

Signature Verification using Graph Matching and Cross-Validation Principle

Ramachandra A C¹, Ravi J², K B Raja³, Venugopal K R³ and L M Patnaik⁴

¹Alpha College of Engineering, Bangalore 562149, India

²Global Academy of Technology, Bangalore 560098, India

³University Visvesvaraya College of Engineering, Bangalore University, Bangalore 560 001, India

⁴Vice Chancellor, Defence Institute of Advanced Technology, Pune, India

ramachandra.ace@gmail.com

Abstract

Identification of a person depending on his physiological or behavioral characteristics is done using Biometric System. Signature verification is a commonly used biometric method and is widely used for financial transactions. In this paper, we propose Signature Verification using Graph Matching and Cross-Validation Principle (SVGMC) algorithm. Pre-processing is carried out to extract signature feature to obtain high resolution for smaller normalization box. The identical measure between two signatures in the database is determined by (i) Bipartite graph G , (ii) Complete matching in G and (iii) Minimum Euclidean distance. An optimum threshold value is determined using Cross-validation technique to select reference signatures. Pre-processing is performed on the given signature to extract test feature. Then the test feature is compared with the threshold value to verify the test signature. Better Equal Error Rate (EER) is obtained for skilled and random forgeries.

Keywords: Biometrics, Offline Signature Verification, Bipartite graph, Complete Matching, Cross-Validation, Equal Error Rate.

I. INTRODUCTION

Within the field of human identification, the usage of biometrics is growing because of its unique properties such as hand geometry, iris scanning, fingerprint and DNA analysis. The verifications are necessary for many routine activities such as boarding an aircraft, crossing international borders and entering a secure physical location. The higher levels of security and easier interactions to the end user are provided by biometrics for identity verification. The biometrics verifies the person based on feature vectors derived from physiological or behavioral characteristics. Any physiological or behavioral characteristics should possess the following characteristics to serve as a biometric: *Uniqueness, Permanence, Acceptability, Collectability* and *the minimum cost to employ these biometrics*. Physiological biometric measures some physical feature of a person such as face, fingerprint, iris, ear, palm print, retina, DNA, hand and finger geometry. Behavioral biometric measures the action of a person such as speaking, writing. Few physical features remain relatively stable over time, while behavioral characteristics tend to change over time due to health, psychological state and aging. The person can often create false negatives hiding his true identity by consciously changing the behavior. The behavioral biometrics are collected from a cooperative person. Physiological biometrics may be represented by a single

sample, whereas behavioral biometric generally requires several samples due to their variability.

Signature verification can be divided into two groups On-line and Off-line. On-line signature verification involves more electronic [1] equipment and it uses signatures captured by pressure-sensitive tablets that extract dynamic properties of a signature in addition to its shape. Dynamic features include the number and order of strokes, the overall speed of the signature, the pen pressure at each point etc. and make the signature more unique and more difficult to forge. Off-line signature verification involves less electronic equipment and the features for off-line verification are much simpler. In this only the pixel image can be evaluated. As compared to on-line signature verification systems, off-line systems are difficult to design as many desirable characteristics such as the order of strokes, the velocity and other dynamic information are not available in the off-line case. The verification process has to wholly rely on the features that can be extracted from the trace of the static signature images only. Although difficult to design, off-line signature verification is crucial for determining the writer identification as most of the financial transactions in present times are still carried out on paper. Therefore, it becomes all the more essential to verify a signature for its authenticity. The design of any offline signature verification system generally requires the solution of five sub problems: data acquisition, pre-processing, feature extraction, comparison process and performance evolution. For achieving this one could either trace or imitate the signature by hard way. The non-intrusive characteristics of signature make it the *de facto* standard for identification and verification of a person. The signature biometrics varies depending on fatigue, mental state and ergonomics. An efficient verification system shall be able to detect forgeries and reduce the rejection of genuine signatures. The two different types of forgeries considered for signature verification are Random forgeries and Skilled forgeries. The problem of signature verification is difficult for skilled forgeries compared with random forgeries.

Contribution: In this paper, we propose SVGMC algorithm in which we use two concepts viz., Graph matching and Cross-validation for signature verification. The signature extraction method is used in pre-processing to obtain high resolution of signature for smaller normalization box. The signatures are compared by

constructing a bipartite graph from which a minimum cost complete matching is obtained and the measure of dissimilarity i.e., the Euclidean distance is determined. Cross-validation principle is used to solve the problem of selection of reference signatures, which derives the best reference set of signatures for the system producing optimal decision threshold value.

II. RELATED WORK

Quan and Liu [2] proposed an online signature verification system based on hidden markov model/artificial neural network hybrid model. The model is constructed by using a time delay neural networks as local probability estimators for hidden markov model, where a posterior probability of the model is worked out by the Viterbi algorithm. The use of artificial neural network as probability estimators accounts for the contextual information. Alisher and Yanikoglu [3] presented an online signature verification system with improved decision criterion using multiple, normalized distance values between test and reference signatures as features. They used three different classifiers such as bayes classifier, support vector machines, and a linear classifier in conjunction with principal component analysis. They obtained the lowest average equal error rate values when tested with skilled forgeries.

Feng and Wah [4] proposed an extreme point warping technique for the functional approach in signature verification instead of dynamic time warping. This method warps a set of selective points i.e., the extreme points on the signal rather than the whole signal. This preserves the local curvatures between the extreme points, which prevent forged signals taking advantage from the warping process. Jonas and Drygajlo [5] introduced the use of gaussian mixture models for on-line signature verification. The individual gaussian components represent local signer-dependent features that characterize spatial and temporal aspects of a signature

and are effective for modeling its specificity. This work focuses on an automated order selection for signature models based on the minimum description length principle. Algorithm is compared with hidden markov models. Shafiei and Rabiee [6] presented an on-line handwritten signature verification system using hidden markov model. The signature is segmented based on its perceptually important points and a number of features that are scale and displacement invariant are then computed for each segment. The sequence of features is used for training to achieve signature verification.

III. MODEL

In this section, Block diagram of SVGMC are discussed.

Block diagram of SVGMC:

Figure1 gives the block diagram of Signature Verification using Graph Matching and Cross-Validation Principle (SVGMC) system.

Signature database: The signature samples are collected from website as well as scanned on A4 sheet with the grid size of 6.3 cm * 4.5 cm using *hp Scan Jet 3400C* scanner at *300dpi resolution*. Database consists of genuine signatures only.

Pre-processing: The principal objective of pre processing is to obtain a transformed image with enhanced quality. It includes i. Noise removal, ii. Rotation, iii. Smoothing, iv. Thinning, v. Signature extraction and vi. Normalization.

i. *Noise removal:* Noise removal is required to eliminate the pixels that are not part of the signature, but contained in the image. Generally signature image consists of salt and pepper noise, which is removed using median filter

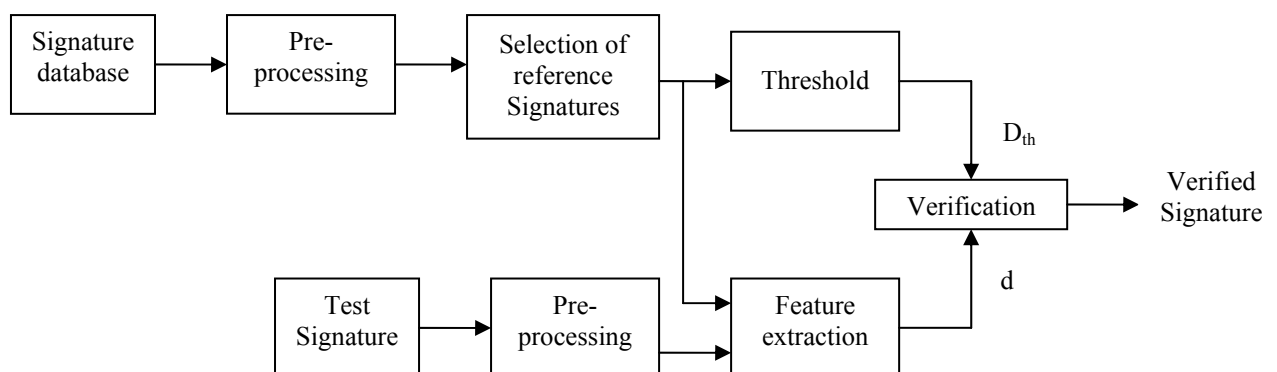


Figure. 1: Block diagram of SVGMC system.

ii. *Rotation:* Rotation of a signature is necessary as time domain approaches are sensitive to angle variations

compared to frequency domain approaches. It coincides the axis of mass of inertia of all the signatures to the same horizontal axis. The edge of the signature is first detected

using Canny edge detector to which Radon transform is applied and the angle of rotation is measured in anticlockwise direction. The edge is skeletonized to preserve pixel connectivity before applying Radon transformation. The signature is then rotated clockwise to remove skewness.

iii. *Smoothing*: Smoothing is performed to remove Additive White Gaussian Noise from signature and to expose its features for further processing. The adaptive filter, which preserves edges and high frequency components of the signature, is used for smoothing.

iv. *Thinning*: Thinning is a morphological process necessary for the reduction of data and computational time. A fast parallel Zhang-Suen algorithm is used as it preserves pixel connectivity and end points, which is necessary for graph matching based signature verification system. It consists of two sub-iterations: one aimed at deleting the south-east boundary points and the north-west corner points while the other one is aimed at deleting the north-west boundary points and the south-east corner points. It reduces the signature to a skeleton of unitary thickness.

v. *Signature extraction*: Extract the smallest box that covers the signature so that the extra background created due to rotation is removed. The smallest box is determined by the height and width of the signature and is then cropped to the measured dimension. The allowance for little background is given in all directions so that the signatures do not touch the boundary of the box.

vi. *Normalization*: Normalization is required to standardize the size of signatures having interpersonal and intrapersonal differences.

Selection of Reference Signatures: The Cross-Validation principle decides the validity of the genuine signature to be in the reference set by comparing it with other genuine signatures. The genuine dataset of signatures S_1, S_2, S_m are considered and the Euclidean distances between one genuine signature and the remaining genuine signatures are determined forming a distance vector say DV_1 . Similarly, the distance vectors DV_2, DV_3, \dots, DV_m are determined for signatures S_2, S_3, \dots, S_m . The ratio of mean to standard deviation SD of each distance vector is determined and considered as the respective decision factor as given in Equations (1), (2) and (3)

$$\text{Decision factor of } S_1(DF_1) = \frac{\text{Mean}(DV_1)}{\text{SD}(DV_1)} \dots\dots\dots (1)$$

$$\text{Decision factor of } S_2(DF_2) = \frac{\text{Mean}(DV_2)}{\text{SD}(DV_2)} \dots\dots\dots (2)$$

$$\text{Decision factor of } S_m(DF_m) = \frac{\text{Mean}(DV_m)}{\text{SD}(DV_m)} \dots\dots\dots (3)$$

The average of all decision factors is determined as given in an Equation (4)

$$DF_{avg} = \frac{DF_1 + DF_2 + \dots + DF_m}{m} \dots\dots\dots (4)$$

Compare DF of each signature with DF_{avg} and the signatures whose DF 's are approximately equal to DF_{avg} are chosen as reference. The average value of decision factor is considered in order to provide trade off between the maximum value of decision factor, which increases acceptance of forgeries FAR and the minimum value of decision factor, which increases rejection of genuine signatures FRR . The systematic selection of reference set results in reduced error rate.

Threshold: Consider a set of n reference signatures say RS_1, RS_2, \dots, RS_n . The dissimilarity measure i.e., the Euclidean distance ED_1 between any two signatures say RS_1 and RS_2 is determined if

$$\rho_{min} \leq 0.9 * \rho_{max}$$

where ρ_{min} and ρ_{max} are the minimum and maximum pixel densities of RS_1 and RS_2 respectively else the pair is not considered for determining the distance. Similarly, the Euclidean distances $ED_2, ED_3, \dots, ED_\alpha$ for all possible pair of signatures are determined. For n reference signatures, the number of Euclidean distances α is given by Equation (5)

$$\alpha = {}^n C_2 - m = \frac{n!}{(n-2)! * 2!} - m \dots\dots\dots (5)$$

Where m is the number of signature pairs ignored. The maximum Euclidean distance is considered as the threshold value D_{th} as given in Equation (6)

$$D_{th} = \max(ED_1, ED_2, \dots, ED_\alpha) \dots\dots\dots (6)$$

Feature extraction: The test signature say TS is pre-processed and the dissimilarity value i.e., the Euclidean distance say d_1 between TS and the reference signature RS_1 is determined if

$$\rho'_{min} \leq 0.9 * \rho'_{max}$$

where ρ'_{min} and ρ'_{max} are the minimum and maximum pixel densities of TS and RS_1 respectively else the dissimilarity measure d_1 is taken as infinity. Similarly, Euclidean distance from TS to all other reference signatures say d_2, d_3, \dots, d_n is determined. The minimum distance obtained is considered as the test feature d for TS as given in Equation (7)

$$d = \min(d_1, d_2, \dots, d_n) \dots\dots\dots (7)$$

Verification: The extracted feature of test signature d is compared with the threshold value D_{th} . If d is less than or equal to D_{th} , then the test signature is accepted as genuine else it is rejected as forgery.

IV. ALGORITHM: SVGMC SYSTEM

Table 1 gives algorithm for SVGMC system in which Cross-validation principle is used to select reference set of signatures and the Euclidean distance is considered as the dissimilarity measure between any two signatures.

Problem definition: Given test signature and large signature database, the objective is to verify the authenticity of the test signature by comparing with the database using SVGMC algorithm.

TABLE 1: SVGMC Algorithm.

- *Input:* Test signature, genuine signature database.
- *Output:* Verified signature.
 - i. Pre-processing of given signature database.
 - ii. Selection of reference set of signatures from pre-processed database using Cross-Validation principle.
 - iii. The maximum dissimilarity measure obtained by comparing reference signatures with one another is considered as the decision threshold value D_{th} .
 - iv. Test signature is pre-processed.
 - v. The pre-processed test signature is compared with each of the reference signatures and respective dissimilarity values are calculated using Hungarian method.
 - vi. The minimum dissimilarity value is considered as the test feature d .
 - vii. If $d \leq D_{th}$, then the given test signature is accepted as *genuine* else it is rejected as *forgery*.

V. PERFORMANCE ANALYSIS

For performance analysis signature database of five persons are considered and for each person 24 genuine signatures and 30 skilled forgeries are considered. The three tests performed are as follows:

Genuine test: Genuine signatures are verified against reference signatures to compute False Rejection Rate *FRR*. Out of available 24 genuine signatures of one person, 3 are selected as reference and remaining 21 are used for testing. Therefore, the total number of test signatures equals $21 * 5 = 105$. *FRR* is computed as the percentage of the ratio of number of genuine signatures rejected to the total number of test signatures.

Skilled forgery test: Skilled forgeries are verified against reference signatures to compute False Acceptance Rate *FAR-S*. All the 30 skilled forgeries of a person are tested yielding a total of $30 * 5 = 150$ test signatures. *FAR-S* is computed as the percentage of the ratio of number of skilled forgeries accepted to the total number of test signatures.

Random forgery test: For any individual the genuine signatures of others are considered as random forgeries. Random forgeries are tested to compute False Acceptance

Rate *FAR-R*. The total number of test signatures is $24 * (5-1) * 5 = 480$. *FAR-R* is calculated as the percentage of the ratio of number of random forgeries accepted to the total number of test signatures. These tests are performed using different sizes of normalization box: $8 * 16$, $16 * 32$, $24 * 48$, $32 * 64$, $40 * 80$ and $48 * 96$. For every specific normalization box decision threshold value is varied using a Rejection Constancy Factor *RCF* as given in Equation (8)

$$D_{max} = D_{th} * RCF \dots\dots\dots (8)$$

where *RCF* determines the maximum threshold value. A graph of Error rates (*FAR-S* and *FAR-R*) versus *RCF* is plotted and Equal Error Rate for both skilled *EER-S* and random *EER-R* forgeries are determined for each normalization box. *EER-S* and *EER-R* are plotted against different sizes of normalization box as shown in Figure 2. *EER-S* and *EER-R* are tabulated and our algorithm SVGMC is compared with the existing algorithm, Offline Signature Verification using Graph Matching (OSVGM) as shown in Table 2 and 3 respectively.

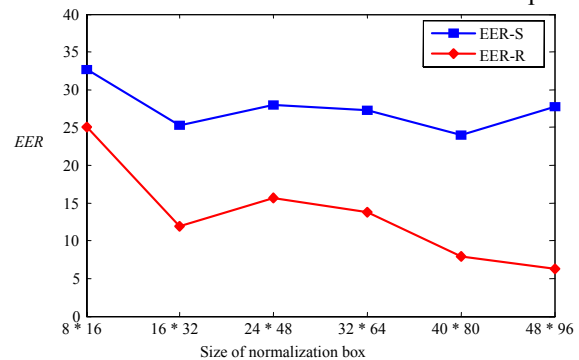


Figure. 2: Equal Error Rate *EER* against different sizes of normalization box.

TABLE 2: COMPARISON OF *EER* OF SKILLED FORGERIS OF SVGMC WITH OSVGM.

Normalization box	OSVGM	SVGMC
8 * 16	37.5	32.67
16 * 32	35.2	25.33
24 * 48	35.0	28.0
32 * 64	29.0	27.33
40 * 80	29.8	24.0

TABLE 3: COMPARISON OF *EER* OF RANDOM FORGERIS OF SVGMC WITH OSVGM.

Normalization box	OSVGM	SVGMC
8 * 16	28.0	25.0
16 * 32	18.5	11.88
24 * 48	20.0	15.63
32 * 64	15.3	13.75
40 * 80	9.0	7.917

VI. CONCLUSION

Signature verification is a widely used behavioral biometric method. In this paper, we propose SVGMC algorithm in which the signatures are checked for identity using Graph matching and the Euclidean distance. The Cross-validation is used to select the reference set of signatures. Pre-processing is done with signature extraction to reduce Equal Error rate *EER*. It is observed *EER* value is reduced compared to the existing algorithm.

REFERENCE

- [1] Shih-Yin Ooi, Andrew Beng-Jin Toeh and Thian-Song Ong. "Offline Verification Through Biometric Strengthening," *workshop on Automatic Identification Advanced Technologies*, pp.226-231, June 2007.
- [2] Z. Quan and K. Liu, "Online Signature Verification based on the Hybrid HMM/ANN model," *International Journal of Computer Science and Network Security*, vol. 7, pp. 313-322, March 2007.
- [3] Kholmatov and B. Yanikoglu, "Identity Authentication using Improved On-line Signature Verification method," *Pattern Recognition Letters*, vol. 26, pp. 2400-2408, November 2005.
- [4] H. Feng and C. C. Wah, "Online Signature Verification using a new Extreme Points Warping technique," *Pattern Recognition Letters*, vol. 24, pp. 2943-2951, May 2003.
- [5] J. Richiardi and A. Drygajlo, "Gaussian Mixture Models for On-line Signature Verification," *Proceedings of International Conference on Multimedia, ACM SIGMM Workshop on Biometrics Methods and Applications*, pp. 115-122, November 2003.
- [6] M. M. Shafiei and H. R. Rabiee, "A New On-line Signature Verification Algorithm using Variable Length Segmentation and Hidden Markov Models," *Proceedings of the Seventh International Conference on Document Analysis and Recognition*, vol. 1, pp. 443-446, August 2003.



Mr. Ramachandra. A. C is an Assistant Professor in the Department of Electronics and communication Engineering, Alpha college of Engineering, Bangalore. He obtained his B.E. degree in Electronics and communication Engineering from Bangalore University. His specialization in Master degree was Electronics and Communication from Bangalore

University and currently he is pursuing Ph.D. in the area of Image Processing under the guidance of Dr. K. B. Raja, Assistant Professor, Department of Electronics and Communication Engineering, University Visvesvaraya college of Engineering, Bangalore. His area of interest is in the field of Signal Processing and Communication Engineering.



Mr. Ravi.J. is an Assistant Professor in the department of Electronics and Communication Engineering, Global Academy of Technology, Bangalore. He obtained his B.E. Degree in Instrumentation Technology from Bangalore University, Bangalore. His specialization in Master degree was Digital Electronics from Visvesvaraya Technological University, Belgaum. He is

pursuing Ph.D. in the area of Biometric applications. His area of interest is in the field of Digital Image Processing.



K B Raja is an Assistant Professor, Dept. of Electronics and Communication Engg, University Visvesvaraya college of Engg, Bangalore University, Bangalore. He obtained his Bachelor of Engineering and Master of Engineering in Electronics and Communication Engineering from University Visvesvaraya College of Engineering, Bangalore. He was awarded

Ph.D. in Computer Science and Engineering from Bangalore University. He has over 35 research publications in refereed International Journals and Conference Proceedings. His research interests include Image Processing, Biometrics, VLSI Signal Processing, computer networks.



K R Venugopal is currently the Principal and Dean, Faculty of Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. He obtained his Bachelor of Engineering from University Visvesvaraya College of Engineering. He received his Masters degree in Computer Science and Automation from Indian

Institute of Science Bangalore. He was awarded Ph.D. in Economics from Bangalore University and Ph.D. in Computer Science from Indian Institute of Technology, Madras. He has a distinguished academic career and has degrees in Electronics, Economics, Law, Business Finance, Public Relations, Communications, Industrial Relations, Computer Science and Journalism. He has authored 27 books on Computer Science and Economics, which include Petrodollar and the World Economy, C Aptitude, Mastering C, Microprocessor Programming, Mastering C++ etc. He has been serving as the Professor and Chairman, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. During his three decades of service at UVCE he has over 200 research papers to his credit. His research interests include computer networks, parallel and distributed systems, digital signal processing and data mining.



L M Patnaik is a Vice Chancellor, Defence Institute of Advanced Technology (Deemed University), Pune, India. During the past 35 years of his service at the Indian Institute of Science, Bangalore. He has over 500 research publications in refereed International Journals and Conference Proceedings. He is a Fellow of all the four leading Science and Engineering Academies in India;

Fellow of the IEEE and the Academy of Science for the Developing World. He has received twenty national and international awards; notable among them is the IEEE Technical Achievement Award for his significant contributions to high performance computing and soft computing. His areas of research interest have been parallel and distributed computing, mobile computing, CAD for VLSI circuits, soft computing, and computational neuroscience.