Volume 3, Issue 8, August 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

SURF Based Design and Implementation for Handwritten Signature Verification

Surabhi Garhawal
Department of Computer Science,
Gyan Ganga College of Technology, Jabalpur, India

Neeraj Shukla
Professor, Department of Computer Science
Gyan Ganga College of Technology, Jabalpur, India

Abstract— People are comfortable with pen and papers for authentication and authorization in legal transactions. Due to increase in amount of offline handwritten signatures it is very essential that a person's handwritten signature to be identified uniquely. In this paper we will evaluate the use of SURF features in handwritten signature verification. For each known writer we will take a sample of three genuine signatures and extract their SURF descriptors. We will calculate the intra class Euclidean distances among SURF descriptors of this known signature. Key points Euclidean distances, Image distances and the intra class thresholds will be stored as templates. We will calculate various intra class distance thresholds like maximum, average, minimum and range. Each signature claimed to be of the known writers, we then extract its SURF descriptors and calculate the inter-class distances that is the Euclidean distances between each of its SURF descriptors and those of the known template and image distances between the test signature and members of the genuine section. The intra class threshold will be compared to the inter class threshold for the claimed signature to be measured a forgery. A database of 90 signatures consisting of a training set and a test set will be used. Training set creates 54 genuine signatures from 18 known writers each contributing a sample of 3 signatures. The test set will comprise 36 signatures, 18 genuine signatures and 18 forged signatures. Specificity of the verifier will be measured and compared with the results from the analysis of Universal signature database.

Keywords— Static signature verification, SURF feature, FAR (False Acceptance Rate), FRR (False Rejection Rate).

I. INTRODUCTION

Today's society where forgery is rampant, here is the need for an automatic signature verification system to complement visual verification. Biometrics is the technological way that enables the identification or true verification of an individual from its physical or behavioral characteristics depending on their nature. Physiological biometrics calculates some physical features of the subject like fingerprints, iris and finger geometry which are stable over time. And Behavioural biometrics measures user actions like speaking, writing and walking affected by health, age. A signature is a behavioural biometric that a writer learns and acquires over a period of time and becomes his unique identity [12].

The objective of signature verification systems is to differentiate between original and forged signature, related to intra personal and inter personal variability. Intra personal variations is distinction among the signatures of the same person and inter personal is the variation between the originals and the forgeries. There will always be slight variations in a human's handwritten signature, the consistency generated by natural motion and practice over time generates a recognizable pattern that makes the handwritten signature suitable for biometric identification. A signature forgery means an attempt to copy someone else's signature and use them against him to steal his identity there can be basically three types of forgeries [2]: Both offline and online systems are used to detect various types of forgeries.

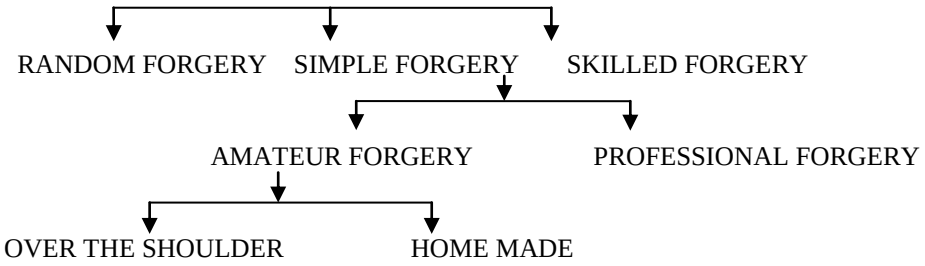

Figure 1.1 Classification of forgeries.

Signature forgeries are classified as follows [12], [9], [13], [28]:

Random forgery: The forger does not have the shape of the writer signature but comes up with a scribble of his own. This forgery accounts for majority of forgery cases though it's easy to detect with naked eyes.

Simple forgery: The forger knows the writers signature shape and tries to imitate it without much practice.
Skilled forgeries: The forger has unrestricted access to genuine signature model and comes up with a forged sample.

II. LITERATURE REVIEW

Hidden Markov Model (HMM)

The approach of Justino et al [6], Graphometric features is static features like the density of pixels and the pseudo dynamic features represented by axial slant. They employ grid segmentation and divide the signature image into four zones each with column containing cells with horizontal and vertical projections. And each column is changed to a characteristic vector assigned a numeric value. So HMM is used for the learning and verification process.

In [13], a system is introduced that uses only global features. A discrete radon transform is a sinograph is measure for each signature binary image at range of $0 - 360$ _, which is a function of total pixel in the image and the intensity per given pixel calculated using non overlapping beams per angle for X number of angles. Periodicity, it is shift, rotation and scale invariant. HMM is used to model each writer signature achieves an AER of 18.4% for a set of 440 genuine signatures from 32 writers with 132 skilled forgeries.

The inference taken form [33], the signature to be trained or recognized is vertically divided into segments at the centre of gravity using the space reference positions of the pixels. Number of segmented signature blocks is equal to the number of states in the HMM for each user notwithstanding the length of the signatures. That shows successful signatures a recognition rate of 99.2% is possible.

Fuzzy Logic

In [3], global features of the signature like the skeleton of the pen trace and the structure of upper and lower envelope are used as shape descriptors. These are experiential by sampling upper and external points from the binary image of the true signature. High pressure regions where the writer made more pressure to be generated to a linear function that is be used for maximizing the correlation between the vertical and horizontal projections of the skeleton. For each shape descriptors a multi- layer perception is assigned and the network is trained with a modified back propagation algorithm and the output of each individual network is combined throughout fuzzy integral voter. By a test set of 1000 signatures the approach obtained 90% true verification.

The authors in [22] propose the system that extracts angle features that are modeled in to a fuzzy model based on Takagi-Sugeno model. That extended to include structural parameters that account for variation in writer's styles and changes in mood and the inputs are optimized to derive multiple rules. This approach obtained over 70% true verification.

In [35] find points as control points on the boundary of the signature. These points are locations of the boundary; show the structural characteristics of a signature. Four different types of local features are extracted from control points on set of training signatures and these features fuzzified for training of FIS. According to that output of FIS, after that make decision that test signature is forgery or genuine. Effectiveness of the algorithm depend on variations between training signatures so if the training signatures of the specific person are not enough similar to each other, the algorithm cannot have good performance and FAR (False Acceptance Rate) will grow.

Neural Networks

The proposed system [25] using structure features from modified direction feature and other features as surface area, length skew and centroid feature where signature is divided into two halves and for each half a position of the centre of gravity is calculating with reference to the horizontal axis. For classification two approaches are compared the Resilient Backpropagation (RBP) neural network and Radial Basic Function(RBF) using a database of 2106 signatures containing 936 genuine and 1170 forgeries. These two classifiers register 91.21% and 88 % true verification respectively.

The works of Alan McCabe [29] Several Network topologies are tested and their accuracy is compared. The most successful version of the NN based HSV system uses a single MLP with one hidden layer to model each user's signature. It is trained using five genuine signatures and one hundred zero-effort forgeries. Using this approach, a 3:3% OER is reported for the best case.

In [36] signature is captured and presented to the user in an image format. Then Signatures are verified cbn using parameters extracted from the signature based on various image processing techniques. It helps in detecting the exact person and it provides more accuracy of verifying signatures as compared to prior works. For verification of signatures some novel features needs to be extracted. For implementation of above this paper uses Feed Forward Neural Network (FFNN) for recognition and verification of signatures of individuals.

The inference taken from [38] Extracted features is used to train a neural network using error back propagation training algorithm. The network could categorize all genuine and forged signatures. When the network was presented with signature samples from database different than the ones used in training phase, out of 300 such signatures (150 genuine and 150 forged) it could recognize 248 signatures correctly. Therefore, the correct classification rate of the system is 82.66% in generalization. Recognition system exhibited 100% success rate by identifying correctly all the signatures that it was trained for. But, it exhibited poor performance when it was presented with signatures that it was not trained for earlier.

Graph Matching

The author [31] proposed CGMOSV algorithm in which the signatures are compared using Graph matching and the Euclidean distance is considered as the dissimilarity measure between them. The Cross-validation principle is used in the

selection of reference set of signatures. The pre-processing of signature is carried out with signature extraction to reduce Equal Error Rate *EER.* It is observed that FRR, FAR and EER values are improved compared to the existing algorithm.
In [30] each pixel is compared with alternating pixel in the other image, thus incurring a huge computational overhead. Images of resolution of P × Q and A x B, P, Q, A and B being usually in the range 300-1200, And compute a non-negative n×m matrix, where the i-th row and j-th column for cost of assigning the i-th pixel to the j-th pixel in considered images 1 and 2 . The complexity of the algorithm amounts to be O (n3) where (n~=m). These critical regions give significantly to the shape of the original image and therefore serve as accurate model of the true signature. These critical regions are utilized as a basis for graph matching, thus reducing the computational overhead by a large amount. Critical regions of size 31×31 are constructed and compared using Hungarian method. And this computation is done for only some identified points, say Ncrit. So the computational time is compact to (Ncrit O (p3)) where (p<<n). Usually value of Ncrit=20, this can amount to around 106 times less than the time overhead.

Statistical and Distance Classifiers

The uniqueness of writers' handwriting is mapped with that of the signature in Srihari et al [12]. The writer sign in a predefined space of 2×2 inches and rotation is normalized with the horizontal axis. The gradient, structural and concavity are used as image descriptors. The gradient detects the local features of the image and the concavity detects the relationship between the structural and the local features. The verification is done by Bayesian classifier .It uses two databases of signature with a total of 106 writers and 3960 samples and obtains FRR of 21.90% and 30.93% respectively .this system uses global descriptors and local features. And split the signature into regions and get the (CoG) of sub region and the distance made by the CoG and the strokes whitespaces. Then learning algorithm used is C4.5 and classifying method is based on a decision tree. It uses 100 genuine signature and 300 forgeries from 20 people who consist of 15 Chinese and 5 people providing English signatures. For both cases over 90% success verification is reported. The method in [24] uses the geometric centre for feature extraction. The centre is obtained throughout vertical and horizontal splitting of the image. Then signatures are taken at different time periods to prove the intrapersonal variations. The classification is done by a Euclidean classifier model which measured variance between any two image vectors. For testing 21 genuine signatures and 30 forgeries are used. Set of different 9 signatures is used for training the model, FAR obtained are 2.08%, 9.75% and 16.36% for random, simple and skilled forgeries receptively. The FRR for original signatures is 14.58%.

Incorporating a Prior Model

[21] That only requires the set of genuine signatures. They use a two stage approach with the training stage where learning parameter of the classifier is used and application stage with primary classifier to get the new user signature and final classifier to map the output of primary classifier and the mapping obtained at the training stage. It uses the global features that provide information about the whole structure of the signature. Then grid gray features are obtained as an average gray value in each grid overlapped on the pre-processed image and pseudo dynamic features descriptors like ink distribution. Set of descriptors, the classifiers give the FRR and FAR for simple forgery as follows. Texture feature 25% and 30.56%; grid features 25.42% and 22.78%, global feature 42.08% and 27.22 % for FRR and FAR respectively.

Support Vector Machine (SVM)

[32] Discrete Radon Transform used for extracts global features from the signatures. During enrolment, a number of reference signatures are used for each registered user and cross aligned to extract statistics about that user's signature. We experimented with SVM classifier and KNN classifier. Using a database of 2250 signatures (genuine signatures and skilled forgeries) from 75 writers our present system achieves a performance of approximately 80 % when used SVM classifier and a performance of approximately70 % in the case of KNN classifier.
In proposed system [37] Signature database was utilized for training the SVM .Then the signature verification accuracy of the model has been evaluated in terms of FAR, FRR and FIR. Accordingly, SVM described in this paper successfully verifies the off-line signature with 90% accuracy.

Scale invariant feature transform (SIFT)

In [34] decided as robust image descriptors. A database of signatures was collected consisting of known writers' signatures and forgeries. The efficiency of the verifier was tested and specificity and the sensitivity were measured for each test taken. It was noted that some writers have large discrepancies between three of their sample signatures such that even a forgery may fall within the intra class distances which may result to a false negative notification. Classifier should have high rates of specificity and sensitivity. To be able to have an efficient classifier we picked the test that had high rates of both specificity and sensitivity. Using a range of 0.05 on both the minimum intra-class distance and minimum intra-class distance as a threshold such that the minimum and maximum inter- class distance should lie within that range. The performance statistics obtained from this test showed that SIFT features can be used with Euclidean distances for offline handwritten signature verification.

III . RELATED WORK IN SURF

Interest Point Detection

It is based on the eigenvalues of the second moment matrix. Where, Harris corners are not scale-invariant. Lindeberg [4] introduced the concept of automatic scale selection. This allows detecting interest points in image, each with their own

characteristic scale. And he experimented with both the determinant of the Hessian matrix as well as the Laplacian to detect blob-like structures. Mikolajczyk and Schmid [7] refined this method; create robust and scale-invariant feature detectors with repeat ability, and they coined Harris-Laplace and Hessian-Laplace. They used a (scale-adapted) Harris measure or the determinant of the Hessian matrix to select the location, and Laplacian to select the scale. Focus on speed; Lowe [5] proposed to approximate the Laplacian of Gaussians (LoG) by a Difference of Gaussians (DoG) filter.

From studying the existing detectors and from published comparisons [18], we can conclude that Hessian-based detectors are more stable and repeatable than their Harris-based counterparts. Moreover, using the determinant of the Hessian matrix rather than its trace (the Laplacian) seems advantageous, as it _res less on elongated, ill-localised structures. We also observed that approximations like the DoG can bring speed at a low cost in terms of lost accuracy.

Interest Point Description

An even larger variety of feature descriptors has been proposed, like Gaussian derivatives [1], moment invariants [19], complex features [8], phase-based local features [10], and descriptors representing the distribution of smaller-scale features within the interest point neighbourhood. The latter, introduced by Lowe [17], have been shown to outperform the others [11]. SIFT for short, computing a histogram of local oriented gradients around the interest point and stores the bins in a 128-dimensional vector. Various refinements on this basic scheme have been pro-posed. Ke and Sukthankar [16] applied PCA on the gradient image around the detected interest point. This PCA-SIFT yields a 36-dimensional descriptor which is fast for matching, however proved to be less distinctive than SIFT in a second comparative study by Mikolajczyk [23] applying PCA slows down feature computation. The authors proposed a variant of SIFT, called GLOH, which proved to be more distinctive with the same number of dimensions. But, GLOH is computationally more expensive as it uses again PCA for data compression.

Recently, Se et al. [20] implemented SIFT on a Field Programmable Gate Array (FPGA) and improved its speed by an order of magnitude. Meanwhile, Grabner et al. [26] also used integral images to approximate SIFT. Their detection step is based on difference-of-mean (without interpolation), their description step on integral histograms. They achieve about the same speed as we, but at the cost of reduced quality compared to SIFT. Generally, the high dimensionality of the descriptor is a drawback of SIFT at the matching step. For online applications relying only on a regular PC, each one of the three steps (detection, description, matching) has to be fast.

An entire body of work is available on speeding up the matching step. All come at the expense of getting an approximate matching. Methods include the best-bin- proposed by vocabulary trees [27], locality sensitive hashing [14], or redundant bit vectors [15]. Complementary to this, we suggest the use of the Hessian matrix's trace to significantly increase the matching speed. Together with the descriptor's low dimensionality, any matching algorithm is bound to perform faster.

IV. SIGNIFICANCE OF THE STUDY

This research sought to evaluate use of SURF in solving handwritten signature verification problems. SURF descriptors are robust image descriptors and cheap to compute in terms of processing requirements compared with other methods like neural networks, support vector machine, scale invariant feature transform and they can easily be used in low resourced environments to reduce losses that arise from forged handwritten signatures and assist to make timely decision.

V. METHODOLOGY

5.1 Introduction

The SURF algorithm takes an image and transforms it into a collection of local features where each of these feature vectors is distinctive and invariant to scaling, rotation or translation of image. The implementation was done in MATLAB. The approach taken is a two step process with signature enrolment and verification. In the test set forged signatures were generated by imitating the genuine signatures for each class on a piece of paper. Then forgery was done by two people each one generate a sample of three forged signatures per class which were given to a third party to chose one forgery which directly resembles the genuine set. Forged signature was also scanned, cropped and stored in portable network graphic (PNG) format.

5.2 Offline Handwritten Signature Verification

The approach used for offline handwritten signature verification was broadly divided into two steps, signature enrolment and signature verification. Signature enrolment had four sub steps namely image pre-processing, extraction of SURF features from signatures, calculation of Euclidean distances between images and creation of the known class signatures template. Signature verification had two sub steps namely outlier detection and comparison of test signature with known set so as to make a decision whether it is a genuine signature or not.

5.3 Signature Enrolment

Signature enrolment concerned preparation of signatures, extraction of SURF features and registration of signatures images and their SURF features in the system.

5.3.1 Image Pre-Processing

The images used were signatures and were extracted from documents through scanning and cropping. A random sample of 18 signers was used; each signer contributed a sample of 3 signatures giving a total of 54 genuine signatures for the training set. The test set consisted of 18 genuine signatures and 18 forged signatures giving a total of 36 signatures for the

test set. A database of 90 signatures was used in the training set and test set. And signature images were stored in portable network graphic format. These images were converted to gray scale for further processing.

5.3.2 Extraction of SURF Features from Signatures

The SURF algorithm is composed of mainly two parts: first, we detect interest point. Second, we perform interest point description. Both of these parts relay on a scale space representation and first and second order differential operators. Uniqueness of the SURF method is that these operations are speeded up by the use of an integral image and box filters techniques. The basic algorithm to compute SURF features can be described in following steps [39]:

Firstly compute an integral image with respect to an input image.

Interest point detection:

1. Then using box filters compute the discrete Hessian operator at several scales.
2. After that compute the local maxima of the hessian determinant operator applied to the scale space in order to select interest point candidates.
3. Using Quadratic interpolation, we need to refine corresponding interest point location.
4. We should store all interest points along with its Laplacian sign.

Finally, constructing the local feature descriptor involves:

1. Calculating the dominant orientation of each interest point.
2. Final computation of the descriptor corresponding to the scaled and oriented neighborhood of the interest points.

Figure 5.1 Example of scale space Gaussian images.

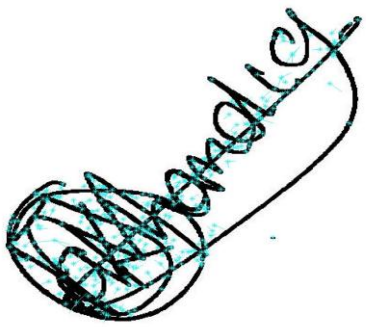

Figure 5.2 Example of a signature with extracted SURF features.

5.3.3 Calculation of Euclidean Distances

Euclidean distance as a measure of variability between images is derived from its success in object recognition; we have two signatures A and B. Let Ai be the ith keypoint in signature A and Bj be the jth keypoint in signature B. The distance D (Ai, Bj) was calculated as the Euclidean distance between Ai and Bj. Ka, Kb are the number of keypoints in signature A and B. Distance measure D (Ai,B) was taken as the average Euclidean distance from the ith keypoint in signature A to all the keypoints of signature B. The image distance involving signature A and signature B is given by:

$$D(A,B) = \frac{1}{K_a}\sum_{i=1}^{K_a} D(A_i, B)$$

5.3.4 Creating the Known Signature Template.

Only the signatures and random writer IDs were used. For every known writer, a sample of three signatures say A, B and C were taken to supply intrapersonal variations. Then template was generated as a MATLAB file and stored. The template has the following:

(i) Writer ID.

(ii) The Euclidean distances between keypoints i.e. D (Ai, B), D (Ai, C), and D (Bj, C).

(iii) The distances between the Signature images i.e. D (A, B), D (A, C) and D (B, C).

(iv) Intraclass thresholds: Maximum among D(A,B),D(A,C) and D(B,C) i.e. max(D(A,B),D(A,C),D(B,C)). Minimum among D(A,B),D(A,C) and D(B,C) i.e. min (D(A,B),D(A,C),D(B,C)). Average on D(A,B),D(A,C) and D(B,C) i.e. avg (D(A,B),D(A,C),D(B,C)). Range on maximum intraclass distance given by max(D(A,B),D(A,C),D(B,C))± 0.05. Range on minimum intraclass distance given by min (D (A, B), D (A, C), D (B, C)) ± 0.05.

Figure 5.3 Example of intra-personal variation.

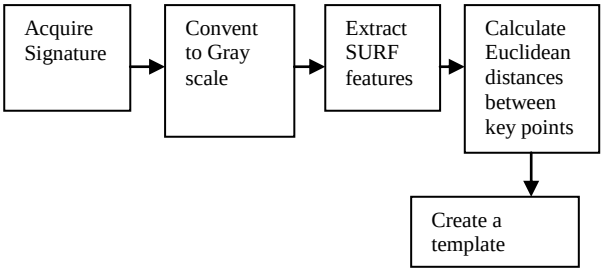

Figure 5.4 Steps in signature enrolment.

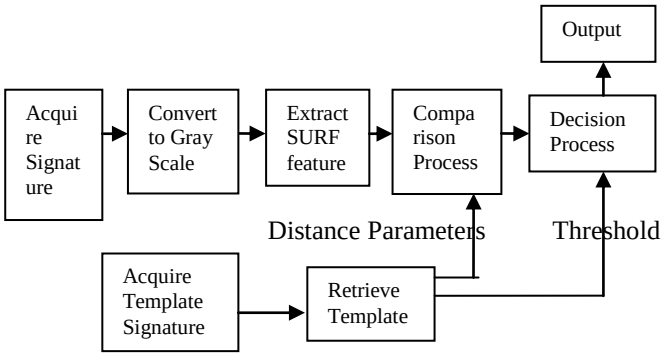

Figure 5.5 signatures Enrolment and Verification

5.4 Signature Verification

Verification is the process of testing whether a claimed signature is that particular signature belongs to a specific class is true or false. Verification provide loading the template MATLAB file enrolled in the system and comparing its stored parameters with those calculated by the outlier detection process.

5.4.1 Outlier Detection

Given a test signature say T claimed to be of a particular writer, the Euclidean distances were calculated between the test signature and each of the three sample signatures resulting to distances between the images i.e. D(T,A), D(T,B) and D(T,C). The inter-class thresholds, max(D(T,A),D(T,B),D(T,C)), min (D(T,A),D(T,B),D(T,C)), avg (D(T,A),D(T,B),D(T,C)) are computed.

5.4.2 Comparison and Decision Criteria

The comparison between the distance parameters of the SURF features of the claimed test signature was done with those of the stored template. Each decision criteria was a binary classification and was taken independently. We let W be (D(T,A),D(T,B),D(T,C)) and Z be (D(A,B),D(A,C),D(B,C)).

Test 1: Compare inter-class maximum distance with intra-class maximum distance as threshold.

Classify T as genuine if the condition *max* (*Z*) > *max* (*W*), if not we classify T as not genuine.

Test 2: Compare average of inter-class distances with the average of intra-class distance as threshold.

Classify T as genuine if the condition *avg* (*Z*) > *avg* (*W*), if not classify T as not genuine.

Test 3: Compare inter-class minimum distance with intra-class minimum distance as threshold.

Classify T as genuine if the condition *min* (*Z*) > *min* (*W*), if not we classify T as not genuine.

Test 4: Using a range of 0.05 on the maximum intra-class distance as a threshold and compare with inter-class maximum distance.

Classify T as genuine if the condition *max* (*Z*) ± 0.05 > *max* (*W*), if not we classify T as not genuine.

Test 5: Using a range of 0.05 on the minimum intra-class distance as a threshold and compare with inter-class minimum distance.

Classify T as genuine if the condition *min* (*Z*)) ± 0.05 > *min* (*W*), If not we classify T as not genuine.

Test 6: Using a range of 0.05 on both the minimum intra-class distance and minimum intraclass distance as a threshold such that the minimum and maximum inter- class distance should lie within that range

Classify T as genuine if the condition *max* (*Z*) ± 0.05 > *max* (*W*) *and min* (*Z*) ± 0.05 > *min* (*W*), if not classify T as not genuine. We classify T as not genuine.

Test 6: Using a range of 0.05 on both the minimum intra-class distance and minimum intraclass distance as a threshold such that the minimum and maximum inter- class distance should lie within that range.

Classify T as genuine if the condition *max* (*Z*) ± 0.05 > *max* (*W*) *and min* (*Z*) ± 0.05 > *min* (*W*), if not classify T as not genuine.

5.5 Signature Verifier Accuracy

To measure the accuracy of the verifier, a set contain genuine signatures and forged signatures. Various performance statistics were used. And these statistics are standard in machine.

(i) **True Positive** (TP) - A classification is a true positive if the signature is genuine and the output of the verifier ascertains that.

(ii) **False Positive** (FP) - A classification is a false positive if the signature is forged and the output of the verifier claims that it is genuine.

(iii) **True Negative** (TN) - A classification is a true negative if the signature is forged and the output of the verifier ascertains that.

(iv) **False Negative** (FN) - A classification is a false negative if the signature is genuine (of known writer) and the output of the verifier claims that it is forged.

(v) **The sensitivity** is the proportion of actual positives which are correctly identified as positives. This is given by:

$$Sensitivity = \frac{TP}{TP + FN}$$

(vi) **The specificity** is the proportion of negatives (forgeries) which are correctly identified, which is given by:

$$Specificity = \frac{TN}{TN + FP}$$

5.6 The Proposed Algorithm

(i) Given the set of known signatures and test signatures signed in a document, scan and crop each class of known's and its relevant test signatures and save them as portable network graphic (PNG) format. (ii) Each signature in the class of known signatures say A, B, C and test signature T, perform SURF extraction.

(iii) For each pair of known signatures A,B, Let Ai be the ith interest point in signature A and Bj be the jth interest point in signature B. Calculate Euclidean distance D(Ai,Bj) and the distance D(Ai,B), the average distance from the ith interest point in signature A to all interest points of signature B.

(iv) Then Calculate image distance D (A, B).

(v) Create template of known signatures class consisting of writer ID, distance parameters and intra - class thresholds.

(vi) For a given test signature T claimed to be of a known writer, Calculate the inter class distances between T and each signature in the class of known's in the template. Get the interclass thresholds.

(vii) Compare the intra - class thresholds in the template with inter- class thresholds.

(viii) At last test the performance of the classifier using the performance statistics.

VI. RESULTS

6.1 Introduction

To measure the accuracy of the SURF based verifier, consisting of genuine signatures and forged signatures was used. Total 90 signatures were used. The training set had 54 genuine signatures for creating the known signature templates. Test set consisted of a total of 36 signatures (18 genuine signatures and 18 forged signatures).

6.2 Examples of Verified Signatures

Table 6.1 shows the image distances between the set of known signatures 16.png, 17.png and 18.png. The intra class maximum, max(D(16,17),D(17,18),D(16,18)) = 1.1710 is greater than the inter class maximum max(D(16,19),D(17,19),D(18,19)) = 1.0700. The intra class average, avg (D(16,17),D(17,18),D(16,18)) = 1.1293 is greater than the inter class average avg (D(16,19),D(17,19),D(18,19)) = 1.0497, the intra class range on maximum intra class distances is 1.2210 is also greater than inter class maximum max (D(16,19),D(17,19),D(18,19))= 1.0700. The intra-class minimum min (D (16, 17), D (17, 18), D (16, 18)) = 1.1069 is greater than inter class minimum distance which is 1.0382. Also the range on minimum, min(D(16,17),D(17,18),D(16,18))- 0.05= 1.0569 is also greater than inter class minimum. Thus based on all the tests signature 19.png is properly classified as genuine. In table 6.2 the inter class distances between the test signature 19.png and the template of known's.

		Actual Condition(Truth)	
		(+ve) Genuine	(-ve) Forgery
Output of the System	(+ve) Genuine	TP	FP
	(-ve) Forgery	FN	TN

Figure 5.6 Confusion matrixes for analysing accuracy

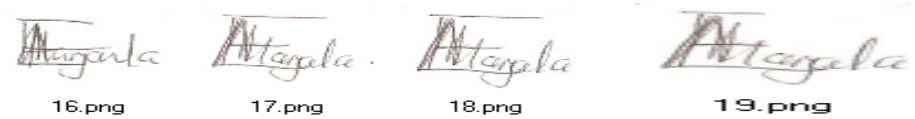

Figure 6.1: Genuine signatures of a known writer. Figure 6.2: Test signature correctly classified as genuine.

Table 6.1: Image distances set of known signatures 16.png, 17.png and 18.png.

Signatures	**Distance description**	**Image distance**
16.png,18.png	D(16,18)	0.88552
17.png,18.png	D(17,18)	0.9368
16.png,17.png	D(16,17)	0.88792

Table 6.2: Image distances between test signature 19.png and set of known signatures.

Signatures	**Distance description**	**Image distance**
16.png,19.png	D(16,19)	0.83288
17.png,19.png)	D(17,19	0.856
18.png,19.png	D(18,19)	0.83056

Figure 6.3: Genuine signatures of a known writer.

Figure 6.4: Test signature correctly classified as forgery.

Table 6.3 shows the intra - class distances among signatures 41.png, 42.png and 43.png. In table 4.4 the inter class distances among known signatures 41.png, 42.png, 43.png and the test signature 45.png.

Table 6.3: Image distances set of known signatures are 41.png, 42.png and 43.png.

Signatures	**Distance description**	**Image distance**
41.png,42.png	D(41,42)	0.84304
41.png,43.png	D(41,43)	0.84304
42.png,43.png	D(42,43)	0.88224

Table 6.4: Image distances between test signature 45.png and set of known's 41.png, 42.png and 43.png.

Signatures	**Distance description**	**Image distance**
41.png,45.png	D(41,45)	0.96096
42.png,45.png	D(42,45)	1.11736
43.png,45.png	D(43,45)	0.84312

6.3 Results from the Proposed Method

MATLAB scripts were used to identify true positives, true negatives, false positives, true positives and to calculate the specificity and sensitivity. Sensitivity is ratio of genuine signatures the classifier is able to correctly identify as genuine from the test set and the specificity is the proportion of the forgeries the classifier is able to correctly classify as forgeries from the test set. Then following statistics were obtained.

6.3.1 Maximum Distance

The specificity of 38.89% was obtained; which is the proportion of forgeries the classifier was able to identify from the testing set and the sensitivity of 77.78% was also obtained; which is the pro- portion of genuine signatures the classifier was able to correctly identify ,that is comparing the maximum intra-class distance with maximum inter-class distance. This means the comparison between the maximum intra - class distance and maximum inter - class distance was better in identifying genuine signatures than in detecting forgeries.

Table 6.5: Performance statistics obtained by the classifier using maximum class distances.

TP	**14**	**FP**	**11**
TN	**7**	**FN**	**4**

6.3.2 Average Distance

Compare the average intra-class distance with average inter-class distance. The specificity of 50% was obtained, which is the proportion of forged signatures correctly identified from the test set and the sensitivity of 44.444% was also obtained, that is the proportion of genuine signatures correctly identified. From these performance statistics it shows the average test was poor and random in both detecting the forged signatures and identifying the genuine signatures.

Table 6.6: Performance statistics obtained by the classifier using average class distances.

TP	**8**	**FP**	**9**
TN	**9**	**FN**	**10**

6.3.3 Minimum Distance

The specificity of 38.889% and the sensitivity of 44.444% were obtained, that is comparing the minimum intra-class distance with minimum inter-class distance. Related to the average test, the minimum distance test performed poorly in both detecting the forged signatures and identifying the genuine signatures.

Table 6.7: Performance statistics obtained by the classifier using minimum class distances.

TP	**7**	**FP**	**10**
TN	**8**	**FN**	**11**

6.3.4 Range of ą0.05 on Maximum Distance

The specificity of 33.3% and the sensitivity of 88.8% were obtained, that is a range of 0.05 on maximum intra-class distance and setting it as a threshold and comparing it with the maximum inter-class distance. This test was the best in terms of sensitivity was able to properly classify highest number of genuine signatures from the test set and the poorest in terms of specificity that means identifying forged signatures.

Table 6.8: Performance statistics obtained by the classifier using the range test on maximum class distances.

TP	**16**	**FP**	**15**
TN	**3**	**FN**	**2**

6.3.5 Range of ą0.05 on Minimum Distance

The specificity of 72.2% and the sensitivity of 50% were obtained, that is a range of 0.05 on the minimum intra-class distance and setting it as a threshold and comparing it with the minimum inter-class distance. This test was the best in identifying the forged signatures from the test set.

Table 6.9: Performance statistics obtained by the classifier using the range test on minimum class distances.

TP	**9**	**FP**	**5**
TN	**13**	**FN**	**9**

6.3.6 Range of ą0.05 on Maximum Distance and Range of ą0.05 on Mini- mum Distance

The specificity of 55.5% and the sensitivity of 77.78% were obtained, that is a range of 0.05 on both the minimum and maximum intra-class distances and setting them as a threshold. In table 4.10 shows the performance statistics obtained by the classifier using the range on both minimum and maximum intra-class distances. A high quality of classifier should have high rates of both specificity and sensitivity. It should be able to correctly classify high proportion of genuine signatures from the test set and also detect high proportion of forged signatures as forgeries in the same test set. Since the performance statistics, this test compared to the rest had high rates on both specificity and sensitivity and was considered for comparison with human experts.

Table 6.10: Performance statistics obtained by the classifier using the range test on both min and max class distances.

TP	**14**	**FP**	**8**
TN	**10**	**FN**	**4**

VII. Conclusion

The objective of this work was mainly to offer an efficient and economically viable offline hand- written signature verifier. In order to meet the objective various existing methods of offline hand- written signature verification were reviewed and SURF features were decided as robust image descriptors. A database of signatures was collected consisting of known writers' signatures and forgeries. The effectiveness of the verifier was tested, specification and the sensitivity was measured for each test taken. It was noted that some writers have large discrepancies between three of their sample signatures such that even a forgery may fall within the intra class distances which may result to a false negative notification this might have been caused by physiological factors. A high quality of classifier should have high rates of specificity and sensitivity. To be able to have an efficient classifier we picked the test that had high rates of both specificity and sensitivity. Using a range of 0.05 on both the minimum intra-class distance and minimum intra-class distance as a threshold such that the minimum and maximum inter- class distance should lie within that range. The performance statistics obtained from this test showed that SURF features can be used with Euclidean distances for offline handwritten verification. While this research is a good start to SURF based handwritten signature verification it can be extended to evaluate other image similarity measures.

References

[1] L. M. J. Florack, B. M. ter Haar Romeny, J. J. Koenderink, and M. A. Viergever "General intensity transformations and di_erential invariants". JMIV, 4(2):171{187, 1994.

[2] Rasha Abbas and Victor Ciesielski, "A Prototype System for Off-line Signature Verification Using Multilayered Feed forward Neural Networks," February 1995.
[3] K. Faez. M. Dehghan. and M. Fathi, "Signature Verification Using Shape Descriptor and Multiple Neural Network," IEEE TENCON 1997-Speech and Image Technologies for Computing and Telecommunications, pp. 415–418, 1997
[4] T. Lindeberg. Feature detection with automatic scale selection. IJCV, 30(2):79 {116, 1998.
[5] D. Lowe. Object recognition from local scale-invariant features. ICCV, 1999.
[6] F. Bortolozi. E. R. Justino., A. E. Yocoubi. and R. Sabourin, "An Off-line Signature Verification System Using HMM and Graph metric features," 4th IAPR International on Document Analysis Systems, Rio de Jeneiro, 2000.
[7] K. Mikolajczyk and C. Schmid. Indexing based on scale invariant interest points. In ICCV, volume 1, 2001.
[8] F. Scha_alitzky and A. Zisserman. "Multi-view matching for unordered image sets, or how do I organize my holiday snaps?" ECCV, volume 1, 2002.
[9] Z. Lin. W. Liang. and R. C. Zhao, "Offline signature verification Incorporating the prior model," International Conference on Machine Learning and Cybernetics, vol. 3, pp. 1602–1606, 2003.
[10] G. Carneiro and A.D. Jepson. "Multi-scale phase-based local features". CVPR (1), pages 736 {743, 2003.
[11] K. Mikolajczyk and C. Schmid. "A performance evaluation of local descriptors". In CVPR, volume 2, June 2003.
[12] S. Srihari. K. M. Kalera. and A. 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.
[13] B. Herbst. J. Coetzer. and J. Preez, "Online Signature Verification Using the Discrete Radon Transform and a Hidden Markov Model," EURASIP Journal on Applied Signal Processing, vol. 4, pp. 559–571, 2004.
[14] M. Datar, N. Immorlica, P. Indyk, and V. S. Mirrokni. Locality-sensitive hashing scheme based on p-stable distributions. In Symposium on Computational Geometry, pages 253{262, 2004.
[15] J. Goldstein, J. C. Platt, and C. J. C. Burges. Redundant bit vectors for quickly searching high-dimensional regions. In Deterministic and Statistical Methods in Machine Learning, pages 137{158, 2004.
[16] Y. Ke and R. Sukthankar. PCA-SIFT: A more distinctive representation for local image descriptors. In CVPR (2), pages 506 { 513, 2004
[17] D. Lowe. Distinctive image features from scale-invariant keypoints, cascade _ltering approach. IJCV, January 2004.
[18] K. Mikolajczyk and C. Schmid. " Scale and a_ne invariant interest point detectors". IJCV, 60(1):63 { 86, 2004.
[19] F. Mindru, T. Tuytelaars, L. Van Gool, and T. Moons. Moment invariants for recognition under changing viewpoint and illumination. CVIU, 94(1-3):3{27, 2004.
[20] S. Se, H.K. Ng, P. Jasiobedzki, and T.J. Moyung. Vision based modeling and localization for planetary exploration rovers. Proceedings of International Astronautical Congress, 2004.
[21] H. S. Srihari and M. Beall, "Signature Verifcation Using Kolmogrov Smirnov Statistic," Proceedings of International Graphonomics Society,Salemo Italy , pp. 152–156, june,2005.
[22] H. Hammandlu and V. M. Krishna, " Off-line Signature Verification and Forgery detection using Fuzzy modeling," Pattern Recognition, vol. 38, pp. 341–356, 2005.
[23] K. Mikolajczyk and C. Schmid. "A performance evaluation of local descriptors". PAMI, 27(10):1615{1630, 2005.
[24] S. Reddy. B. Maghi. and P. Babu, "Novel Features for Offline signature verification.," Journal of Computer,Communication and Control., vol. 1, pp. 17–24, 2006.
[25] M. Blumenstein. S. Armand. and Muthukkumarasamy, "Off-line SignatureVerification using the Enhanced Modified Direction Feature and Neuralbased Classification," International Joint Conference on Neural Networks, 2006.
[26] M. Grabner, H. Grabner, and H. Bischof. Fast approximated sift. ACCV (1), pages 918{927, 2006. [27] D. Nist_er and H. Stew_enius. Scalable recognition with a vocabulary tree. CVPR (2), pages 2161{2168, 2006.
[28] S. I. Abuhaiba, "Offline Signature Verification Using Graph Matching," *Turk J Elec Engine*, vol. 15, no. 1, 2007.
[29] Alan McCabe,"Neural Network-based Handwritten Signature Verification". Journal of computers, volume 3, 2008 .
[30] Ramachandra AC,"Cross-Validation for Graph Matching based Offline Signature Verification". IEEE 978-1-4244-2746-8/08©2008.
[31] Abhay Bansal "Offline Signature Verification Using Critical Region Matching "International Journal of Signal Processing, Image Processing and Pattern Vol. 2, No.1, March, 2009.
[32] A.A. Abdalla Ali,"OFF LINE SIGNATURE VERIFICATION USING RADON TRANSFORM AND SVM/KNN CLASSIFIERS"**,** ISSN 0136-5835. Вестник ТГТУ. 2009. Том 15. № 1. Transactions TSTU.
[33] Dr. S.Adebayo Daramola "Offline Signature Recognition using Hidden Markov Model (HMM)"International Journal of Computer Applications 2010.
[34] Neeraj Shukla "Design and Implementation Handwritten Signature Verification Algorithm using SIFT Features ".International journal of computer engineering and computer application 2010.
[35] M.Nasiri "A Fuzzy Approach for the Automatic Off-line Signature Verification Problem Base on Geometric Features"2012.
[36] Ms. Vibha Pandey **"**Signature Verification Using Morphological Features Based on Artificial Neural Network". International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 7, 2012.

[37] Mandeep Kaur Randhawa "Off-line Signature Verification based on Hu's Moment Invariants and Zone Features using Support Vector Machine". International Journal of Latest Trends in Engineering and Technology (IJLTET) Vol. 1 Issue 3 September 2012.

[38] Pradeep Kumar "Hand Written Signature Recognition & Verification using Neural Network" International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Volume 3, Issue 3, March 2013. [39] www.iopl.im/pub/pre/H2/

