VOL. 10, NO. 9, MAY 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences


www.arpnjournals.com

CONTRAST ENHANCEMENT BASED FORENSICS IN DIGITAL IMAGES AGAINST SECURITY ATTACK USING RSA ALGORITHM

G. Shirley and D. Ebenezer
Department of Electronics and Communication Engineering, Easwari Engineering College, Chennai, India
E-Mail: shalu.ruth@gmail.com

ABSTRACT

RSA algorithm is used to overcome security attack. Neural network classification is used to detect the forgery involved in digital images. Contrast Enhancement is typically used to adjust the global brightness and contrast of digital images. It is significant to detect contrast enhancement for verifying the originality and authenticity of the digital images. The main strategy relies on the blind identification of zero-height gap bins. Two data sets are taken for evaluation, namely, Dataset1 and Dataset2. Dataset1 is the unaltered image and Dataset2 is altered image from the original image. The detection of global contrast enhancement in both the images are determined. The zero-height gap bins in gray level histograms are exploited as identifying features. The probabilities of detection and false alarm determined by thresholds which are calculated as the percentage of the enhanced images correctly classified and that of the unenhanced images incorrectly classified, respectively. The receiver operating characteristic curves are generated for evaluation. The consistency between regional artifacts is checked for detecting image forgeries and locating composition boundaries.

Keywords: RSA algorithm, digital forensics, image forgery, contrast enhancement, neural network, composite image.

1. INTRODUCTION

Contrast enhancement is typically used to adjust the global brightness and contrast of digital images. It is important to detect contrast enhancement for verifying the originality and authenticity of the digital images. First, the focus is on the detection of global contrast enhancement applied to digital images, which are widespread in real applications. Histogram peak/gap artifacts incurred by the JPEG compression and pixel value mappings are analyzed and distinguished by identifying the zero-height gap. Second, it is proposed to identify the composite image created by enforcing contrast adjustment on either one or both source regions. The positions of detected block wise peak/gap bins are clustered for recognizing the contrast enhancement mappings applied to different source regions.

The feature consistency between regional artifacts is checked for discovering the image forgeries and locating the composition boundary. The probabilities of detection (Pd*)* and false alarm (Pfa*)* determined by thresholds are calculated as the percentage of the enhanced images correctly classified and that of the unenhanced images incorrectly classified, respectively. The receiver operating characteristic (ROC) curves are generated for evaluation.

Two data sets are taken for evaluation, namely, Dataset1 and Dataset2.Dataset1 is the unaltered image and Dataset2 is altered image from the original image. The global contrast enhancement is detected in both uncompressed and previously JPEG-compressed digital images. The zero-height gap bins in gray level histograms were exploited as identifying features [1]. A method is worked out to source-enhanced composite images, which invalidates previous detection methods. The composition boundary was accurately located by detecting the inconsistency between detected block wise peak/gap positional distributions. If the user id and password are correct then the pre-processing will take place and procedures are carried out. If the user id and password are incorrect the system will be stopped.

2. RSA ALGORITHM

The encryption and decryption process involves choosing two large distinct primes p and q and then form the public modulus n = pq. Choose public exponent e to be coprime to $(p-1)(q-1)$, with $1 < e < (p-1)(q-1)$.The pair (n, e) is the public key .The private key is the unique integer $1 < d < (p-1)(q-1)$ such that $ed = 1 \bmod (p-1)(q-1)$.Encryption: Split a message M into a sequence of blocks such as $M1$, M2, . . . , Mt where each Mi block satisfies $0 \leq Mi < n$. Then encrypt these blocks. Decryption: Given the private key d and the cipher text C, the decryption function is processed.

The encryption does not increase the size of a message. The message and the cipher text are the integers are in the range of 0 to n - 1.The encryption key is thus the pair of positive integers (e; n). Similarly, the decryption key is the pair of positive integers (d; n).

Each user makes his unique encryption key as public key, and keeps the corresponding decryption key as a unique private key. Time taken using mathematical relations in RSA make steps faster implemented than DES and Blowfish algorithms and with more secured data than symmetric systems [4]. RSA algorithm is more secure for the encryption and decryption using public and private key. It helps us to distinguish authorized and unauthorized clients.

3. PROPOSED SYSTEM

An initial input image is considered. Images from digital cameras can be further processed to improve their quality and accuracy of the digital images. This additional processing is typically executed by special software programs that can manipulate the images in a variety of ways. The RGB color model of the image is converted to

HSV. It is further send to the median filtering block in which one kind of smoothing technique is linear Gaussian filtering and all smoothing techniques are effective at removing noise in smooth patches or smooth regions of a signal but adversely affects the edges of the images.

The adaptive histogram is a computer image processing technique used to improve contrast in images. It improves by transforming each pixel with a transformation function derived from a neighborhood region. Pixels near the image boundary have to be treated specially, because their neighborhood would not lie completely within the image. The peak and gap bins are calculated from the adaptive histogram. The base layer and detail layer reduces the peak/gap bins of the digital image. Then saliency mapping is done with the base and detail layer of the image. Features like image analysis, texture analysis and texture of the digital image is calculated. Using support vector machine technique the image is classified weather its original image or forgery image. Neural network constructs a hyperplane or set of hyperplanes in a high or infinite-dimensional space, which can be used for classification. Since it's of two dataset are large database we opt for neural network than SVM technique. Dataset 1 contains the original characteristic information of the image and dataset 2 will analysis the entire process of the testing image and the two dataset are compared. Based on the analysis of histogram peak-gap artifacts, the peak-gap pattern can be considered as statistical fingerprint for estimating the mapping function which is determined by the gamma parameter.

The fresh image is browsed from the system and the RSA algorithm pre-processing is done. The user id, password and key are given correct then the filtering process is carried out. If the user name, password and the key given is wrong it won't login in and the system gets stopped. The important blocks involved in the process are median filter, adaptive histogram, calculating peak and gap bins, feature calculation, saliency mapping and neural network classification. Image analysis is done by canny edge detector, the feature calculated are contrast, mean, entropy, standard deviation and correlation.

The neural network is used instead of SVM since to enlarge the database, it increases the robustness, accuracy of the digital images. It has to be developed as a user friendly application in a secured way using RSA algorithm. The main strategy relies on the blind identification of zero-height gap bins. Peak bins which behave as impulse noise can be located by median filtering. The block diagram of the system is shown in Figure-1.

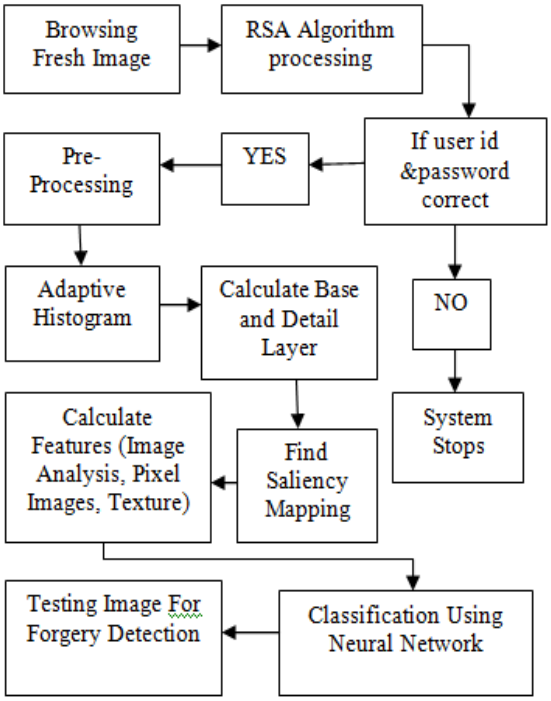

Figure-1. Block diagram.

4. SOFTWARE SIMULATION

4.1 Implementation in MATLAB

The RSA algorithm is used to access only authorized users to carry out the process. If the user and password entered by the client is correct then the process is carried out. The client should give the correct private key to decrypt the encrypted program. The digital image is taken and the image is resized in a particular format. The conversion from RGB to HSV is done to have clear picture of the digital image. The corresponding histograms are also found. Pixel values are calculated for the test image and for the converted image. Median filter is applied to remove noises in the digital images. The histogram of the median filter is found. The image is enhanced in the next step and the histogram is found for the enhanced image. Edge detection using Gauss gradient is done and the base and detail layer of the image is extracted. Saliency mapping is done with the base and detail layers of the image. Image analysis-edge features are calculated and the ROC curve is found for the image. Contrast enhancement for dataset1 and dataset2 are compared. The neural network classification is used to detect the forgery involved in the digital images. The pcode is generated so that even the authorized clients can not alter the program. Thus the output simulation in matlab is done. pcode(fun) obfuscates the code usually as fun.m and then produces a file called fun.p for the original file, known as a P-file. Consider fun is a folder, then all the script or the function files in that folder are obfuscated in P-files. MATLAB creates the P-files in the current folder. The original .m file or folder can be

anywhere on the search path. Pcode (fun1,...,funN) creates N P-files from the listed files. If any inputs are folders, then the MATLAB creates a P-file for every .m file the folders contain. Pcode (fun,'-inplace') creates P-files in the same folder as the script or function files.

5. RESULTS AND DISCUSSIONS

The RSA algorithm is implemented for security purpose. If the user name, password, key given by the user are correct. It will be logged in; if the user name, password and key given are incorrect then it will be logged out. The encryption process is shown in the Figure-2.

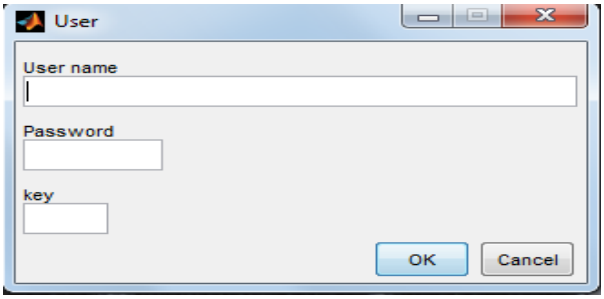

Figure-2. RSA algorithm implementation.

The user name, password and the key is entered by the user. If its incorrect the system will not log in, only if the username password and the key is correct. It will be logged in. The details entered are shown in the Figure-3.

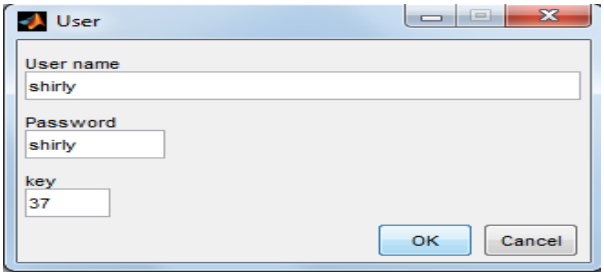

Figure-3. Details are entered.

The input image is resized to a particular size, since in matlab the images are considered for a particular size 256*256.Hence the image is resized shown in the Figure-4.

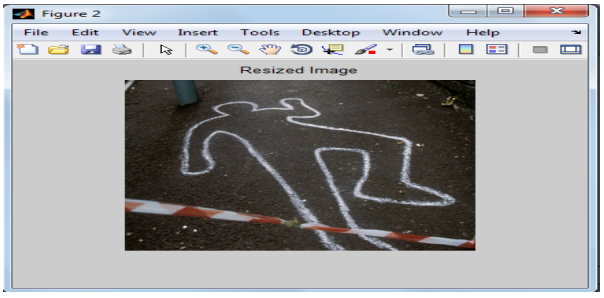

Figure-4. Resized image.

The image is converted from RGB to HSV since to have clarity of the image. The HSV color space describes colors in terms of the Hue, Saturation, and Value. The converted image is shown in Figure-5.

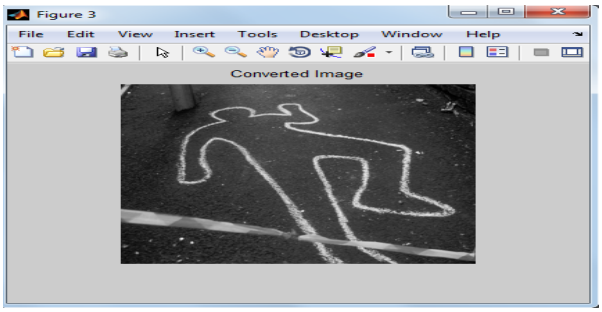

Figure-5. Converted image.

The histogram of the converted image from the RGB to HSV is found. The histogram of converted image is shown in Figure-6.

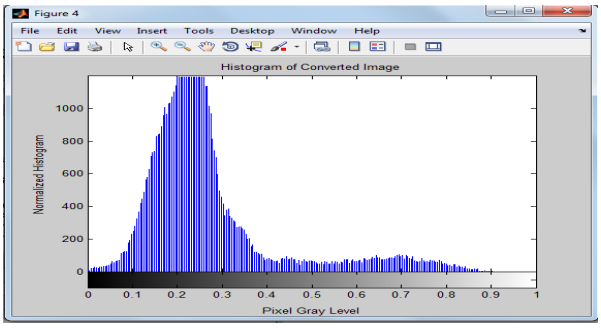

Figure-6. Histogram of the converted image.

The pixel values of the image before conversion of HSV and image after conversion of HSV are mapped in pixel value mapping are shown in the Figure-7.

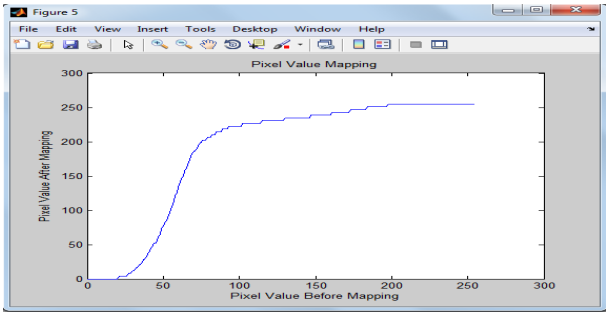

Figure-7. Pixel value mapping.

The filtered image using median filter of the image is done to remove noises like Gaussian noise, salt and pepper noise, impulse noise. The median filter implemented image is shown in the Figure-8.

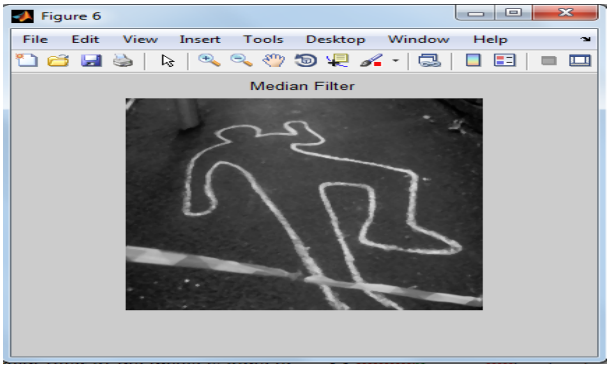

Figure-8. Median filtered image.

The histogram of the filtered image is found from the median filtered image. The histogram of the filtered image is shown in the Figure-9.

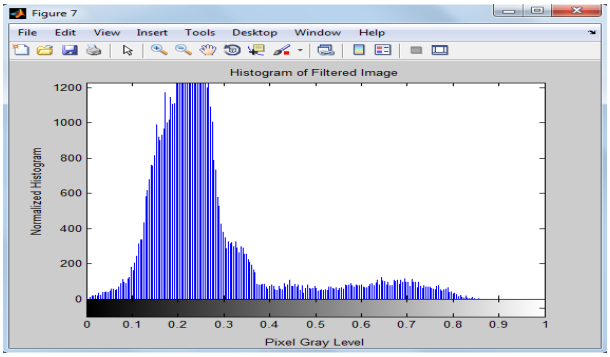

Figure-9. Histogram of the filtered image.

The filtered image is enhanced so that the contrast is enhanced in the image after filtering process. The enhanced image is shown in the Figure-10.

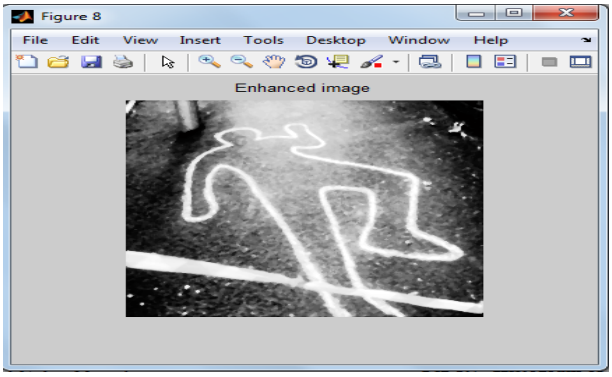

Figure10. Enhanced image.

The histogram of the enhanced image is shown the Figure-11.the contrast of the image is increased in this enhancement process.

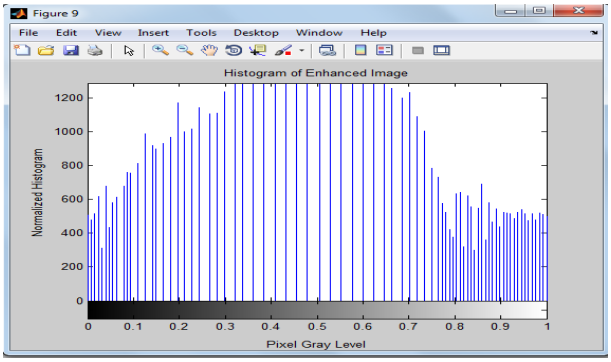

Figure-11. Histogram of enhanced image.

Image gradients may be used to extract information from images. The edge detection using gauss gradient of the image is shown in Figure-12.

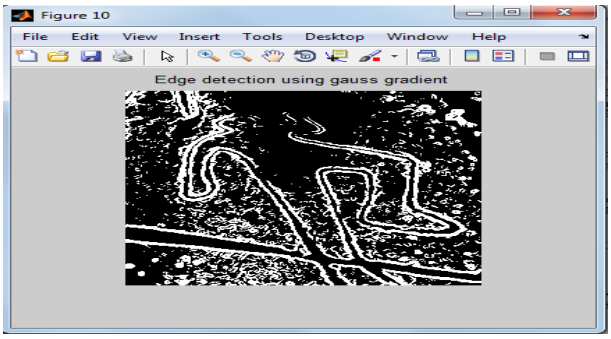

Figure-12. Edge detection using Gauss Gradient.

The base layer provides geographic context for your imagery. It gives the detail layer of the gap bins in the digital image. The base layer of the image is shown in Figure-13.

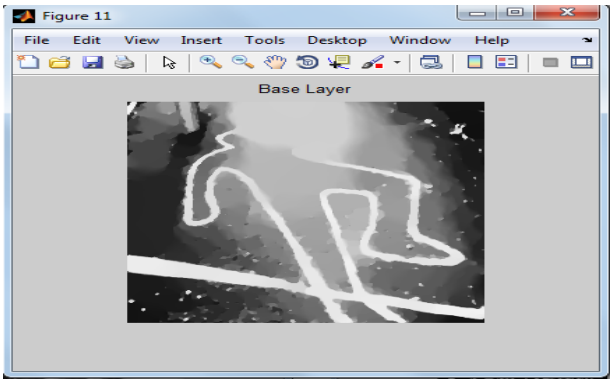

Figure-13. Base layer of the image.

The histogram of the base layer of the image is found. The gap bins in the digital images are reduced and the histogram of base layer of the image is shown in Figure-14.

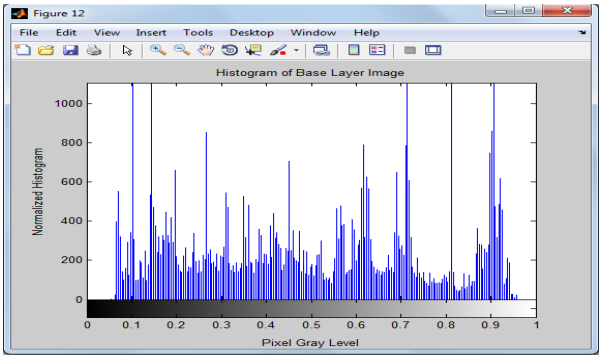

Figure-14. Histogram of base layer of the image

The detail layer of the image is found from base layer subtracted in enhanced image. It gives the details of the gap bins in the digital image. The detail layer of the image is shown in Figure-15.

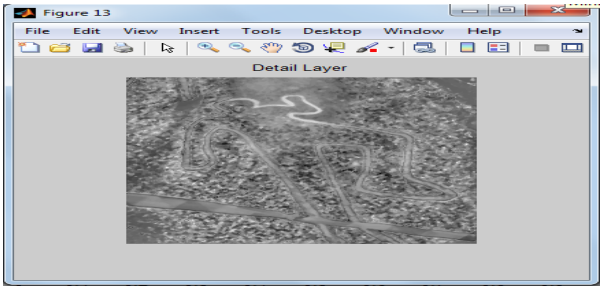

Figure-15. Detail layer.

The Histogram of the detail layer is found. The peak bins are reduced. The histogram of detail layer is shown in Figure-16.

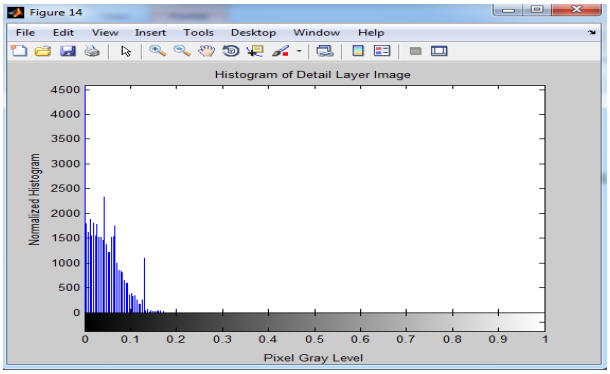

Figure-16. Histogram of detail layer.

Saliency mapping is done using base and detail layer of the image. The complete contrast and saliency estimation can be formulated in a unified way using high-dimensional Gaussian filters. The saliency mapping is shown in Figure-17.

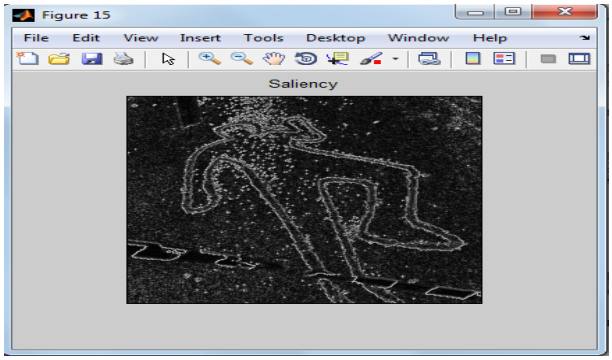

Figure-17. Saliency mapping.

The image analysis edge feature is done by using canny edge operator,for good detection, good localization and minimal response. The image analysis-edge feature of the image is shown in Figure-18.

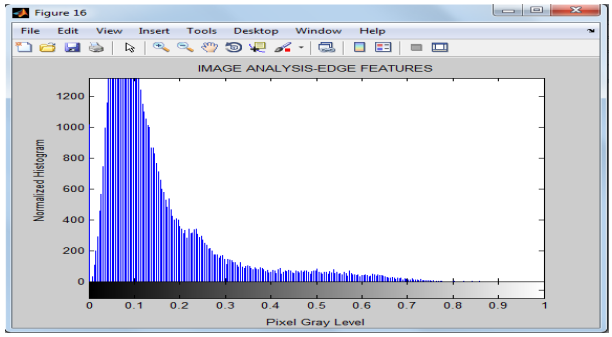

Figure-18. Image analysis-edge features.

The ROC curve the true positive rate (TPR) and false positive rate (FPR) are needed and plotted in the graph. The ROC curve is shown in Figure-19.

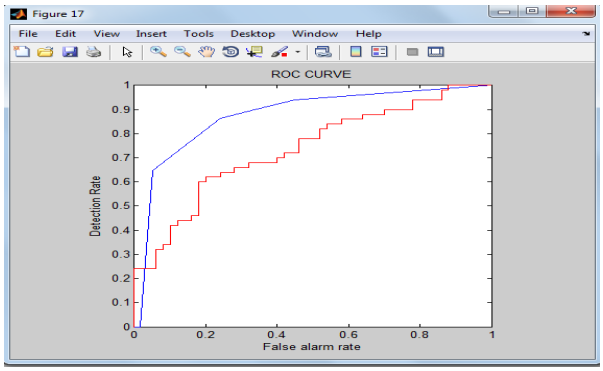

Figure-19. ROC curve.

The probability of detection rate and probality of flase alarm rate is plotted for the dataset1 and dataset 2. The contrast enhancement detection ROC curve for dataset1 is shown in figure-20.

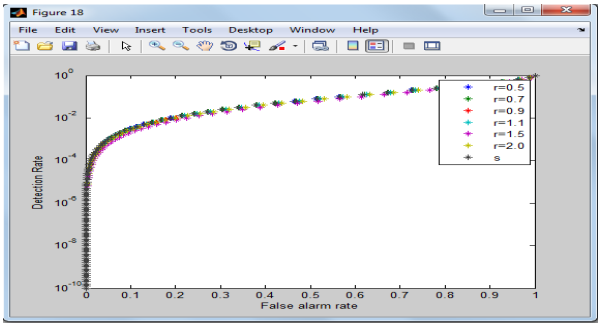

Figure-20. Contrast enhancement detection ROC curve for Dataset 1.

The probability of detection rate and probality of flase alarm rate is plotted for the dataset1 and dataset 2 and the contrast enhancement detection ROC curve for dataset1 is shown in Figure-21. Gamma correction is denoted as 'r' and saliency value is denoted as 's'.

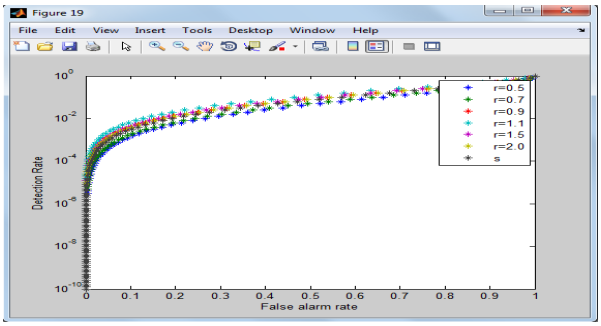

Figure-21. Contrast enhancement detection ROC curve for Dataset 2.

6. CONCLUSIONS AND FUTURE WORK

The proposed work is mainly to deal with the forgery detection in a secure way using RSA algorithm and pcode generation in the digital image using contrast enhancement. RSA algorithm and pcode generation make it more secure from the hackers. The performance parameters such as mean, entropy and standard deviation are measured between SVM technique and neural network. Neural network helps us to increase the number of images, its robustness and accuracy of the digital images. Thus this work can be extended further to develop robustness in this process.

REFERENCES

[1] Andrea Costanzo , Irene Amerini , Roberto Caldelli and Mauro Barni. 2014. 'Forensic Analysis of SIFT Keypoint Removal and Injection', Published in Information Forensics And Security, IEEE Transactions on Vol. 9, No. 9, pp.1450-1464.

[2] Gang Cao and Yao Zhao. 2014. 'Contrast Enhancement-Based Forensics In Digital Images', Published in Information Forensics And Security, IEEE Transactions on Vol. 9, No. 3, pp. 515-525.

[3] Ayesha Khan, Parul Bhanarkar and Pragati Patil. 2013. 'RSA Encryption Technique based on Geo Location',Published in International Journal of Advanced Research in Computer Science and Software Engineering on Vol. 3, No. 4,pp.968-971.

[4] Ali E. Taki El_Deen, El-Sayed A. El-Badawy and Sameh N. Gobran. 2014. 'Digital Image Encryption Based on RSA Algorithm' Published in IOSR Journal of Electronics and Communication Engineering on Vol. 9, No. 1, pp. 69-73.

[5] Hung-Min Sun, Mu-En Wu, Wei-Chi Ting and M. Jason Hinek. 2007. 'Dual RSA and Its Security Analysis' Published in Information Theory, IEEE Transactions on Vol. 53, No. 8, pp. 2922-2933.

[6] Seung won Jung. 2013. 'A modified model of the just noticeable depth difference and its application to depth sensation enhancement', Published in Image Processing IEEE Transactions on Vol. 22, No. 10, pp.1040-1045.

[7] Hong Cao and Alex C. Kot. 2012. ' Manipulation Detection on Image Patches Using FusionBoost', Published in Information Forensics And Security, IEEE Transactions on Vol. 7, No. 3, pp. 992-1002.

[8] Matthew C. Stamm and K. J. Ray Liu. 2010. ' Forensic Detection of Image Manipulation Using Statistical Intrinsic Fingerprints', Published in Information Forensics And Security, IEEE Transactions on Vol. 5, No. 3, pp. 492-506.

[9] Mahdian , B .and Saic, S. (2010) 'A bibliography on blind methods for identifying image forgery', Image Commun., Vol. 25, No. 6, pp. 389-399.

[10] Tarik Arici and Salih Dikbas. 2009. ' A Histogram Modification Framework And Its Application For Image Contrast Enhancement ',Published in Image Processing, IEEE Transactions on Vol 18, No. 9, pp. 1921-1935.

[11] Fari H. 2009. 'Image forgery detection', IEEE Signal Process. Mag., Vol. 26, No. 2, pp.16–25.

[12] Swaminathan A., Wu M. and Liu K. J. R. 2008. 'Digital image forensics via intrinsic fingerprints', IEEE Trans. Inf. Forensics Security, Vol. 3, No. 1, pp. 101–117.