A Signature Best feature selection matching using FAST and genetic algorithm

Mohammad Q. Jawad*, Tamara Z. Fadhil

1University of Information Technology and Communication

* mohammad.qassim2002@uoitc.edu.iq

Abstract. Verification for human is an important method for identifying persons. One of the most important biometric verification is signature which is used to ensure human privacy, both in banking and electronic business signature is the main authentication step for verify the user identity. In this paper system be tested by genetic algorithm to choose the best feature to applied in training and testing which will reduce the require time needed for matching and training and to obtain better matching by checking only the strong features. The feature selection algorithm allows us to reduce the process time and have more accurate results. The GA diagram was acquainted and applied with an element Issue choosing a subset to approve the mark. The calculation demonstrated striking execution in all tests led System split mainly to many stages which is mainly (pre-processing, feature extraction using FAST (Fast Affine Invariant Image Matching), feature reduction (best feature selection) using genetic algorithm and matching process using neural network) The system was tested with 240 signature images with accuracy of 87% with the matching process. The system is simulated and tested using MATLAB.

Keywords— offline signature matching, FAST, SVM, feature selection, genetic algorithm.

1. Introduction

For person identification and authentication examine many techniques used, the main technology used is Biometrics, features obtained from each person is different than others. Biometric systems mainly based on two fields (physical and behavioral Biometric), where the physical biometric can refer to as (Iris and fingerprints) and behavioral is mainly based on signature, handwriting as well as voice. Verification based on behavioral biometric using personal signature is the widely used. The written signature is the global verification system used in many banks and transactions used in physical and e-business, old verification methods globally replaced by automatic (computer based) verification methods which led to reduce time, complexity and errors happens during this verification phase. Verification of person signature usually applied either online (dynamic) or offline (static) based on the techniques used for signature acquirement. [1-8], dynamic method collects information such as pen pressure and speed and the entry device is tablet [9]. Static method collect information by using scanners devices to scan images contain signature [11], the challenge with offline system is the extracted feature and how to compare with pre-defined features obtain from user since the age and situation of person (e.g. sickness) is an impact factors to the obtained signature which effect detecting the original and forgery one [13]. Offline verification system preferable by the organizations since there is no need to special measurements (pressure etc...) and signature simply scanned using usual used scanner in offices and this system will simply match with saved database [10].

1.1 Related Works

Berrin Yanikoglu et al [14] authors proposed online signature verification system mainly based Fourier descriptors. Feature extracted after apply pre-processing step which is done in two steps (Time normalization and Stroke concatenation) where the signature cropped and pre-processed to remove unneeded information and feature obtained by applying the Fourier descriptors extract strong features related to each other and provide additional dimension to the recognition by checking the pressurization of pen while signing on smart tab.

Loris Nanni et. al. [15] authors claims that the system extract global features using multi-matcher system that is used for verification of offline system this matcher split the verification to step into man y phases...
to obtain more accurate results where pre-processing step is simply done by applying thresholding (hashing), Prakash [16] a framework suggested for check signatures which is mainly work on the representation of symbolic signature which is done via examine global features combining with edge, authors claims that there system is beat all the other world element-based systems. Alisher Kholmatov et. al. [17] the proposed system work on many additional factors that can be very effective to the verification phase by checking the contrast of back focuses in the tested signature and organizing (mark directions) and contrast between focuses (successive). In [18] Harpreet Kaur used SURF as feature extraction that is used in an offline verification system of signature these features simply applied in neural network methods and use SUPPROT VECTO MACHINE (SVM) as matcher.

2. Proposed system
In this paper proposed system for offline signature verification and matching, this system composed from four main steps Figure 1, and algorithm (1) show that steps:

1. Pre-processing: the scanned image pre-processed to remove unnecessary information and to apply normalization for the signature images.
2. Feature extraction: features extracted from the normalized images using Fast Affine Invariant Image Matching (FAST) these feature will discard the angel and lightness.
3. Feature selection: genetic algorithm will be used to reduce the number of features by choosing only the strong features to be used in matching with features saved in the database.
4. Feature matching: SUPPROT VECTO MACHINE (SVM) used to provide supervised learning and, matching to obtain the matching result.

Figure 1. proposed system steps.

Figure 2. represent the flowchart of the proposed system:
Algorithm 1 proposed system algorithm.

| Step 1: Read signature image (x, y) |
| Step 2: FOR i=0 to (image size) |
| Preprocessing step: |
| Step 3: Otsu’s thresholding |
| Step4: Normalization |
| Step5: Morphological operation |
| Step6: Median filtering |
| Feature extraction step: |
| Step 5: extract features using FAST |
| Feature selection step: |
| Step 6: reduce number of features using genetic algorithm |
| Feature matching step: |
| Step 7: feature matching using SUPPROT VECTO MACHINE (SVM) and FAST |
| Step 8: END |

2.1 Pre-processing
In this step image which scanned by using known scanners and scanning techniques will probably contain noise which may affect the matching quality and noise if not be removed will probably defines as features. This step mainly contains internal steps to pre-process the image:

- **Otsu’s thresholding** (convert image to binary): this method was applied by using open-cv library to apply it, by simply choose thresholds that could be found between two peaks and select the middle if the number more than two.
- **Normalization**: image data will normalize in this phase to work on the contrast of the image by adjusting it using histogram stretching or shrinking as needed.
- **Morphological operation**: this used to process images (signature images) by shapes where usually the signature contain mathematical shapes and curves that form it, mainly Dilation and Erosion used where the Dilation represent the maximum value in image neighbour and the Erosion will find the minimum value in image neighbour. And since the image converted to binary using the Otsu’s thresholding then the maximum value will be one and the minimum value will be zero.
- **Median filtering**: applying the median as a noise removal to reduce the data and remove unwanted information from image, the concept of this filter is to order pixels and select the median which enhance the image and remove the noise effectively.

These phases’ application results shown in Figure 3.

2.2. Features extraction using Fast Affine Invariant Image Matching (FAST):
This feature extraction is done by simply apply set of transformation to images using affine methods the resulted data will simply comparable with the Scale Invariant methods like (SIFT and SURF) FAST used to compute the minimum discrete set of transformation before the comparison process applied and features obtained which made the entire process accurate in time and resources.
The resulted signature image will go through set of descriptors which is saved about half of the time of other descriptors with same accuracy and the features extracted represent good feature that can used to explain signature. The algorithm will usually work on the horizontal and vertical and global features.

**Figure 3.** pre-processing internal phases for the signature image (a: original image b: Otsu’s thresholding c: Normalization d: Morphological operation e: Median filter f: final output).

**Figure 4.** shows the features extracted by applying FAST.

**Figure 4.** feature extracted from images using FAST algorithm.

Features will enter to feature selection step to minimize the number of features and choose the strong ones.

### 2.3. Feature selection

This step is done by using genetic algorithm steps explained briefly in algorithm (2) where the strong features will be chosen by applying genetic algorithm. Features extracted will deals as a chromosome to the genetic algorithm. **Figure 3.** shows five output signature images where feature extracted from the outputs images and the repeated features in all images will chosen as a candidate central features and each central feature selected from these values will deal with the features data, each feature in the normalized signature image distance calculated to the central to get fitness data the strong connection to the central feature will applied to minimize the number of features and chose the better ones.

- Candidate selection criteria: best feature is only selected as an input to the genetic algorithm.
- number of candidates: 8*8 array of candidates
- valuation/cost functions: consistency of features to neighbor features
- type of chromosome encoding: real number
- crossover type: Single-point crossover, reproduction strategy: no reproduction applied
Algorithm 2 proposed feature selection using genetic algorithm.

| Step | Description |
|------|-------------|
| Step1: | set number of chromosome which is equal to number of strong features. |
| Step2: | select the strongest chromosome to be the central |
| Step3: | distance calculated to the other features from the central and considered as fitness. |
| Step4: | crossover applied to feature selection (best ones). |
| Step 5: | END |

Figure 5. shows features remaining after applying the genetic algorithm to the extracted features.

![Figure 5](image)

**Figure 5.** feature extract after applying genetic algorithm.

2.4. Feature matching

Support vector machine (SVM) is applied as a supervised learning classifier in the proposed system to ensure better classification and to learn the system to recognize the signature from database of signatures. The features obtained after applying the genetic algorithm to reduce the amount of data used is not linearly separable so the outcome of the genetic algorithm will fed to the Support vector machine (SVM) for detecting the original and the forgery signature and the matching of the classified data using FAST which is shown in **Figure 6.**

![Figure 6](image)

**Figure 6.** signature matching using strong features only.

3. Experimental result

The number of the datasets images saved in the database is 240 and the accuracy of the system is 87% which calculated be found the number of correct matching divided by the number of the total matches. **Table 1.** shows the features details that is saved in the database which is contain x1 and x2 represent the coordinate of the extracted features, sigma is the Maximum Compressive Stress; angle is the angle of the selected features and description of the feature itself.

The corresponding histogram and the remapping function after applying the four steps of the proposed system is shown in **Figure 7-8.**

The verification information of identification of owner of signature is loaded from the database after the verification process is complete (such as name, blood type ...etc), this can be used to show who is the person who do the sign in case of matching founded and show null information if there is no match.
Figure 7. Signature correspondence histogram.

Figure 8. Remapping to sample signed image.

Table 1. Features details (sample).

| $X_1$   | $Y_1$   | $\text{Sigma}_1$ | $\text{Angle}_1$ |
|---------|---------|-------------------|-------------------|
| 255.985 | 268.211 | 10.0488           | 188203            |
| 549.287 | 206.143 | 2.07153           | -1.78414          |
| 334.34  | 205.129 | 30.6663           | 2.86021           |
| 557.709 | 279.426 | 8.05597           | -1.816            |
| 284.351 | 187.033 | 4.95115           | -0.57109          |
| 542.833 | 318.928 | 5.0135            | 1.31486           |
| 258.336 | 234.157 | 2.40973           | 1.16213           |
Where x1 and x2 represent the coordinate of the extracted features, sigma is the Maximum Compressive Stress and angle is the angle of the selected features. System view is shown in figure below (Figure 9.)

4. Conclusion
In this paper a system proposed for verification and identification of offline signature. Scanned signature images need to be pre-processed before processing the data, the features obtained from any feature extraction method should be accurate and effective in this paper. FAST is used to obtain features from signature images and the data resulted is minimized via genetic algorithm by choosing the best features to use it in the verification and classification where SUPPORT VECTOR MACHINE (SVM) and FAST used as a classifier/matcher that is used to detect forgery and original signature. This system could be converted to verify online signature by adding a suitable entry pad and metrics to get data for the online verification to used it when feature extraction.

5. References
[1] M. Kayaoglu, B. Topcu, and U. Uludag, 2015, Biometric matching and fusion system for fingerprints from non-distal phalanges, arXiv:1505.04028.
[2] J.H. Shah, M. Sharif, M. Yasmin, S.L. Fernandes, 2017, Facial expressions classification and false label reduction using LDA and threefold SVM, Pattern Recognit. Lett. Published Online, ISSN 0167-8655.
[3] J.H. Shah, Z. Chen, M. Sharif, M. Yasmin, S.L. Fernandes, 2017, A novel biomechanics-based approach for person re-identification by generating dense colour sift salience features, J. Mech. Med. Biol. 17 (07).
[4] M. Sharif, S. Mohsin, M.Y. Javed, M.A. Ali, 2012, Single image face recognition using Laplacian of Gaussian and discrete cosine transforms, Int. Arab J. Inf. Technol. 9 (6) pp. 562–570.
[5] M. Sharif, A. Saad, 2012, Enhanced SVD based face recognition, J. Appl. Comput. Sci. Math. 6 (12) pp.49–53.
[6] M. Sharif, S. Mohsin, M.J. Jamal, M.Y. Javed, M. Raza, 2011, Face recognition for disguised variations using gabor feature extraction, Aust. J. Basic Appl. Sci. 5 (6), pp. 1648–1656.
[7] M. Sharif, K. Ayub, D. Sattar, M. Raza, S. Mohsin, 2012, Enhanced and fast face recognition by Hashing algorithm, J. Appl. Res. Technol. (JART) 10 (4), pp. 607–617.
[8] M. Sharif, J.H. Shah, S. Mohsin, M. Raza, 2013, Sub-holistic hidden Markov model for face recognition, Res. J. Recent Sci. 2 (5), pp. 10–14.
[9] V. Nguyen, M. Blumenstein, 2011, An application of the 2d Gaussian filter for enhancing feature extraction in off-line signature verification, in: Document Analysis and Recognition (ICDAR), International Conference, pp. 339–343.

[10] R. Kumar, J. Sharma, B. Chanda, 2012, Writer-independent off-line signature verification using surroundedness feature, Pattern Recognit. Lett. 33, pp. 301–308.

[11] J.F. Vargas, M.A. Ferrer, C. Travieso, J.B. Alonso, 2011, Off-line signature verification based on gray level information using texture features, Pattern Recognit. 44, pp.375–385.

[12] S. Khan, A. Dhole, 2014, A review on offline signature recognition and verification techniques, Int. J. Adv. Res. Comput. Commun. Eng. 3, pp. 6879–6882.

[13] A. Chugh, C. Jain, P. Singh, P. Rana, 2015, Learning approach for offline signature verification using vector quantization technique, in: Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India (CSI) Volume, 1, pp. 337–344.

[14] Sae-Bae, Napa, and Nasir Memon. 2014, Online signature verification on mobile devices, IEEE Transactions on Information Forensics and Security 9.6, pp. 933-947.

[15] Abaza, Ayman, et al. 2013, A survey on ear biometrics, ACM computing surveys (CSUR) 45.2.

[16] Plamondon, Réjean, Giuseppe Pirlo, and Donato Impedovo, 2014, Online signature verification.” Handbook of Document Image Processing and Recognition. Springer London, pp. 917-947.

[17] Parodi, Marianela, Juan C. Gomez, and Marcus Liwicki. 2012, Online signature verification based on Legendre series representation: Robustness assessment of different feature combinations, Frontiers in Handwriting Recognition (ICFHR), International Conference on. IEEE.

[18] Kaur, Harpreet, and Simarjeet Kaur, 2011, Disconnected Hindi Signature Recognition Using Surf Feature Extraction and Neural Networks Approach.