INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN: 2278 – 0211 (Online)

Signature Verification And Application In Data Encryption

Mr. S. P. Kosbatwar
Assistant Professor, Department of Computer Engineering,
Smt. Kashibai Navale College of Engineering, Pune, India

Rohit K. Marne
Department of Computer Engineering, Smt. Kashibai Navale College of Engineering
Pune, India

Saurabh S. Thube
Department of Computer Engineering, Smt. Kashibai Navale College of Engineering
Pune, India

Satyajeet V. Sabale
Department of Computer Engineering, Smt. Kashibai Navale College of Engineering
Pune, India

Abstract:

This paper tells how the signature verification is used for security problems. An improved offline signature verification scheme is used which is based on the feature points. The scheme described gives the differences between the two types of original and forged signature. This method takes care of all types of forgeries done in the signature. The two parameters used in signature verification scheme are False Acceptance Rate (FAR) and False Rejection Ratio (FRR).

Key words: *Offline signature, FAR(False Acceptance Rate), Feature point, FRR(False Rejection Rate), Forgeries, Euclidean Distance model.*

1.Introduction

Signature verification is used in automatic identity verification applications such as legal, banking and other applications. This paper discusses the importance of a signature verification, it explains how it can be implemented and developed through certain features. This paper deals with the method of verification of the signature and recognition by using the features that characterizes the signature.

The signature verification and recognition allows the user to detect whether a signature is original or forged. The algorithms used have given improved results as compared to the previously proposed algorithm. A lot of research has been done on offline signature verification. In the signature verification is based on Feature Point Extraction Method. The verification is performed by comparing the trained feature points with the feature points that are extracted from the image. Each pixel of the signature is studied and extracted the end points of the signature.

There are three different types of forgeries as follows. The random forgery is the forgery which is done by the person who doesn't know the shape of original signature. The simple forgery is the type of forgery which is represented by a signature sample which is written by a person who knows the shape of the original signature without much practice. The skilled forgery is represented by a suitable form of the genuine signature. Fig.1 shows the different types of forgeries.

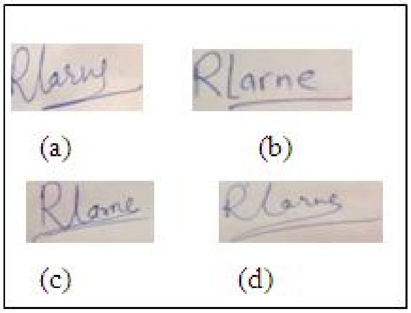


Figure 1: (a) Original Signature, (b) Random forgery, (c) Simple Forgery, and (d) Skilled forgery.

2.Proposed Method

Offline signature verification consists of the steps given below :

- Image Preprocessing.
- Feature Extraction.

- Pattern Matching.
- Signature Recognition.

- Image Preprocessing : In this the image is first taken from the user on the paper. Then it is taken by scanner in Portable Network Graphics (PNG) format as shown in the Fig. 2.

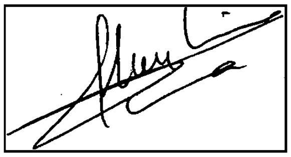
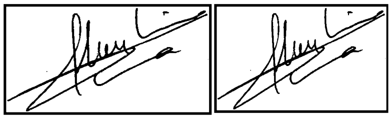


Figure 2: Portable Network Graphics(PNG)

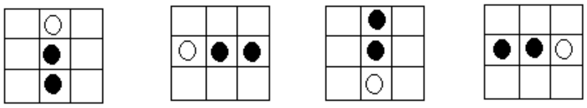
We get all the values of the colors. The Red, Green, Blue values are stored in some variable. These values are used to convert the image into the greyscale image. The GreyScale is found by taking the average of all RGB values. Then the thresholding of the image is done for the black and white image. The threshold value is set and according to that value the bit is set to zero or one where one indicates white and zero indicates black. The images are shown in the Fig. 3.



(a) (b)

Figure 3: (a) Grayscale image (b) Threshold image

In thinning the signature made by some marker pen or pen having some width is taken and it is made to the regular size. The Stentiford Algorithm is used for the thinning purpose. It uses the following four templates :



T_1 T_2 T_3 T_4

The algorithm is as follows :

- Find a pixel location (i,j) where the pixels in the image match those in template T_1 . With this template all pixels along the top of the image are removed moving from left to right and from top to bottom.
- If the central pixel is not an endpoint and has connectivity number = 1, then mark this pixel for deletion.

    - Endpoint pixel : A pixel is considered an endpoint if it is connected to just one other pixel. That is, if a black pixel has only one black neighbor out of the eight possible neighbors.

    - Connectivity number : It is a measure of how many objects are connected with a particular pixel.

$$Cn = \sum_{k\in S} N_k - (N_k \,.\, N_{k+1} \,.\, N_{k+2})$$

Where N_k is the color of the eight neighbors of the pixel analyzed. N_0 is the center pixel and the rest are numbered in counterclockwise order around the center.

S = {1,3,5,7}

In segmentation the image is divided into the segments/parts in a grid. The pattern is set for the image. One is set for the black pixel and zero for the white pixel. In translation the image is moved to the center position. Then it scaled to the size. The thinning is as shown in the Fig 4.

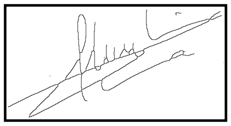
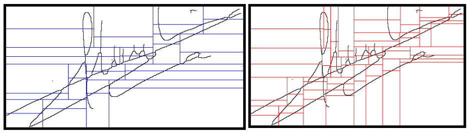


Figure 4: Signature using Stentiford Thinning

- Feature Extraction : In this the features of the image is extracted. The geometric features are based on two sets of points. The image is divided into thirty vertical (v1,v2,v3,….,v30) and the horizontal splitting results thirty points (h1,h2,h3,…...,h30). These feature points are obtained with relative to a central geometric point of the image. Here the centered image is scanned from left to right and calculate the total number of black pixels. Then again from top to bottom and calculate the total number of black pixels. Then divide the image into two halves w.r.t. the no. of black pixels by two lines vertically and horizontally which intersects at a point called the geometric center. The Fig. 5 shows the splitting of the image in vertical and horizontal.

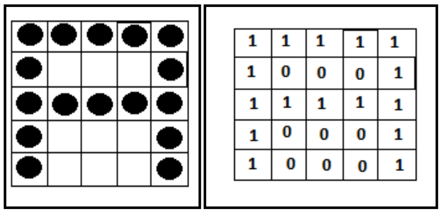
•



(a) (b)

Figure 5: Image divided along (a) X-axis (b)Y-axis

- Pattern Matching : Here the matrix is created. The matrix consists of zeros and ones. Zero represents the pixel is white and one represents the pixel is black. The matrix created is compared with the values of matrix that has been stored in the database. The following figure shows the example of how the image is stored in the matrix form. Here "A" is taken to illustrate.



1	1	1	1	1
1	0	0	0	1
1	1	1	1	1
1	0	0	0	1
1	0	0	0	1

(a) (b)

Figure 6 :(a) Image of the letter A (b) Matrix representation of A

Here the letter A is shown. The pixels that are black in color represents one in the matrix representation and the white pixels represents zero. Like this all the image is converted to the matrix form containing ones and zeros. This matrix is then compared to the matrix that is stored in the database.

- Signature Matching : The signature from the user is taken. The four to five sets of the signature are taken from the user as every time the user can't do the exact signature. Therefore for some deviation it is taken from the user. These sets of signature are stored in the database. Now when the user wants to access to the application, his signature is taken from any means i.e. by taking the photograph or scanning, then it is matched with the set of the signatures that are kept in the database. If matched then allowed to access the application.

3.System Design

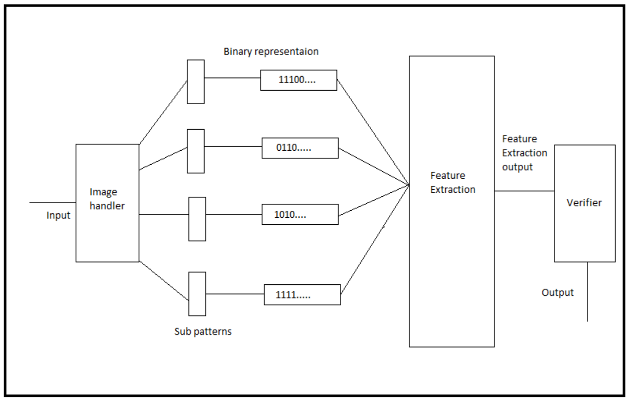


Figure 7

The design starts with the analysis model and architecture as the major inputs. The principal activity of design is to refine the analysis model such that it can be implemented with the components of the architecture.

The operation procedure of present system is very simple especially in manual system. The signature to be verified is scanned, the scanned image will be given to the system. The system will extract pixel values from image, convert into a binary image, and hence to a matrix. This matrix will be converted in to real a valued vector by a sequence of operations based on the features present in the signature, in the training stage the system will produce weight vector from this vector and save it in database. At the verification stage the system repeats the same procedure as above, uses the corresponding saved weight vector as the comparison criteria for verification.

The most important phase of a project from the point of view of an end user is nothing but input/output design. Actually the application communicates with the user through the interfaces. This work also gives a special attention towards the interface design. A self explanatory GUI is adopted.

Input to the system is, scanned JPEG image which contains the signature. As output the system goes to the application if the signature matches.

4.Result

The two signatures are matched with each other to check whether they match or not. The score for each match is given. The highest score indicates that the signature is not matched. The lowest score indicates that the signature is matching approximately. The value of the score is set to 10000.

5.Future Work

There is lot that can be done to extend the functionality of the proposed system. The same design can be used for other pattern recognition algorithms with small modifications. Improving the image extraction process independent of image size and orientation, and including an electronic image reading device to the system interface, the system can be improved as a commercial product. More over the accuracy of the system can be improved further by using digital signing pad and considering pen tip pressure graph on this digital signing pad as a characteristic for verification.

6.Conclusion

In this paper we have discussed an offline signature verification technique using grid based feature extraction. The preprocessed signature is segmented into grid. Matrix corresponding to grid is formed and arrays containing number of black pixels in rows and columns formed. From analysis it has been observed that proposed technique gives better FAR and FFR than existing verification techniques.

7.Refernce

1. Vahid Kiani, Reza Pourreza, Hamid Reza Pourezza, “Offline Signature Verification Using Local Radon Transform and Support Vector Machines”, International Journal of Image Processing(IJIP), Vol.3, No.5, pp.184-194,2010.
2. Dakshina Ranjan Kisku, Phalguni Gupta, Jamuna Kanta Sing, “Offline Signature Identification by Fusion o Multiple Classifiers using Statistical Learning Theory”, Computer Vision and Pattern Recognition, USIA 2010.
3. Mishra, Prabit Kumar and Sahoo, Mukti Ranjan, “Offline Signature Verification Scheme”, 2009.
4. Priyanka Chaurasia, “Offline Signature Verification using High Pressure Regions”, Patent No. US 7,599,582 b1,2009.
5. Meenakshi K. Kalera, Sargur Srihari and Aihua Xu,“ Offline Signature Verification and Identification using Distance Statistics”, International Journal of Pattern Recognition and Artificial Intelligence, Vol.18, No.7, pp.1339-1360, 2004.
6. Banshider Majhi, Y Santhosh Reddy, D Prasanna Babu, ‘‘Novel Features for Offline Signature Verification’’ ,International Journal of Computers,Communications & Control, Vol. I, No. 1, pp. 17-24, 2006.
7. Banshidhar Majhi, Y. Santhosh Reddy and D. Prasanna Babu, 2006. Novel features for offline signature verification. Int. J. Comput. Commun Control, 1: 17-24. http://www.journal.univagora.ro/download/pdf/20.pdf.
8. Edson, J., R. Justino, A. El Yacoubi, F. Bortolozzi and R. Sabourin, 2000. An off-line Signature Verification System Using HMM and Graphometric features. DAS, pp: 211-222.http://www.livia.etsmtl.ca/publications/2000/JustinoDAS.pdf.
9. Menezes, Alfred; Paul C. van Oorschot; Scott A. Vanstone (October 1996). Handbook of Applied Cryptography. CRC Press. ISBN 0-8493-8523-7.
10. Cormen, Thomas H.; Charles E. Leiserson; Ronald L. Rivest; Clifford Stein (2001). Introduction to Algorithms (2e ed.). MIT Press and McGraw-Hill. pp. 881–887. ISBN 0-262-03293-7.
11. Plamondon.R., Brault J.J., 'A Complexity Measure of Handwritten curves: Modeling of Dynamic Signature Forgery', IEEE Trans. on Systems, Man and Cybernetics, Vol.23, No.2, 1993, pp. 400-413.

12. P.Salembier, A.Oliveras, and L.Garrido, “Anti-extensive connected operators for image and sequence processing”, IEEE Trans. Image Proc. 7(4), pp. 555-570, 1998.