Volume-3, Issue-10, Oct-2014 • ISSN No 2277 - 8160

Research Paper Education

An Analysis of Offline Signature Verification System

G. Precilla Jansi Rani

Research Scholar Mother Teresa Women's University Kodaikanal.

ABSTRACT

In this high-tech era of growing e-society, the forgery detection has been a challenging area of Biometrics. The actions made by any individual can be utilized as an identification mark. Some of the metrics are handwritten signature, voice, etc., will be included in Behavioral Biometrics. Physiological Biometrics, which means the appearance of a person, will be used to identify a particular person such as Iris, Face, Gait and Fingerprints were used. For the human identification process, Signature Verification is most frequently used even before the invention of the computers. Signature Verification System hereinafter called SVS is categorized by two approaches. Online/ Dynamic approach uses digitized devices which can be produced dynamic information like Pressure, Velocity, etc., whereas in Offline/ Static Signature Verification approach, it uses the written signature of a person by using pen and paper. This paper presents a survey of related researches for various offline SVSs.

KEYWORDS : Signature Verification, Pattern Matching, FAR, FRR

INTRODUCTION

Handwritten Signature is the most popular biometrics for person identification. In SVS, the signature would be captured as an image by using a scanner in order to obtain a digitized image that would be represented by the M x N pixels. That signature image is the input for the system. The aim of the SVS is to find out whether the given signature is original or a forged one. Unlike Online/Dynamic SVS, the Offline SVS has to work a lot to find out the genuinity of the system due to the lack of the dynamic information. It is a challenging issue of the Offline SVS. The signature of a person has normally two types of variation- Intrapersonal defines the differentiation between the same person's signatures due to age, illness, time and abnormal conditions and but Interpersonal defines the differentiation between the original and forgery of the given signature.

FORGERY

Signature forgery has been defined as an attempt to copy some one's signature and use that against that person to get his/her identity.

Generally forgery can be classified into 3 types.

- Random Forgery: This type of forgery includes the signer will know only the name of the person, whose signature is to be copied and the signer does not know about the signature's shape, style etc.,
- Simple Forgery: The Signer has the information regarding the person's Name, Signature Shape, Style and etc., prior signing.
- Skilled Forgery: In this kind of forgery, the signer will be well trained the person's signature prior signing, with the good practice of the signer. He / She can easily make the signature as an original.

Signature Verification System mainly focusing the signature recognition instead of Character Recognition. Because basically the alphabets of the signature cannot be identified easily and the signature will be appeared as an image with their own styles, which includes curves, lines etc. So the signature image will be considered as a special distribution of pixels. For Signature Recognition, a more flexible and efficient approach is needed. This research work would be able to discover such a method for signature verification.

TYPES OF ERROR RATES

The performance of the SVS can be defined by some of the metrics like False Rejection Rate (FRR) error rates related to the signatures which are genuine, that are rejected by the system. That is the genuine signature is treated as a forged signature. These are called Type I errors., False Acceptance Rate (FAR) error rates related to the signatures which are forged, that would be accepted by the system as an original. That is the forged signature classified as genuine signature. These are called Type II errors. Average Error Rate (AER) defines the average of Type I errors and Type II errors can be calculated by this AER to find out the originality of the given input.

PHASES OF OFFLINE SIGNATURE VERIFICATION SYSTEM

SVS is a Pattern Recognition problem and a typical pattern recognition system has the following phases.

- Data Acquisition
- Preprocessing
- Feature Extraction
- Classification/Verification
- Performance Evaluation

Data Acquisition

Capturing the signature image, which is the input to the system, is the foremost step of SVS. The images of the signatures are scanned using digitized device like scanner. That scanned images are stored digitally for offline processing.

Preprocessing

This phase leads the given signature image to simplify the subsequent operations without losing relevant information which involves Noise Reduction, while scanning an image it might have some noises like image with some less clarity, color differences etc. Using some noise filters like Median Filter can be used to remove those noises for the best result. Resizing is used to resize the given image by cropping it's boundary for worthy look of the signature image. Binarization is a kind of transformation of Color image to Gray Scale image and then it will be transformed into Black and white as Binary image. Thinning as its name like this is used to reduce the thickness of signature to be a thin line as one pixel thick for the feature extraction process. Clutter Removal to use the technique of masking if there are any isolated black dots those will be removed before the processing. Skeletonization is used to select the foreground pixels of the signature image representing the signature pattern by a collecting of curves and arcs.

Feature Extraction

By reducing the given data to measure some features or properties is called Feature Extraction. A perfect feature extraction, extracts a minimal feature set that maximizes interpersonal distance between the signature examples of various person, while minimizing intrapersonal distance for those belonging to the same person. Feature Extraction is categorized into three ways based on Global, Local and Geometric/ Transition Features.

Global Features: It is used to describe the signature image as a whole and the features are extracted from all the pixels confining the signature image. In global featuring, different types of features are available like, Signature Area, Aspect Ratio, Maximum Horizontal Histogram, Maximum Vertical Histogram, Edge Point numbers, Horizontal and Vertical Center, Signature Height, Image Area, Pure Height, Pure Width, Vertical Projection Peak, Horizontal Projection Peak, Global Slant Angle, Local Slant Angle, Number of Cross Points, Number of Edge Points and Centre of Gravity:

Local Features: The signed image will be splited into partitions by some geometric processes. These are categorized into two broad ways. Contextual Local Features which means if the partition of a signature interprets a text is called contextual and Non-Contextual Local Features for if the partition of a signature image leads to be a drawing is called non-contextual.

Geometric/Transition Features: The geometry and topology of a signature image is known as these kinds of features and it is used to preserve the local and global properties such as Ability to tolerate with Distortion, Style Variation, Rotational Variation and Degree of Translation.

Classification/Verification

This phase classifies and labels the features obtained from the feature extraction and makes a final decision for classification. SVS classification can be invoked by Template Matching Approach, Statistical Approach, Structural/Syntactic Approach, Spectrum Analysis Approach and Neural Network Approach

Performance Evaluation

The performance evaluation is done by measuring the accuracy of a method or in other words by measuring the FRR, FAR and AER.

Various Offline SVS Approaches

Initially SVS used for the verification by using Templates. Template is a collection of signature images which can be tested against the given image as original or forged one. This kind of approach is the easiest method for pattern recognition. It is used to detect the Casual/Simple forgeries from genuine signatures successfully. But it is not well suited for skilled forgeries. Pattern Recognition/ Template Matching system was implemented by so many researchers.

Fang et al [1] proposed two methods to identify the skilled forgeries with the help of template. First method is entirely based on the one dimensional optimal matching of the signature patterns and the second one is for two dimensional signature patterns.

Dr. Daramola Samuel [2] proposed a SVS, which has chosen 100 original and 200 forged signature as Template. It has divided the test signature's image into 64 cells based on center of gravity. The entire system used three feature vectors as Image Cell size (F1), Image Center angle relative to the cell lower right corner (F2) and Pixels normalized angle relative to the lower right corner (F3). In Training stage, the system calculated a threshold value for each F1, F2 and F3 feature vectors. As well in Classification stage, Euclidean Distance has been used for testing the signature originality with the template. If the calculated distance value is lesser than the threshold value means, the given input is an original, a forged one if not. The FAR rate is 1% and FRR is 0.5%.

Ibrahim S.I. Abuhaiba [3] developed a SVS which has taken the image's raw binary pixel intensities. Signature verification used as Graph Matching problem by the Hungarian Method. This system has taken several subjects for Testing. For the genuine signature verification Genuine Test has been used. To treat the entire genuine signature as random forgeries, there is a test called Random Forgery Test. To test the skilled forged signatures, as well skilled forgery test is available. This system has ERR as 26.7% for skilled forgeries and 5.6% for Random forgery which is achieved by 32x64 pixels.

Sepideh Afsardoost [4] proposed a verification system which used Geometric center feature for Vertical, Horizontal and Diagonal splitting of image. It used six center points for both vertical splitting and horizontal splitting and 8 center points used for diagonal splitting. Totally 20 center points has been used to authenticate the signatures. However diagonal splitting is too complicated and it should be well trained with normalization. In training stage with the threshold value, this stage will be used to compare the threshold value of the trained signature of templates with the threshold value of the incoming signatures. If the incoming threshold value is lesser than the trained signature's threshold that can be treated as an original, it will be rejected if not. In classification stage, it used statistical approach like variance, standard deviation. The FAR rate is 10% and FRR is 15%.

H. Baltzakis and N. Papamarkos [5] developed a system by using Global, grid and texture features. This system has a special two stage Perceptron OCON (One Class One Network) classification structure. The first stage, the results of the Neural Network and Euclidean Distance will be taken as input of the classifier. The output of the first stage will be given as the input to the second stage with radial base function (RBF) neural network structure for the final decision. The FAR rate is 9.81% and the FRR rate is 3%.

Ramachandra C. Jyothi et.al [6] proposed a system for offline signature verification. It used only the Global features like Maximum Horizontal and Vertical Histogram, Horizontal and Vertical centers of signatures, Aspect Ratio, Edge Points of the signature. Total of 315 genuine and 210 forged signatures were taken to the process. This system has been developed by using Euclidean Distance. The evaluated FRR is 5.4% and FAR is 4.6%.

Abhay Bansal et.al [8] proposed a method for this offline signature authentication. This system was proposed by 1. Pattern Matching, especially Pattern Matching is triangle matching with K_d Ratio, 2. Area Matching with the threshold value, 3. Point Matching by Graph Matching. The FAR rate is 0.08% and for Simple forgery FRR is 13.02%. For skilled forgery the FRR is 2.64%.

J.B. Fasquel and Brugnooghe [9] proposed an offline verification system with the combination of some statistical classifiers. This system consists of three steps. 1. It is used transforming the original signature using the identity and 4 Gabor transformations. 2. To inter-correlate the analyzed signature with the similarly transformed signatures in the database. 3. Finally, the authentication of the signatures would be performed by fusing the decisions, which are obtained by each transform. The FRR rate is 62.4%.

Sharifah Mumtazah and Syed Ahmad et.al [10] developed another handwritten verification system with some statistical techniques. The Hidden Markov Modeling (HMM) has been used for developing a reference model for each local feature. Three layers of statistical techniques were used. In the first layer, matching score will be calculated based on the HMM. In the second layer by using the z-score analysis and normalization function, the calculated score will be used for mapping into the boundary ranges of acceptance or rejection. Then in the third layer Bayesian inference technique has been used to decide the acceptance or rejection. For random forgeries the FAR rate is 22% and for skilled forgeries the FAR rate is 37%.

COMPARISON OF THESE TECHNIQUES

S.No	Year	Author	Journal	Techniques	Features used	FRR	FAR	AER
1.	2000	Fang et al []	Pattern Recognition	Index Based Approach for Pattern Matching by statistical techniques	Binary & Grey-level images were used.			18.1%
2.	2010	Dr.Daramola Samuel,Ibiyemi Samuel	International journal of Engineering Science and Technology	Euclidean Distance	Image Cell size (F1),Image Center angle relative to the cell lower right corner (F2) Pixels normalized angle relative to the lower right corner (F3).	0.5%	1%	

S.No	Year	Author	Journal	Techniques	Features used	FRR	FAR	AER
3.	2007	Ibrahim S.I. Abuhaiba []	Turk Journal of Elec. Engineering	Signature verification used as Graph Matching problem by the Hungarian Method.				
4.	2008	Sepideh Afsardoost et.al	ICSP	Statistical approaches like Variance, Standard Deviation	Geometric center feature for Vertical, Horizontal and Diagonal splitting of image	15%	10%	
5.	2001	H.Baltzakis N.Papamarkos []	Engineering Applications of Artificial Intelligence	Neural Network and Euclidean Distance	Perceptron OCON (One Class One Network) classification structure	3%	9.81%	
6.	2009	Ramachandra C. Jyothi et.al []	International Advance Computing Conference	Euclidean Distance	Global features like Maximum Horizontal and Vertical Histogram, Horizontal and Vertical centers of signatures, Aspect Ratio, Edge Points of the signature.	5.4%	4.6%	
7.	2008	Abhay Bansal et.al []	First International Conference on Emerging Trends in Engineering and Technology	Pattern Matching, Area Matching and Point Matching	Triangle matching with K_d Ratio, Area Matching with the threshold value, Point Matching by Graph Matching.	Simple: 13.02% Skilled: 2.64%.	0.08%	
8.	2004	J.B. Fasquel and Brugnooghe []	International Journal on Document Analysis and Recognition	Used the combination of some statistical classifiers	1. Transforming the original signature using the identity and 4 Gabor transformations. 2. To inter-correlate the analyzed signature with signatures in the database. 3. Authentication by fusing the decisions, obtained by each transform.	62.4%.		
9.	2009	Sharifah Mumtazah and Syed Ahmad et.al []	World Congress on Computer Science and Information Engineering	Hidden Markov Modeling (HMM) and statistical techniques			Random: 22% Skilled: 37%	

Conclusion

In this e-society, Signature Verification System is used to authenticate the human handwritten signature for testing the signature whether it is an original or a forged one. The above table illustrated an analysis of some techniques which are existed to implement the signature verification system. This paper has focused to find out various approaches which were developed so many Signature verification systems in various aspects.

REFERENCES

[1]. B. Fang,C.H.Leung,Y.Y. Tang, K.W.Tse, P.C.K. Kwok and Y.K. Wong,"Offline Signature verification by the Tracking of feature and stroke positions," Pattern Recognition, vol. 36, pp. 101,2003. | [2]. Daramola Samuel and Prof. Ibiyemi Samuel, "Novel feature extraction technique for offline signature verification system," International Journal of Engineering Science and Technology, vol ED-2(7), pp.3143, 2010. | [3]. Ibrahim S.I Abuhaiba, "Offline Signature Verification using Graph Matiching", Turk J Elec Engin, Vol 15, no. 1, pp. 89-104,2007. | [4]. Sepideh Afsardoost, Siamak Yousefi and Mohammed Ali Khorshidi, "Offline Signature Verification Using Geometric Center Features", ICSP, pp. 1491-1494, 2008. | [5]. Baltzakis H and papamarkos N 2001. A New signature verification technique based on a two-staged neural network classifier. Engineering Applications of Artificial Intelligence 14(2001) (pp 95-103). | [6]. Ramachandra A C, Pavithra K, Yashavini K, Raja K B, Venugopl K R and Patnaik L M. 2008. Cross-validation for Graph matching based offline signature verification. India Conference INDICON 2008 | [7]. Ramachandra C, Pavithra K, Jyothi Srinivasa Rao, Raja K B, Venugopl K R and Patnaik L M. 2009. "Robust offline signature verification based on Global features", International Advance Computing Confernece(IACC 209),IEEE, March 2009. | [8]. Abhay Bansal, Divye Garg and Anand Gupta, "A Pattern Matching Classifier for offline Signature verification", First International conference on emerging Trends in Engineering and Technology, 2008. | [9]. J. B. Fasquel and M. Bruynooghe. 2004. A hybrid opto- electronic method for fast off-line handwritten signature verification. International Journal on Document Analysis and Recognition (2004) | [10]. Ahmad S M S, Shakil A, Faudzi M A, Anwar R M and Balbed M A M. 2009. A Hybrid Statistical Modeling, Normalization and Inferencing Techniques of an Off-line Signature Verification System. 2009 World Congress on Computer Science and Information Engineering |