Detection and Extraction Features for Signatures Images via Different Techniques

F M Alsuhimat, F S Mohamad, M Iqtait

Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Kuala Terengganu, Malaysia

karaklove@yahoo.com

Abstract. Signature is one of the most important features to identify individuals. It represents a specific mark that includes handwritten characters or symbols. Also, signing takes place in a wide range of businesses, such as bank transactions and government documents so it provides a good way to maintain security, in biometric systems. Signature is used as a feature to identify the user by extracting a set of features. Over time, a number of techniques have been developed to identify and extract a set of features from the signature image. Although there are many of these techniques, there is a set of elements that determines the feasibility of using a particular technique, such as accuracy, computational complexity, and the time needed to extract features. In this paper, three widely used feature detection algorithms, SURF, BRISK and FAST, these algorithms are compared to calculate the processing time and accuracy for set of signatures correctly. Three techniques have been applied using (UTSig) dataset; the results showed that the BRISK algorithm got the best result among the feature detection algorithm in terms of accuracy and the FAST algorithm got the best result among the feature detection algorithm in terms of run time.

1. Introduction

A handwritten signature is used in many of the daily work of individuals in order to ascertain the identity of the individuals in carrying out a particular task. Therefore, it is necessary to provide systems that are able to maintain signatures and use them securely to identify individuals accurately. One of the most important problems with handwritten signatures is when someone impersonates our signature to steal our identity. In this case we need systems that can protect signatures and use them to identify individuals with a highly level of certainty.

A handwritten signature is defined as a means that includes letters, symbols, or as a nickname that is handwritten by the individual to carry out a range of applications, such as signing a contract or paying a bank check. In addition, a handwritten signature represents a procedure used by individuals to give approval for the implementation of a particular decision or to take specific steps [1].

Although the signature feature has a range of advantages that make it better than other biometric features, the process of identifying the signature contains some weaknesses, because of the different patterns of signatures that result from differences in the signature of the individuals each time, these differences occur because of a variety of factors, such as: personal emotions, lack of an individuals’
sense of stability, and environmental changes surrounding the individuals. In addition to that the occurrence of fraud in signing is easier than the occurrence in other biometric traits [2].

A signature recognition system is used for verifying signature and detects any forgery but before verification phase the signature went through some phases, like: normalization, feature extraction, and classification. These phases are very important to verify signature, because handwritten signature could differ according to the individual's behavior or position [3].

Moreover, the signature is a behavioral characteristic of individuals used in the field of biometrics systems in order to verify the identity of individuals, and with the increasing use of biometric features in the field of security, the signature appears as a biometric feature that provides a secure means of delegating individuals and ensuring their identity in legal documents. As well as the high level of acceptance by individuals to use this feature in the field of biometric systems compared to other biometric features, such as (hand geometry, iris scan, or DNA). All these reasons have led to an increase in the proliferation of signature recognition systems and the need for further developments on these systems.

In this paper, our objective is to study the features extraction phase. Therefore, three types of features extraction algorithms have been chosen, discussed and applied on signatures images, features are detected and extracted using SURF (Speeded-Up Robust Features), BRISK (Binary Robust Invariant Scalable Key points) and FAST (Features from Accelerated Segment). Various set of images of signatures have been used in order to calculate the comparison factors (accuracy and run time) for each algorithm. Also, matching features between first and second images were found, depending on this information of the comparison process between among three algorithms.

2. Related Work

The signature verification system aims at distinguishing between two categories: the original signature and the forged signature. In addition to the fact that the original signature of the individual itself contains a difference and contrast due to a number of factors, such as the signature that does not begin or end at the same point of time. The relative between signature elements (letters or symbols) varies each time the signature is made so the task of distinguishing and comparing signatures is difficult even for the same person.

The feature extraction is considered the second phase in biometric system. This phase involves the process of identifying and detecting a range of features in the image, whether signature, fingerprint or else, such as: width, length, and number of pixel, in order to compare biometric samples, identify and verify individuals. In signature recognition systems there are three types of features that can be extracted, global features, including height to width ratio of signature, gravity center and signature area. The second type is local features, including critical points and slant features, while the third type, a geometric feature, represents the local and global features of the signature [4].

The feature extraction phase in the signature recognition systems aims at identifying a set of original sample features in order to compare them with user sample features for verification purposes. There are two types of features: first type is function features including speed, compression and position. Such features will be used in verification systems of the signature online. The second type is the parameter features, which is divided into two local parameters and global parameters [5].

According to [6], the effectiveness and efficiency of signature recognition systems depends mainly on the stage of extracting the features so it is necessary that the techniques used at this stage are efficient and high speed. In addition, the features that are extracted must be able to distinguish between the real signature and counterfeit.

The feature extraction process is based on minimizing the dimensions of the original signature image and extracting a set of hidden parameters in the signature image. These features are selected with great
accuracy in order to make the distinction between the original signature and the counterfeit easier. These features include:

Local shape descriptors: represent a wide group of global parameters, such as high pressure points, and context shape [7]. Chain code: process of coordinate a start point and determine the directions of the following points till reaching the start point again [8]. Graphometric features: represent a set of intrinsic traits from an individual handwriting pattern, which may be employed for signature recognition, such as: curvature, pressure and histogram features including number of pen pixels in the circular sector [9]. Interior stroke distributions: this trait represents the process of calculation the number of stroke that distributed in the image [10].

3. Overview of Method

In this section, the techniques that are used for feature detection and comparison process are described briefly. Also, the algorithm used for each technique and feature matching has been described.

3.1 SURF Algorithm

Speed Up Robust Features (SURF), a fast and powerful algorithm used to detect and extract features, was developed by [11]. This algorithm relies on Hessian matrix which has good accuracy and performance. In image $(F)$, the given point for this image is $x = (x, y)$ and Hessian matrix $H(x, \sigma)$ in $x$ at scale $\sigma$, it can be defined as:

$$H(x, \sigma) = \begin{bmatrix} L_{xx}(x, \sigma) & L_{xy}(x, \sigma) \\ L_{yx}(x, \sigma) & L_{yy}(x, \sigma) \end{bmatrix}$$

(1)

Where $L_{xx}(x, \sigma)$ is the result of the convolution of the second order derivative of Gaussian filter $\frac{\partial^2}{\partial x^2} g(\sigma)$ with the image $(F)$ in point $x$, and same for $L_{xy}(x, \sigma)$ and $L_{yx}(x, \sigma)$. Figure (2) show $y$-direction and $xy$-direction in second order derivative of Gaussian filter.

3.2 FAST Algorithm

Features from Accelerated Segment Test (FAST) relies on a different approach to other algorithms, based on an automated learning approach that adapts for processing, by identifying a set of few points within the range of interests and rejecting points that have no benefit [12].

In 1998, FAST algorithm was presented as a new technique for corner detector [13]. Also, FAST needs a set of criteria in order to allow matching feature point from corner detector, these criteria as follow:

3.3 BRISK Algorithm

Binary Robust Invariant Scalable Key-points (BRISK) is characterized by the fact that computations are significantly less complex, its use distance rather than Euclidean distance and it is faster than the Fast algorithm and the SURF algorithm.

According to [14] BRISK is a new algorithm designed to identify key points that match the description by evaluating this algorithm shows that the performance of high quality compared to calculations less complex. In addition, the algorithm BRISK has faster implementation than the Surf algorithm.

3.4 Dataset

The comparison process of three algorithms implemented on a set of signatures images from (UTSig) dataset. This dataset has "(115) classes containing: (27) genuine signatures; (3) opposite-hand signed samples and (42) simple forgeries. Each class belongs to one specific authentic person. UTSig has 8280 images collected from undergraduate and graduate students of University of Tehran and Sharif University of Technology, signatures were scanned with 600 dpi resolution and stored as 8-bit Tiff files" [15, p1].
3.5 Comparison Process

The comparison of the three algorithms was performed by calculating the run time and accuracy of each algorithm. The following equation was used to calculate the accuracy of each algorithm:

\[
\frac{1}{n} \sum_{i=1}^{n} \frac{I_m}{I_{ex}} \times 100
\]  

Where: \(I_m\) = Total no. of matched features, \(I_{ex}\) = Total no. of extracted features from original image, \(n\) = Total no. of images used.

4. Results and Discussions

First, the comparison process for the three algorithms was done on a single image. After that the number of images increased each time at a rate of (1, 4, 8, 10) images. Table 1 shows the results of comparison process for the three feature detection algorithms depending on the accuracy and run time for each algorithm; Figure (1) shows both original and destroyed image used to test the three algorithms, Figure (2) shows the result of SURF algorithm, for detection features process and matching features process, while Figure (3) shows the result of BRISK algorithm, for detection features process and matching features process, and Figure (4) shows the result of FAST algorithm, for detection features process and matching features process.

| No. of Images | Algorithm | Extracted Features | Matched Features | Run Time (sec) | Accuracy (%) |
|---------------|-----------|--------------------|------------------|---------------|--------------|
| 1             | SURF      | 807                | 90               | 0.38          | 11.15        |
|               | BRISK     | 285                | 49               | 0.25          | 17.19        |
|               | FAST      | 420                | 28               | 0.17          | 6.67         |

Table 1. Comparison of different feature detection algorithms.
| No. of Images | Algorithm | Extracted Features | Matched Features | Run Time (sec) | Accuracy (%) |
|---------------|-----------|--------------------|------------------|---------------|--------------|
|               |           | Original Image     | Distorted Image  | Original Image | Distorted Image |               |               |
| 4             | SURF      | 561                | 574              | 135           | 135           | 0.20          | 50.13         |
|               | BRISK     | 180                | 152              | 27            | 27            | 0.14          | 31.25         |
|               | FAST      | 245                | 725              | 20            | 20            | 0.12          | 8.16          |
| 8             | SURF      | 712                | 531              | 86            | 86            | 0.22          | 32.83         |
|               | BRISK     | 244                | 279              | 47            | 47            | 0.14          | 52.35         |
|               | FAST      | 340                | 1012             | 32            | 32            | 0.12          | 9.41          |
| 10            | SURF      | 859                | 905              | 135           | 135           | 0.26          | 46.03         |
|               | BRISK     | 311                | 295              | 53            | 53            | 0.15          | 49.91         |
|               | FAST      | 330                | 1505             | 28            | 28            | 0.14          | 24.85         |

From the Table 1 we can note that when the comparison process has been done on (one, eight and ten) images, the accuracy of BRISK algorithm is better than the other two algorithms. When the comparison process has been done on (four) images, the accuracy of SURF algorithm is better than the other two algorithms as in Figure (5). In addition, for the run time we can note that the best run time was for FAST algorithm, as in Figure (6).

![Figure 5. Accuracy vs number of images](image)

![Figure 6. Run Time vs number of images](image)

Therefore, the number of images play an important role in the comparison process between the three algorithms, where BRISK algorithm got highest accuracy among other algorithm in the cases that contains (one, eight and ten) images but when we test four images, the SURF algorithm get the highest accuracy. This means that SURF algorithm can get highest accuracy when it tests four images, while the BRISK algorithm can get best accuracy at many cases (one, eight and ten) images.

On the other hand, the FAST algorithm in all cases got the lowest accuracy, but it got the best run time at all case. Also, the above table shows that run-time is decreased each time the number of images is increased for BRISK and FAST algorithms.

### 5. Conclusions

In this paper the comparison process of SURF, BRISK and FAST feature detection algorithms has been done on a set of signature image from (UTISG) dataset in order to measure performance through calculating the run time and accuracy for each algorithm. The three algorithm used here are popular algorithms used for feature detection, where the main elements to choose better feature detection algorithm are computational complexity and accuracy. The comparison process is done between the
original images and the distorted images among all algorithms. After that the run time and accuracy calculated for each algorithm in order to find the best feature detection algorithm. The experimental results showed that, the BRISK algorithm got the best result among the feature detection algorithm in terms of accuracy and the FAST algorithm got the best result among the feature detection algorithm in terms of run time, also the results showed that the number of images have effect on the accuracy and run time of the algorithm.

For future work other feature detection algorithms will be test with the same number of images, also change and increase the number of images will be test using these three algorithm and different algorithm, in order to find the best future detection algorithm for signature images, and the suitable number of images among all feature detection algorithms.

6. References
[1] Fotak T, Baca M and Koruga P 2011 Wseas Transactions on Signal Processing 4 117-29
[2] Daqrouq K, Sweidan H, Balamesh A and Ajour M 2017 Entropy 19 1-20
[3] Jahan T, Anwar S and Al-Mamun A 2015 Global J. of Computer Science and Technology: F Graphics & Vision 15 1-7
[4] Gunjal S, Dange B and Brahmane A 2016 International Journal of Computer Applications 141 6-12.
[5] Hafemann L, Sabourin R and Oliveira L 2017 Pattern Recognition 70 163-76
[6] Bhosale V and Karwankar A 2013 International Journal of Computational Engineering Research 3 8-12
[7] Bonilla J, Ballester M, Gonzalez C and Hernandez J 2009 Proceedings of the 2009 10th International Conference on Document Analysis and Recognition, (Washington: IEEE Computer Society) 126-130.
[8] Bharathi R K and Shekar B H 2013 International Conference on Advances in Computing, Communications and Informatics (Mysore: IEEE conference) 2063-68
[9] Parodi M, Gomez J C and Belaid A 2011 International Conference on Document Analysis and Recognition Document Analysis and Recognition (Beijing: IEEE conference) 1289-93
[10] Narayana M, Annapurna L and Mounika K 2017 IJECET 8 120-8
[11] Bay H, Ess A, Tuytelaars T and Gool L 2008 International Journal of Computer Vision and Image Understanding 110 346-59
[12] Ghosh P, Pandey A and Pati U 2015 ACCENTS Transactions on Image Processing and Computer Vision 1 p 1-7
[13] Trajkovic M and Hedley M 1998 Image and Vision Computing 16 75-87
[14] Leutenegger S, Chli M and Siegwart R Y 2011 Computer Vision (Barcelona: IEEE conference) 2548-55
[15] Soleimani A, Fouladi K and Araabi B 2016 IET Biometrics 6 1-8

Acknowledgement
This study is part of the project under Fundamental Research Grant Scheme (FRGS): RR227. We would like to acknowledge Ministry of Higher Education Malaysia and Universiti Sultan Zainal Abidin, Malaysia for supporting and funding this study.