ISSN : 2278 – 1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2012

Performance of Signature Analysis Using Secure Sketch Method and Neural Network Approach

Vidya Kulkarni[1], S. S. Apte[2], Bhagyashri Wali[3]

GogteInstitute of Technology, Belgaum,Karnataka

ABSTRACT - ***This paper presents the Performance of signature analysis using Secure Sketch method and Neural Network approach. Here secure sketch method is suggested [1] which is developed to generate hash values from handwritten data. Individual hash values will be generated by using secure sketch and neural network approach. Performance of the Neural Network (PNN) is higher compared to the secure sketch method based on the collision and acceptance criterions.***

Keywords - Secure sketch, Probabilistic Neural Network(PNN), Hash functions, quantization.

I. INTRODUCTION

Many resent researches have been done in the field of biometrics. An important part of it is generating an individual and stable hash values .One problem of generation of these hashes lies in the varying biometric data of the same person, called as intra-class variation.Another problem is the inter-class similarity, which describes similar biometric data caused by different individuals.The main aim of biometric hashing is the generation of individual and stable hash values for a person.

Deriving individual keys from biometric information is one of the applications for biometric hashes in cryptographic systems. The hash generation object is based on a body part (E.g. fingerprint, iris) or on behavior(e.g. handwriting, voice) of a person.

The signature is widely used as a means of personal verification. Verification can be performedeither Offline or Online depending on the application. Online systems use dynamicinformation of a signature which is captured while doing the signature. In offline systemsthe scanned images of a signature are used and work will be performed on them.Some of the featuresextracted from these signatures are Baseline Slant Angle, Aspect Ratio, and Normalized

Area, Center of Gravity, number of edgepoints, number of cross points, and the Slope of the line joining the Centers of Gravity oftwo halves of a signature image. Before extracting the features, preprocessing [8] of ascanned image has to be performed to isolate the signature part and to remove any spurious noisepresent in it.

The system is trained initially using a database of signatures obtained from thoseindividuals whose signatures have to be authenticated by the system. For each subject amean signature is obtained by integrating the above features derived from a set of his/hergenuine sample signatures. This mean signature acts as a template for verificationagainst a claimed test signature. The details of preprocessing as well as the features depicted aboveare described in the paper below.

Signature Recognition involves a process known as ‘dynamic signature recognition’. Here, the focus is not on the ‘look’ of the signature, but on the behavioral patterns inherent to the process of signing. This includes changes in timing, pressure, and speed. It is straightforward to duplicate the visual appearance of a signature andvery difficult to duplicate behavioral characteristics.

This paper is structured as follows: The next section describes the previous work of other authors. The third section explains the secure sketch generation approach in which preprocessing and feature extraction is also introduced. The fourth section describesthe evaluation of the performance of hash generation using secure sketch as well as the PNN. Finally, the fifth sectiongives the summary of a paper and an overview of futurework in the field of biometric hashing.

II. PREVIOUS WORK

In [1],“Biometric Hash Generation and User Authentication based on Handwriting using Secure Sketches”,the authors T. Scheidat, C. Vielhauer, J.Dittmanndiscussed about BioHash algorithm that was

ISSN : 2278 – 1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2012

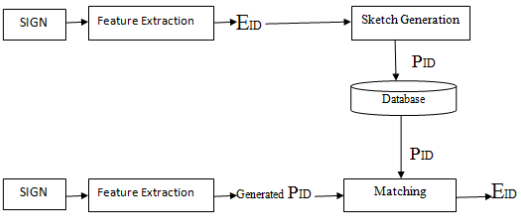
developed to generate unique hashes from dynamic hand written data. They performed sketch generation and feature vector reconstruction by using Secure Sketch algorithm.

Y. Sutcu, Q. Li, and N. Memon, in [2] "Protecting Biometric Templates with Sketch: Theory and Practice" have studied that how secure sketch can be applied to protect the templates. They have proposed a general framework to design and analyze a secure sketch for biometric templates. And also they have discussed how secure sketches are used in the design of multifactor authentication systems.

S. Tulyakov, F. Farooq, V. Govindaraju: "Symmetric Hash Functions for Fingerprint minutiae" [4], has worked on fingerprints to secure the information of it. First the fingerprints are collected from the scanners. One way transformation is performed. Set of minutiae points from the scanned fingerprint images are extracted and hash functions are applied on them. Verification is done by using fingerprint matching algorithm.

In [5], "A cryptographic biometric authentication system based on genetic fingerprints, U. Korte, M. Krawczak, J. Merkle, R. Plaga, M. Niesing, C.Tiemann, H. Vinck, U. artinihave specified a system for authentication and key derivation using genetic fingerprints which prevent the recovery of stored biometric information for verification. A detailed security analysis which is based on estimates of the entropy of DNA data is presented. They have analyzed the typical frequency and structure of errors in DNA measurements and shown that the scheme is robust and efficient.

III. SECURE SKETCH GENERATION



Signatures from people are collected and are enrolled. During this enrolment, the secure sketch algorithm extracts k statistical features from each of the given reference samples of signatures. From these a single feature vector E_{ID} is derived which is used to calculate the secure sketch P_{ID} as helper data for each person and is stored in the database. The test signature is taken to be verified with the trained signature for matching.

A.Pre-processing

The scanned signature image may contain spurious noise that has to beremoved to avoid errors in the further processing steps. The gray image $I_o$of size M*N is inverted to obtain an image $I_i$in which the signature part consisting of higher gray levels form the foreground.

$$\mathbf{I_i\ (i,\ j) = I_o,\ max\text{-}\ I_o\ (i,\ j)} \quad \textbf{..... (i)}$$

Where,I_o,maxis the maximum gray-level. The background, which should be ideally dark, may consist of pixels or group of pixels with gray values between that of foreground and background.

These are removed by performing a row averaging process to generate the row averaged image I_{ra}, which is given by,

$$\mathbf{I_r(i,j) = I_i(i,j) - l{=}1\Sigma M\ I_i(l,j)/M}$$
$$\mathbf{I_{ra}(i,j) = I_r(i,j)\ if\ I_r(i,j) > 0}$$
$$\mathbf{= 0 otherwise} \quad \textbf{..... (ii)}$$

By using an n*n averaging filter,noise removal and smoothening is achieved to generate a cleaned image I_a.

$$\mathbf{I_a(i,j) = 1/9\ (l{=}i\text{-}1\Sigma i{+}1\ k{=}j\text{-}1\Sigma j{+}1\ I_{ra}(i,k))}$$
$$\textbf{..... (iii)}$$

B.Feature Extraction

1. *Width:* The width of scanned signature.

2. *Height:* The height of scanned signature.

3. *Aspect ratio=W/H*

The aspect ratio (A) is the ratio of width to height of the signature. The bounding box coordinates of the signature are determined and the width (Dx) and height (Dy) arecomputed using these coordinates.

$$\mathbf{A = D_x/D_y} \quad \textbf{..... (iv)}$$

4. *Baseline Slant Angle:*The imaginary line about which the signature is assumed to rest is called Baseline. The angle of inclination of this line to the horizontal is called the Slant Angle Θ. To determine the slant angle the ratio of the maximum horizontal projection to the

ISSN : 2278 – 1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2012

width of the projection is maximized over a range of values of angle of rotation θ.

$\mathbf{P_H(i)} = \mathbf{j=0\Sigma N-1\ I_T(i,j)}$
$\rho(\theta) = \mathbf{H(\theta)/W(\theta)}\ -\theta_1<\theta<\theta_2$
$\mathbf{H(\theta)} = \mathbf{Max\ P_H(i)}$
$\mathbf{W(\theta)}$ = **number of non-zero elements in** $\mathbf{P_H(i)}$
…….....(v)

Θ is the value of θ at which ρ(θ) attains maximum. The ratio ρ (θ) is smaller at every angle other than the baseline slant angle. The threshold image $I_T$is rotated by this angle to obtain the slant normalized signature image I_R.

5. *Normalized area of the signature:* Normalized area (NA) is the ratio of the area occupied by the pixels of the signature to the area of bounding box.

$\mathbf{NA = \Delta/(D_xD_y)}$,
Where,Δ is the area of signature pixels.

6. *Centre of Gravity:* The Centre of Gravity is the 2-tuple (X,Y) given by,

$\mathbf{X = j=0\Sigma N-1\ P_V(j)*j/\Delta}$
$\mathbf{Y = i=0\Sigma M-1\ P_H(i)*i/\Delta}$,

Where,$P_V$and $P_H$are the vertical and horizontal projections respectively.

7. *Slope of the line joining theCentres of Gravity of the two halves of signature image:* The signature images are divided into two halves, left and right and separately determine the centres of gravity of the two halves. The slope of the line joining the two centresserves as an attractive feature to distinguish signatures.

8. *Number of Edge Points:* A point that has only one 8-neighbor is an edge point. In order to extract theedgepoints in a given signature, a 3×3 structuring element is used with all coefficients equalto 1.

9. *Number of Cross Points:* Cross point is a point that has at least three 8-neighbors. The structuring elementwhich was used to extract edge points, was also used to extract the cross points in asignature.

10. *Writing pressure:* Checks the thickness oflines & takes the average.

C.Generation of secure sketch P_{ID}

In order to generate one reference feature vector E_{ID} for each user, the midpoint for each feature is determined and stored in midpoint vector E_{mid}. Thus, in the first step the interval I is calculated which is given by the minimum (E_{min}) and maximum (E_{max}) of the feature values of the samples derived during the enrolment process:

$$\mathbf{I = E_{max} - E_{min}} \text{..... (1)}$$

The second step calculates the midpoint $E_{mid}$for each feature of the user. Then a quantized midpoint E'_{mid} is calculated as shown in equation (2) under the given condition. The quantization step S which is equal to the maximum interval length is determined based on the intervals of all the users.

$$\mathbf{E'_{mid} = E_{mid}/\ S} \text{..... (2)}$$

under the conditions,

$\mathbf{E'_{mid} * S} \leq \mathbf{E_{mid}}$ **and**

$\mathbf{(E'_{mid}-1) * S} > \mathbf{E_{mid}}$

Equation (3) determines the CB_{cond} as parameter for a codeword generation in step three

$$\mathbf{CB_{cond}} = \frac{\mathbf{(E_{max} - E_{min})/\ 2}}{\mathbf{S}} \quad \text{…...……(3)}$$

Using CB_{cond} and account for the condition in equation (4) a codebook is constructed by calculatingthe corresponding codeword C based on quantized midpoint E'_{mid} using the equation (5):

$$\mathbf{|E'_{mid} - C| \leq CB_{cond}} \text{……..……(4)}$$

$$\mathbf{C} = \frac{\mathbf{E'_{mid}}}{\mathbf{(2 * CB_{cond} + 1)^2}} \text{……(5)}$$

The secure sketch P_{ID} for user ID is calculated, in the last step, by subtraction of the correspondingcodeword C from the quantized midpoint as shown in (6).

ISSN : 2278 – 1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2012

$$P_{ID} = E'_{mid} – C \text{..... (6)}$$

TABLE I

EVALUATION RESULTS FOR SECURE SKETCH AND PNN METHOD WITH THREE CRITERIONS.

Criterion	SSHcode	NN	SSHcode %	NN %
Collision	9	4	56	25
Acceptance	7	12	43.75	75
No Match	0	0	0	0

IV. EVALUATION

The next subsection describes the evaluation of the performanceof hash generation using secure sketch as well as the PNN.

Methodology

Here we have verified the genuine signature of a person with the false one by comparing the trained and the test signatures. We have taken the reference criterion as acceptance, collision and no match.

We have collected the data of 16 people; from each person 8 signatures are obtained. From these 8 signs, 7 are used for training and 1 for testing.

Both Secure Sketch and PNN areimplemented using these signatures.As shown in table 1, for the number of samples in the database, we got the collision rate as*56%* for Secure Sketch method and *25%* for PNN. Acceptance rate is *43.75%* for Secure Sketch method and *75%*for PNN method.No Match criterion is *0%* as we have checked for only 16 people's samples in the database.

V. CONCLUSION AND FUTURE WORK

In this paper a method is suggested based on thesecure sketch framework. In the comparative evaluation of the verification and/or hashgeneration modes of the presented secure sketchmethod and a method using neural network, it is shown that theperformance of the algorithm is better using neural network approach compared to that of secure sketch method.

On one side, the secure sketch calculates the best results with the parameter "time taken".

For the number of samples in the database, collision rate for Secure Sketch method is *56%* and for PNN it is *25%*. Acceptance rate is *43.75%* for Secure Sketch method and *75%* for PNN method. No Match criterion is *0%*, as depicted graphically in fig 1.

The Secure Sketch algorithm is worse than the Neural Network method in each tested scenario using the hash generation mode. Here the best result is calculated by the PNN method.

Thus the conclusion is that PNN is best as compared to the secure sketch method.

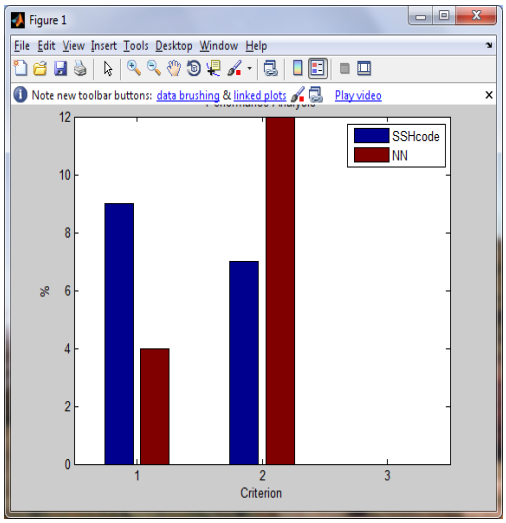


Fig 1: Performance Graph

The above graph shows the performance of Secure Sketch method as well as PNN in the form of Bar graph.

REFERENCES

[1]Tobias Scheidat, Claus Vielhauer, Jana Dittmann*"Biometric Hash Generation and User Authentication based on Handwriting using Secure Sketches".*

[2] Y. Sutcu, Q. Li, and N. Memon, *Protecting Biometric Templates with Sketch: Theory and Practice*, IEEE Transactions on Information Forensics and Security, vol. 2, no. 3, 2007, 503–512.

[3] C. Vielhauer, R. Steinmetz, A. Mayerhöfer: *Biometric Hash based on Statistical Features of Online Signature*, Proc. of the International Conference on Pattern Recognition (ICPR), Quebec City, Canada, Vol. 1, 2002.

[4] S. Tulyakov, F. Farooq, V. Govindaraju: *Symmetric Hash Functions for Fingerprint minutiae*. International Workshop on Pattern Recognition for Crime Prevention, Security and
Surveillance, Bath, 2005.

[5] U. Korte, M. Krawczak, J. Merkle, R. Plaga, M. Niesing, C. Tiemann, H. Vinck, U. artini: *A cryptographic biometric authentication system based on genetic fingerprints*, In:Alkassar, Siekmann (Eds.): Sicherheit 2008 - Sicherheit, Schutz und Zuverlässigkeit; Beiträge der 4. Jahrestagung des FachbereichsSicherheit der GesellschaftfürInformatike.V., Saarbrücken, 2008.

[6] C. Vielhauer, *Biometric User Authentication for IT Security:* From Fundamentals to Handwriting, Springer, New York, 2006.

[7] S.G. Kanade, D. Camara, E. Krichen, D. Petrovska-Delacrétaz, B. Dorizzi: *Three factor scheme for biometricbased cryptographic key regeneration using iris*, In proceedings of BSYM '08: The 6th Biometrics Symposium in conjunction with The Biometric Consortium Conference (BCC), September 23-25, Tampa, Florida, USA, 2008,

[8] *"Handwritten Signature Verification"*by AshishDhawan,Aditi R. Ganesan.