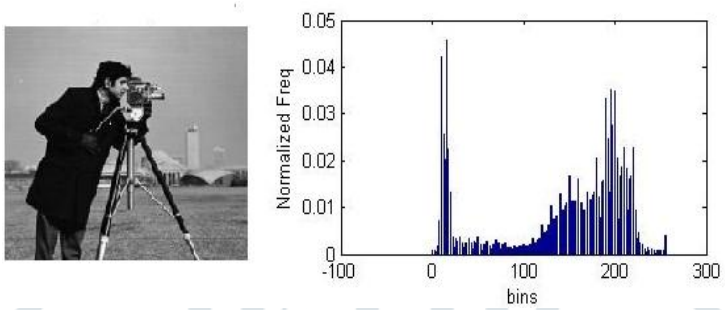

Fig. 3: Contrast enhanced input image and its histogram

Local Contrast Enhancement Detection

Cut-and-paste type image forgeries are detected using local contrast enhancement algorithm. The positional information of peak and gap bins could serve as fingerprinting feature for identifying different contrast enhancement manipulations. Figure.4 shows the composite image detection technique. From the figure, the test image I is first divided into non overlapping blocks. The zero-height gap bins are detected using global contrast enhancement detection algorithm. The positions of detected gap bins are stored. Peak positions are located by thresholding the difference between the gap-filled histogram and its filtered version. Peak bins are behaved as impulse noise. The detected peak positions are labeled. To further decrease detection errors, the extracted peak/ gap positions are corrected by retaining the co-existing peak/ gap positions in most blocks. The detected co-existing gap positions are recorded as Vg. To eliminate the gap bins which might not be caused by contrast enhancement, the corrected gap/peak position vector is generated using hadamard product.

To discriminate two source regions, first set a reference position vector for either one. Each block can be classified by the similarity between its position vector and the reference one. The block with the largest number of zero-height gap bins is believed to locate within one source region. To measure the overall similarity between the gap position vectors, each gap-involved pair should be investigated first. The similarity between V^{i}_{gc} and V_{gr}, denoted by m_g^i can be defined as the equation

$$m_g^i = \frac{\sum_{k \in \Omega_i \cap \Omega_{gr}} V_{gc}^i(k) \cdot V_{gr}(k)}{\sum_{k \in \Omega_i \cap \Omega_{gr}} V_{gc}^i(k) \cdot V_{gr}(k) + \overline{V_{gc}^i}(k) \cdot V_{gr}(k) + V_{gc}^i(k) \cdot \overline{V_{gr}}(k)}$$

Where, V^{i}_{gc} is the corrected gap position and V_{gr} is the gap reference vector. The reference peak position V_{pr} vector is created by combining the peak position vectors which are more possible from the source region of $V_{gr.}$ The similarity between V_{pc}^i and V_{pr}, marked as m_p^i, is defined in the same form by replacing the gap variables with the corresponding peak ones. If no peak involved pair exists, then we mark m_p^i = 1.

Adaptive SVM classifier for Composite Detection

Support Vector Machine (SVM) algorithm which is used for the classification of images, which takes into account all the parameters of the image. The goal of image classification is to predict the categories of the input image using its features. Using contrast enhancement detection algorithm image is classified into original or not. After that SVM is used to identify the tampered regions in the manipulated image. The process consists of two phases which are training phase and a testing phase. The training phase is the process of taking content that is known to belong to specified classes, and creating a classifier on the basis of the known content. This trained data are loaded in the testing phase and given to the SVM classifier. Using SVM, we can remove unnecessary region artifacts. Testing is the process of running the classifier on unknown content to determine the class

membership for the unknown content. During the training phase, the peaks and gaps of input image is compared with the ground truth image's peaks and gaps. If both regions are true, then it is tampered region, otherwise normal region. Ground truth images are known labels. Using ground truth images, we can identify whether the system is performing in a right way or not. We can validate the accuracy of the system. The peak and gap similarities of ground truth image are extracted and saved in a file. Test image features are compared with the stored features of ground truth image. Based on the comparison, forgery region is better detected with the help of the classifier. Compared to the previous method the proposed method has more than 10 percentage accuracy of forgery detection due to the nonlinear data analyzer. This method reduces the time and computational complexity. Figure.5 & 6 shows the proposed global contrast enhancement detection and figure.7 shows the composite image detection using the proposed method.

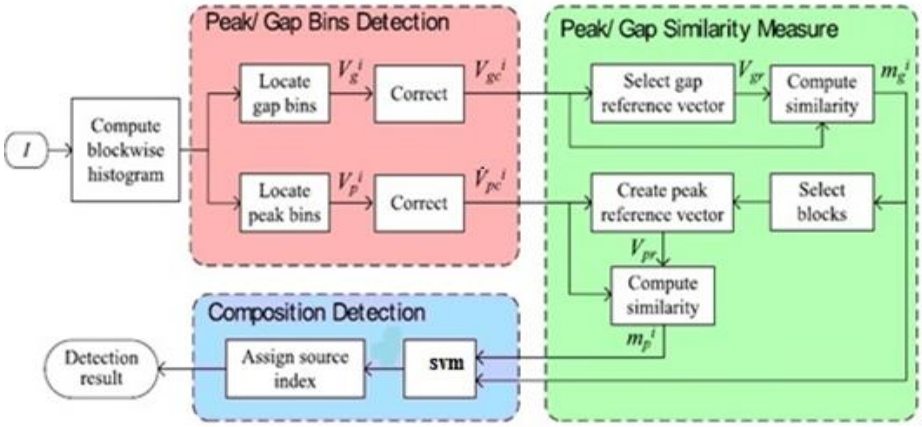

Fig. 4: Composite image detection technique.

Fig. 5: Input image and its gray scale image.

Fig. 6: Forgery region detection using the proposed method & its blockwise forgery region detection.

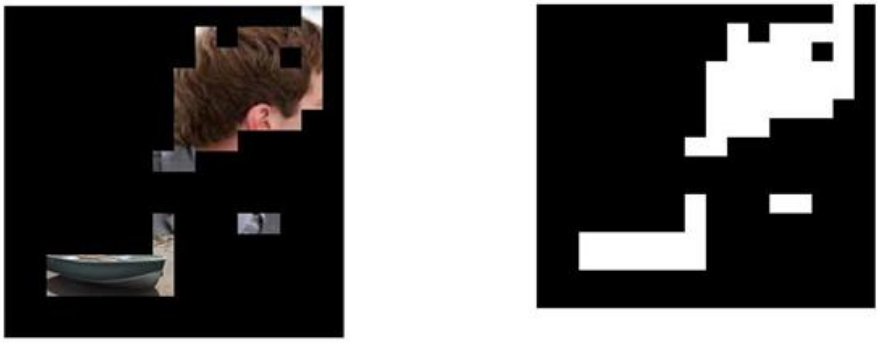

Fig. 7: Cut-and-paste type image forgery region detection using the proposed method and its blockwise detection.

IV. RESULT AND DISCUSSION

The input image is converted into gray scale image. Then the histogram is calculated. From the histogram, number of zero-height gap bins is detected. Consider w1 = 3(neighboring bins) and τ = 0.001(threshold value). Using the number of zero-height gap bins, we can findout whether the test image has undergone contrast enhancement or not. In the composite image detection algorithm, the peak/gap similarity measures m_g^i and m_p^i values are estimated by the blockwise pixel-value histogram and then apply SVM classifier for detecting the tampering region. Forgery regions are denoted using white blocks and background regions are denoted using black blocks. The accuracy of the proposed method is higher than the previous methods. The accuracy of the proposed method can calculated based on True Positive (TP), True Negative (TN), False Positive (FP), False Negative (FN) values. The receiver operating characteristic (ROC) curves are generated for evaluation. Figure.8 shows the Receiver operating curve.

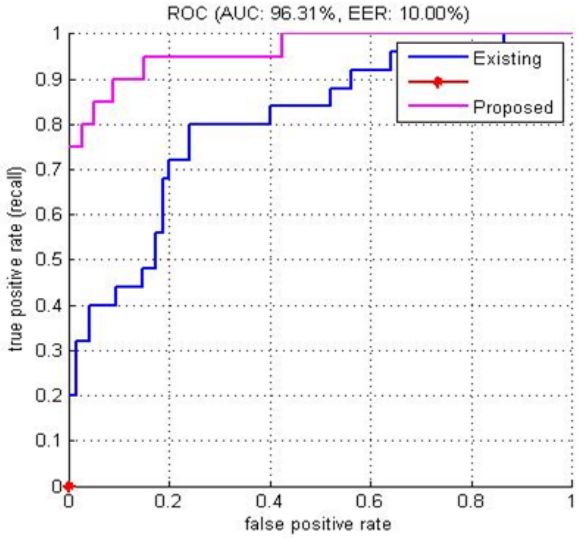

Fig. 8: ROC curve: Comparison of tampering region detection between existing and proposed method.

From the figure. 8, it is clear that the accuracy of the proposed method 90 % and expected error rate (EER) is only 10 %. There for the proposed method is better than the previous methods.

V. CONCLUSIONS AND FUTURE WORK

With the increased importance of digital images in various applications, where authenticity is of prime importance, it is necessary to verify the integrity and authenticity of digital images. But the creation of digitally forged images has increased. Detecting these image manipulations has become an important problem. The histogram of original image exhibits a smooth contour and that of enhanced image contains sudden peaks and gaps. In the proposed method, from the images histogram, the peak and gap similarities are calculated. The positions of detected blockwise peak/gap bins are clustered for recognizing the contrast enhancement mappings applied to different source regions. Finally, support vector machine (SVM) classifier is used to classify the input image into two categories. For that SVM is trained about the image, i.e which image belongs to normal and which belongs to forgery class. SVM classifier is used to detect the tampering regions more accurately in a composite image. Using ground truth image, tampered region is detected from the composite image. The experimental results show that the proposed method achieves high classification rate and considerably outperforms the previously presented methods. We can improve the efficiency of the ground truth image so that the tampered region is more accurately detected. When the efficiency of the ground truth image improved, accuracy of the proposed method can also be improved.

REFERENCES

[1] Hany Farid, "Image Forgery Detection [A survey]," IEEE Signal Processing Magazine, March 2009.

[2] M. Stamm and K. Liu, "Blind forensics of contrast enhancement in digital images," in 15th IEEE Int. Conference on Image Processing, 2008. ICIP 2008, Oct. 2008, pp. 3112–3115.

[3] A. Swaminathan, M. Wu, and K. J. R. Liu, "Digital image forensics via intrinsic fingerprints," *IEEE Trans. Inf. Forensics Security, vol. 3, no. 1*, pp. 101–117, Mar. 2008.

[4] M. C. Stamm and K. J. R. Liu, "Forensic detection of image manipulation using statistical intrinsic fingerprints," *IEEE Trans. Inf. Forensics Security, vol. 5, no. 3, pp. 492–506, Sep. 2010*.

[5] G. Cao, Y. Zhao, and R. Ni, "Forensic estimation of gamma correction in digital images," in Proc. 17th IEEE Int. Conf. Image Process., Hong Kong, 2010, pp. 2097–2100.

[6] M. C. Stamm and K. J. R. Liu, "Forensic estimation and reconstruction of a contrast enhancement mapping," in *Proc. IEEE Int. Conf. Acoust.,Speech Signal, Dallas, TX, USA, Mar. 2010, pp. 1698–1701*.

[7] Lin, X., Li, C.-T., and Hu, Y., "Exposing image forgery through the detection of contrast enhancement," Proceedings of IEEE International Conference on Image Processing, Melbourne, Australia (Sept. 2013).

[8] Gang Cao, Yao Zhao, *Rongrong Ni "*Contrast Enhancement-Based Forensics in Digital Images*,"* IEEE transactions on information forensics and security, vol. 9, no. 3, march 2014.

[9] Anita Sahani, K.Srilatha "Image Forgery Detection Using Svm Classifier," in Dept. Of E.C.E., Sathyabama University, Chennai, 2014.

[10] V.P.Kavitha, M.Priyatha "Novel Digital Image Forgery Detection Method Using SVM Classifier," in Dept. of ECE, Velammal Engineering College, Chennai, 2014.

[11] T. Arici, S. Dikbas, and Y. Altunbasak, "A histogram modication framework and its application for image contrast enhancement," IEEE Trans. Image Process., vol. 18, no. 9, pp. 19211935, Sep. 2009.

[12] B. Mahdian and S. Saic, "A bibliography on blind methods for identifying image forgery," in Image Commun., vol. 25, no.6,pp. 389399, Jul. 2010.

[13] T. Bianchi and A. Piva, " Detection of non-aligned double JPEG compression based on integer periodicity maps," in IEEE Trans. Inf. Forensics Security,vol. 7, no. 2., pp. 842848.

[14] T. H. Cao and A. C. Kot, "Manipulation detection on image patches using FusionBoost," in IEEE Trans. Inf. Forensics Security, vol. 7, no. 3.,pp.9921002, Jun. 2012.

[15] M .Sridevi, C.Mala and S.Sandeep "Copy – move image forgery detection," Computer Science & Information Technology (CS & IT) , Vol. 52 pp. 19–29, 2012.