Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 04, April -2018

OFFLINE FORGERY DETECTION OF HANDWRITTEN SIGNATURE USING GAUSSIAN EMPIRICAL RULE

[1]G.Gowri Pushpa, [2]G.Santoshi

[1, 2] *Assistant Professor, Department of CSE, ANITS, Visakhapatnam.*

ABSTRACT - *Signature authentication is most widely used in verifying a person's identity. In this paper Global and Geometric features are discussed. Before extracting the features, preprocessing of a scanned image is necessary to isolate the region of interest part of a signature and to remove any spurious noise present. The system is trained initially with the data-set of signatures obtained from those individuals whose signatures are to be authenticated by the system. All the features are computed for training samples of signature. There are some variation itself in features of genuine set of signatures. If testing signature sample satisfies the Gaussian empirical rule it is authenticated as original signature otherwise a forged one.*

KEYWORDS: *Global and Geometric features, Gaussian empirical.*

1 INTRODUCTION

A signature is a signatory or signer of a person identity and it may be confused with an autograph, which is chiefly an artistic signature. This can lead to confusion when people have both an autograph and signature. Verification can be achieved either Offline or Online.

Figure 1 A sample signature image

Signature Verification system can be generally divided into two categories: A static method (called as Offline) that extracts shape related information as in Figure 1. It is generally used for lower authentication needs. Off-line data is a 2-D image of the signature. Processing Off-line signature is complex due to the absence of stable dynamic characteristics. Difficulty also lies in the fact that it is hard to segment signature strokes due to highly stylish and unconventional writing styles. A dynamic method (called as Online) with time related information that extracts dynamic features such as speed, pressure, time information which cannot be imitated. It is used for higher authentication. In present system a signature sample is taken and its global and geometric features are calculated and are verified using Euclidean distance to authenticate whether the sample considered is original or a forged one.

1.1 FORGERY AND ITS TYPES

The action of forging a copy or imitation of a document, signature, banknote, or work of art. Forgery is one the techniques of fraud including identity theft with a produced altered objects of another's rights illegally.

1.1.1 Types of forgery

The main task of any signature verification system is to detect whether the signature is genuine or not. The forgeries signature is difficult to obtain the instrument and the results of verification depend on the type of the forgery as in Figure 2.

Basically there are three types:

1. Random forgery: A signature sample that belongs to a different writer
2. Simple forgery: A signature with the same shape or the genuine writer's name
3. Skilled forgery: A Signature is written by a person who had access to a genuine signature for practice.

@IJAERD-2018, All rights Reserved

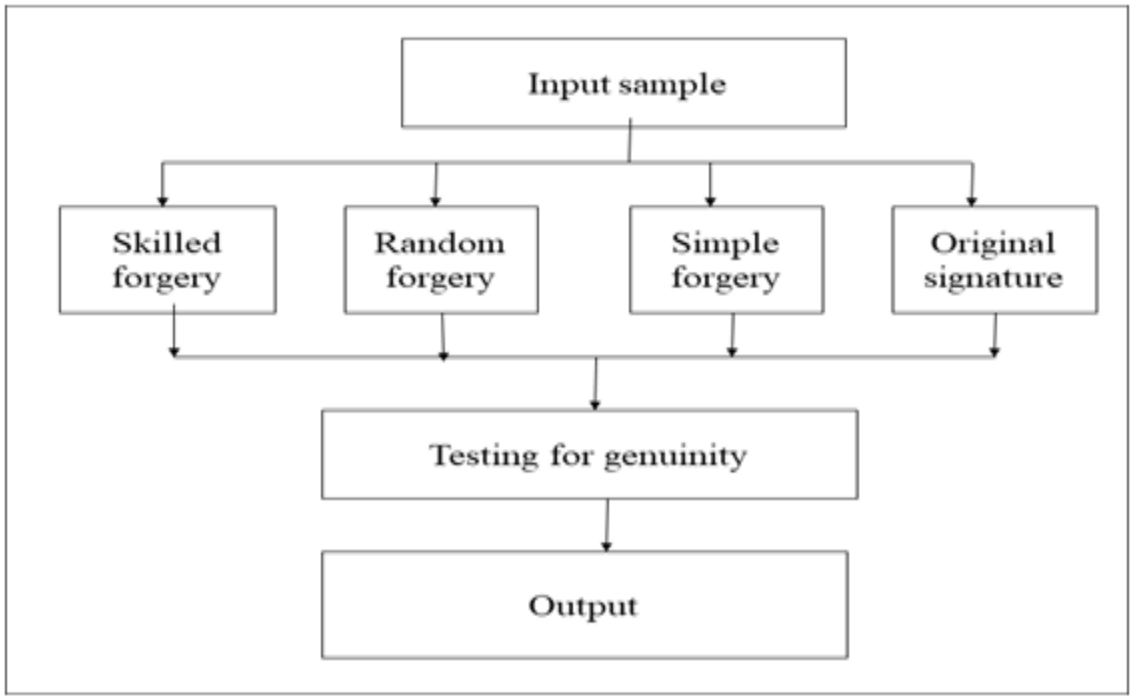

Figure 2 Forgery types

2. BACKGROUND WORK

2.1 Steps Involved In Preprocessing

The preprocessing steps are very much necessary for the signature authentication as without the region of Interest is very difficult to cross verify the steps involved in preprocessing are shown in the below section**.**

2.1.1 RGB to Gray Scale conversion:

The first pre-processing step is to convert an RGB image in Figure 3 to a Gray Scale image in Figure 4 that means conversion of a true color image RGB to the grayscale intensity image.

Figure 3 RGB Image Figure

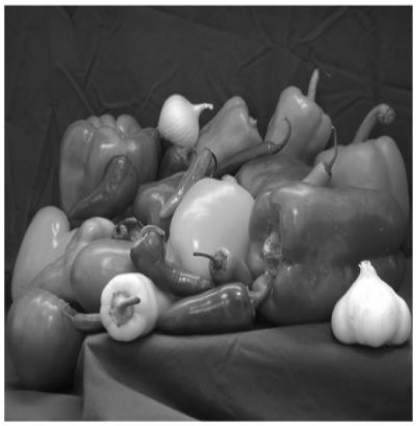

Figure 4 Gray Scale Image

2.1.2 Binarization:

Binarization means converting a gray scale image into a binary image. A binary image as in Figure 6 is a digital image that has only two possible values for each pixel. Typically the two colors used for a binary image are black and white though any two colors can be used. Binary images are also called bi-level or two-level. Statistical analysis of gray- level images may include determination of mean, variance. Standard deviation, contrast stretch, histogram etc. or it can be a combination of any of these Determination of a threshold value is very much important and perhaps the most sensitive part of any image binarization scheme because a wrong value of threshold may result in losing some image information (an object can be considered as part of background and vice versa).

@IJAERD-2018, All rights Reserved

$$Q=S/(X*Y) \quad (1)$$

where

Q=Threshold Value
S=Sum of all the pixel value in the image
X=height of the image
Y=width of the image

Figure 5 Original Image

Figure 6 Binarized Image

2.1.3 Edge Detection:

Edge detection is a method of identifying edges in a digital image at which the image brightness changes sharply. In this paper we are using the canny edge detector is an edge detection operator that uses to detect a wide range of edges in images.

2.1.4 Noise removal:

Image noise is a method of removing noise from image. In this for removing noise from an image as in Figure 7 after applying Median filter as in Figure 8 that removes noise efficiently.

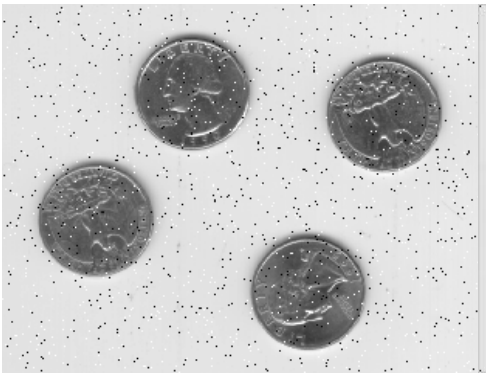

Figure 7 Image with noise

Figure 8 after applying Median Filter

2.1.5 Region of Interest:

Cropping is done with respect to bounding box of image by calculation the first foreground row, first foreground column, last foreground row, last foreground column to obtain region of interest.

Figure 9 Image showing region of interest

2.2 FEATURE EXTRACTION

The objective feature of this phase is to extract the features of the test image that will be compared to the features of training image for verification process. There are two types of features ie. Global and Geometric feature [3]. The Global features are Height, Width, Aspect ratio, Area of black pixels and Normalized Area. The Height is the distance between two points in the vertical projection and must contain more three pixels of the image for a binary image. For a binary signature image, width is the distance between two points in the horizontal projection and must contain more than 3 pixels of the binary image. Aspect Ratio is defined as ratio of width to height of a signature. Area of black pixels can be

@IJAERD-2018, All rights Reserved

defined as the number of black pixels in the image. The normalized area of black pixels can be defined as ratio of number of black pixels to the total number of pixels in the image. The Geometric features [8] are Mean, Variance and Standard deviation. The mean of a data set is simply the arithmetic average of the values in the set, obtained by summing the values and dividing by the number of values.

$$\mu=\sum X/N \quad (2)$$

In a data set is the arithmetic average of the squared differences between the values and the mean

$$\sigma^2= (\sum(X-\mu) \wedge 2)/N \quad (3)$$

The standard deviation is simply the (positive) square root of the variance.

$$\sigma = \sqrt{((\sum(X-\mu)^2)/N)} \quad (4)$$

3 PROPOSED WORK

Gaussian distribution can accommodate around 99.7% of features or observations which fall within three standard deviation of the mean and which is between μ-3σ and μ+3σ. Feature points are considered as the features extracted from query signature images while mean and standard deviation are found from signature database. Each feature point is tested within the range of three standard deviation of the mean. The equation below is used to select some important feature points from a given signature.

$$|\mu - x| <= k * \sigma \quad (5)$$

where
μ and σ are mean and standard deviation
x is the value of some feature extracted from signatures
k can be 1, 2, 3 and derived from Gaussian empirical properties to test the closeness of the current query sample to the distribution mean of database.

The purpose of forgery detection is to design a program through which we can detect a forged signature from that of an original one. The existing algorithms are used to detect forged signatures but the false acceptance rate and false rejection rate are high. In order to reduce these para

meters we use Gaussian Empirical Rule [5].

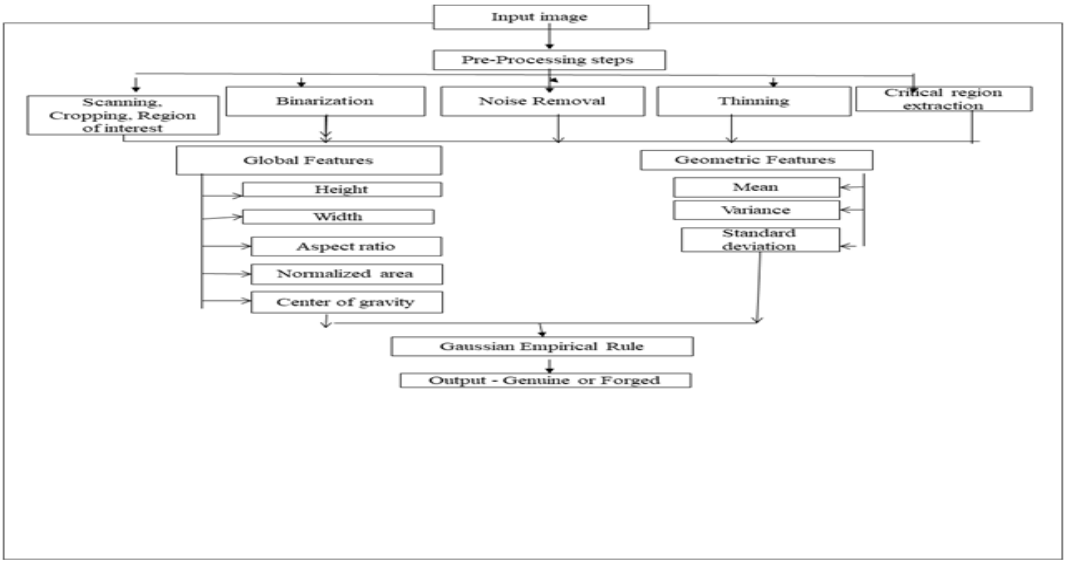

Figure 10 System Architecture

3.1 ALGORITHM STEPS FOR GAUSSIAN EMPIRICAL RULE

The Gaussian rule[5] is applied to the query signature sample for which all the global and geometric features are calculated. The geometric features are considered from that of the corresponding original signature of query signature that is already available in the trained set as shown in Figure10. Trained set of Signature originals should be collected

@IJAERD-2018, All rights Reserved

from various persons. Based on these trained signatures the query signatures are authenticated whether they are genuine or forged one. In Gaussian Empirical rule implementation as explained in equation 5. The geometric features mean and standard deviation are considered from trained set itself.

Pre- processing steps are

Consider an input query signature.

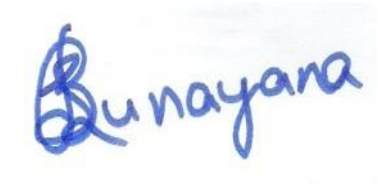

Figure 11 Query Image

In Figure 11 query is now to undergo the pre-processing steps like RGB to Gray scale image, binarization, edge detection, noise removal and region of interest.

Step 1: The Gray image is obtained as follows
Step 2: Binarized Image and Edge detection (using canny edge detection algorithm).
Step 3: Noise free (Using median filter to remove salt and pepper noise from the image).
Step 4: Region of interest by cropping.
Step 5: Extract the global features like height of the image, width of the image, aspect ratio, area of black pixels in the image and its normalized area.

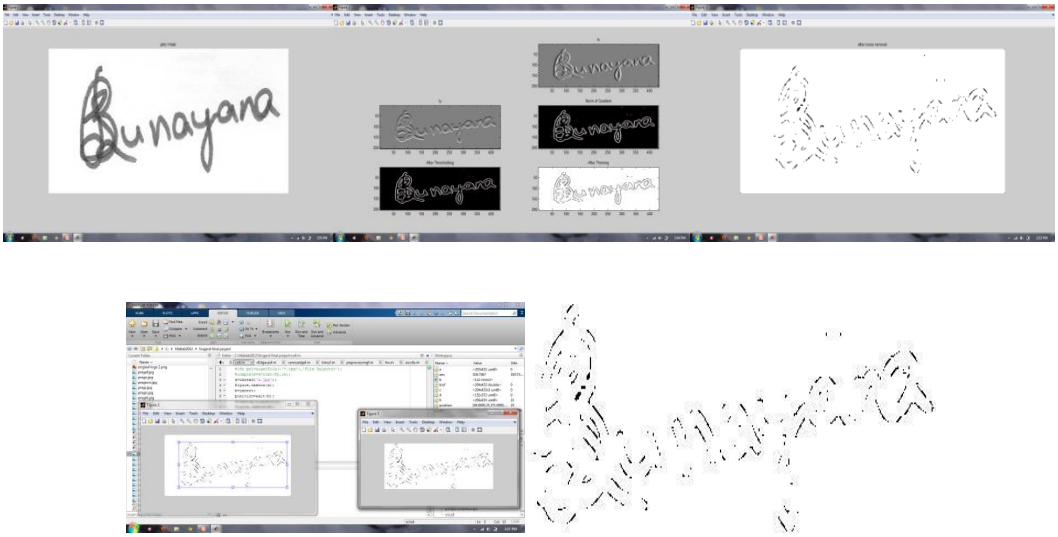

Figure 12 Preprocessing Steps

4 EXPERIMENT RESULTS

4.1 INPUT:

Figure 13 A query sample Figure 14 The trained sample

@IJAERD-2018, All rights Reserved

OUTPUT:
The query sample when authenticated using Gaussian empirical rule is resulted as a forged one.

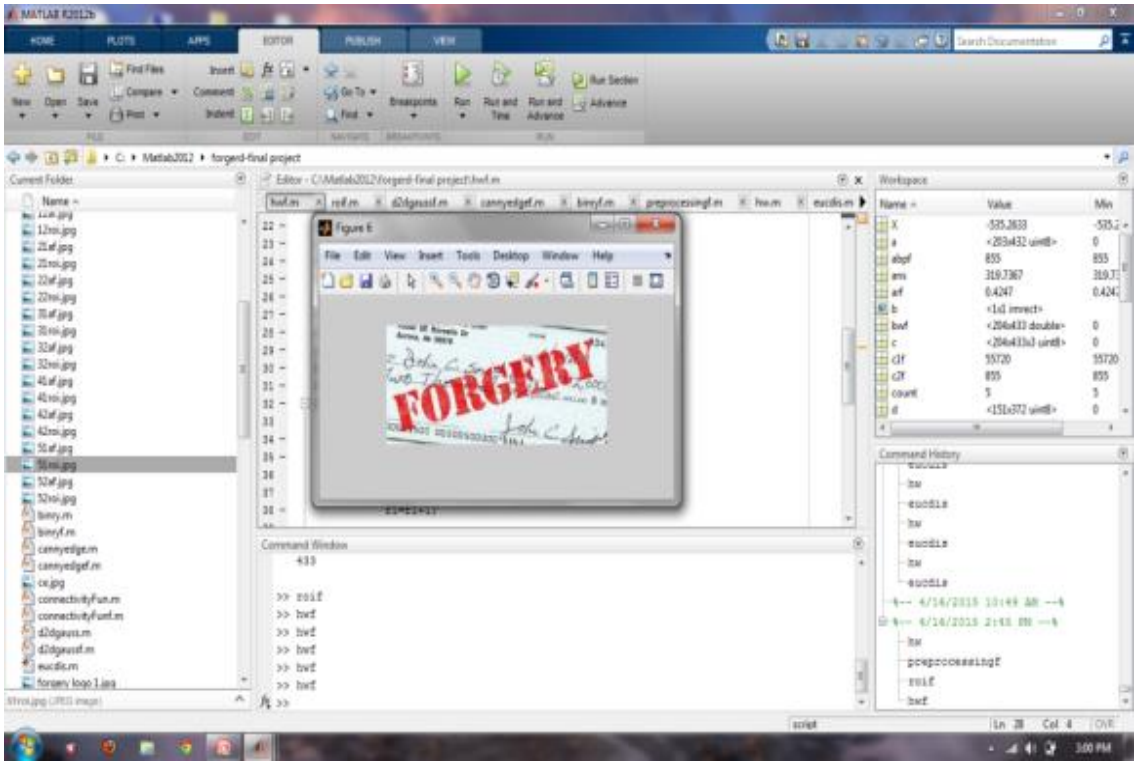

Figure 15 Output obtained after Gaussian rule implementation

4.2 COMPARISON OF TEST RESULTS:

The comparison of outputs is done using proposed system characteristics and existing system characteristics. The characteristics involved in this process are False Acceptance Rate and False Rejection Rate. False acceptance rate can be defined as ratio of the number of forged signatures authenticated as original to the total number of forged signatures. False rejection rate can be defined as ratio of the number of original signatures authenticated as forged to the total number of original signatures.

Table 1 Proposed System Characteristics

Types of Signatures	False Acceptance Rate (FAR)	False Rejection Rate (FRR)
Original	-----	0
Forged	0.13	-----

Table 2 Existing System Characteristics

Types of Signatures	False Acceptance Rate (FAR)	False Rejection Rate (FRR)
Original	-----	0.6
Forged	0.6	-----

5 CONCLUSION

The results of Gaussian Empirical Rule are observed and the implementation is better than that of Euclidean distance in authenticating the signatures. In Gaussian empirical rule, each feature is compared with the multiple of standard deviation and if all the features satisfies then it is authenticated as original otherwise forged but where as in Euclidean distance, an acceptance range is considered and authentication of signatures is decided which varied the FAR and FRR.

@IJAERD-2018, All rights Reserved

By comparing the two characteristics FAR and FRR results of proposed system are shows the efficient. The scope of improvement to the proposed system can be developed in various algorithms such as graph theory, SVM etc.

REFERENCES

[1] Armand, S., Blumenstein, M. and Muthukkumarasamy V, "*Offline signature verification using the enhanced modified direction feature and neural-based classification*", Proceedings of International Joint Conference on Neural Networks, Vancouver, pp.684–691, (2006).

[2] Anu Rathi, Divya Rathi, Parmanand Astya , "*Offline handwritten Signature Verification by using Pixel based Method*" International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Volume 1 Issue 7, September (2012).

[3] K. Huang, H. Yan, "*Off-line signature verification based on geometric feature extraction and neural network classification*", Pattern Recognition, volume 30, issue 1, pp. 9-17, (1997).

[4] M. Hanmandlu, K.R. Murali Mohan, S. Chakraborty, G. Garg, "*Fuzzy modeling based signature verification system*", in: Proceedings of the sixth International Conference on Document Analysis and Recognition, USA, pp.110- 114, (2001)

[5] D. R. Kisku, A. Rattani, P. Gupta, "*A Novel Approach to Offline Signature Verification using Gaussian Empirical Rule*", 6th European Conference on Information Warfare and Security (ECIW 2007), pp. 139-150, (2007).

[6] R. Sabourin, R. Plamondon, G. Lorette, "*Offline identification with handwritten signature images: survey and perspectives*", Structured Image Analysis, Springer, New York, 1992, pp 219-234. Advanced in Information Sciences and Service Sciences Volume 2, issue 3, September (2010)

[7] R. Plamondon, S.N SriHari, "*Online and Offline handwriting recognition: a comprehensive survey*", IEEE Trans. Pattern Anal. Mach. Intell. Volume 22 issue 1, pp 63-84, (2000).

[8] V. Nguyen, M. Blumenstein, G. Leedham, "*Global features for the offline signature verification problem*", 10th International Conference on Document Analysis and Recognition, ICDAR.,(2009)

@IJAERD-2018, All rights Reserved