

Detection and Feature Extraction for Images Signatures

Fatma Susilawati Mohamad*, Fadi Mohammad Alsuhiat, Mohamad Afendee Mohamed, Mumtazimah Mohamad, Azrul Amri Jamal

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

*Corresponding author E-mail: fatma@unisza.edu.my

Abstract

The signing process is one of the most important processes used by organizations to ensure the confidentiality of information and to protect it against any unauthorized penetration or access to such information. As organizations and individuals enter the digital world, there is an urgent need for a digital system capable of distinguishing between the original and fraud signature, in order to ensure individuals authorization and determine the powers allowed to them. In this paper, three widely used feature detection algorithms, HARRIS, BRISK (Binary Robust Invariant Scalable Keypoints) and FAST (Features from Accelerated Segment), these algorithms are compared to calculate the run time and accuracy for set of signature images. Three techniques have been applied using (UTSig) dataset; the experiment consisted of four phases: first, applying the techniques on one image, then on four images, then on eight images, finally applying the techniques on ten images where time and accuracy were calculated for each algorithm in the all phases. 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.

Keywords: Feature Extraction; Feature Detection; HARRIS; FAST; BRISK.

1. Introduction

A handwritten signature is an individual's personal skill which includes a set of marks and characters drawn in a particular language, the signature is often used to allow persons to perform certain transactions such as banking transactions where the signature defines the permitted validity of the individual through making sure that his signature is the forged or genuine signature.

A handwritten signature contains different elements such as letters, symbols and nickname where all these elements is handwritten by the individual in order to implement a set of transactions like paying a bank check and for give a permission or approval to carry out a particular decision [1].

In present, signature detection and identifications is playing main role in almost all the field where secrecy and security are the main concerns for all individuals and countries. Also, using signature detection can help in determine the identity of individuals and their authorization for do a specific job [2].

A signature recognition system is a way to verify signature in order to detect any forgery, before get the final result from verification phase, the recognition process consists of a set of stages include normalization, feature extraction and classification, these three stages are very important to verify signature because the handwritten signature can vary each time depending on the behavior and position of the individual [3]. Figure 1 illustrates example of different patterns of signatures for the same individual.

The second phase in signature recognition systems is features extraction phase, which include the process of determine and detecting a set of features in the signature image, such as: number of pixel, width, corner and length where this phase consider an important because it's the base of the process of compare biometric samples and verify individuals [4].



Fig. 1: Example of different patterns of signature

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.

The feature extraction phase aims at identifying a group of original image features in order to verify purposes through compare them with user sample features. There are two types of features: first type is function features including speed, compression and position such features used in verification systems of the signature online while the second type is the parameter features which is divided into two types, local parameters and global parameters [4]. The feature extraction phase is relying on determine image features with great accuracy through minimize the dimensions of the original image then extract a group of hidden traits in the image, in order to facilitate the process of differentiation between original and fake signatures.

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 BRISK (Binary Robust Invariant Scalable Key points), FAST (Features from Accelerated Segment) and HARRIS. 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 images were found for each algorithm.

2. Methodology

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.

2.1. 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 [6].

In 1998, FAST algorithm was presented as a new technique for corner detector [7]. Also, FAST needs a set of criteria in order to allow matching feature point from corner detector, these criteria as follow.

2.1.1. Consistency

This criterion means that the detected points should be characterized as not sensitive to any noise change. This means that they do not move when multiple images are taken from the same scene.

2.1.2. Accuracy

This criterion means that the detection of corners should be closest to the correct positions.

2.1.3. Speed

This criterion means that detection is required as quickly as possible, where the process of detect corners not useful unless they are fast. Figure 2 shows test of FAST algorithm.

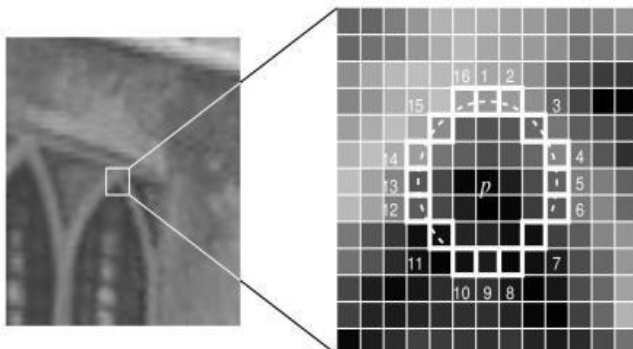


Fig. 2: Fast algorithm

2.2. 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 [8], 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. Figure 3 shows BRISK sampling pattern.

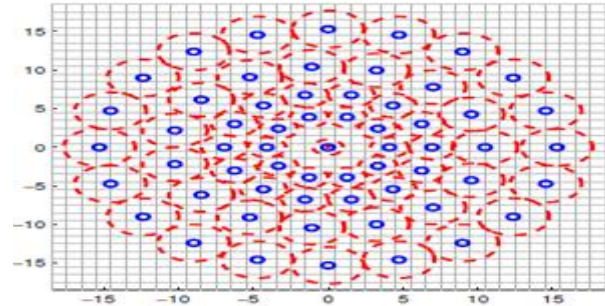


Fig. 3: Brisk sampling pattern

From the above figure, we can see that they consist of a binary series and the comparison tests between the points are simple and that the neighborhood points are in specific circles with one center and equal spacing.

BRISK is easily scalable for faster execution by reducing the number of sampling-points in the pattern at some expense of matching quality, which might be affordable in a particular application. Moreover, scale and/or rotation invariance can be omitted trivially, increasing the speed as well as the matching quality in applications where they are not needed [8].

In this algorithm, the strength of gradient between pairs is computed using the following equation:

$$g(\mathbf{p}_i, \mathbf{p}_j) = (\mathbf{p}_j - \mathbf{p}_i) \cdot \frac{I(\mathbf{p}_j, \sigma_j) - I(\mathbf{p}_i, \sigma_i)}{\|\mathbf{p}_j - \mathbf{p}_i\|^2}$$

2.3. HARRIS Algorithm

The Harris corners algorithm employs as key-points based method for detect the forgery in the region. In addition, Harris corner detector algorithm determine static features to geometric transformations, where its used as a key-points operation in order to represent the internal structure of identical image areas [9].

Also, Harris corner detector algorithm is an invariant rotation technique that determines the corners of the image [10]. "Harris corner detection is based on the second moment auto correlation matrix. This matrix describes the Gradient distribution of input images at point x , weighted by Gaussian $G(x, \sigma)$ as the following [9]:

$$M = G(x, \sigma) \begin{bmatrix} I_x^2(x, \sigma) & I_x I_y(x, \sigma) \\ I_x I_y(x, \sigma) & I_y^2(x, \sigma) \end{bmatrix}$$

where I_x^2 , I_y^2 , I_x , and I_y are square derivatives of input image (I). Figure 4 shows test of HARRIS algorithm.

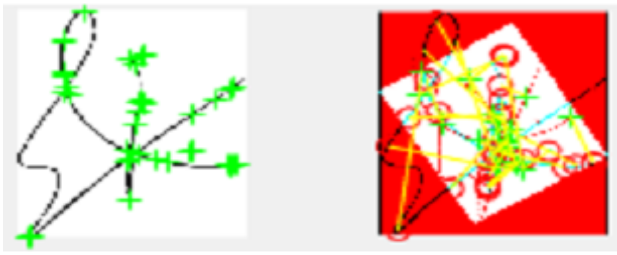


Fig. 4: Harris algorithm

2.4. 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 [10].

2.5. 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:

$$\frac{1}{n} \sum_{i=1}^n \frac{I_m}{I_{ex}} * 100$$

where I_m = Total no. of matched features, I_{ex} = Total no. of extracted features from original image and n = Total no. of images used.

3. Results and Discussion

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 5 shows both original and destroyed image used to test the three algorithms.

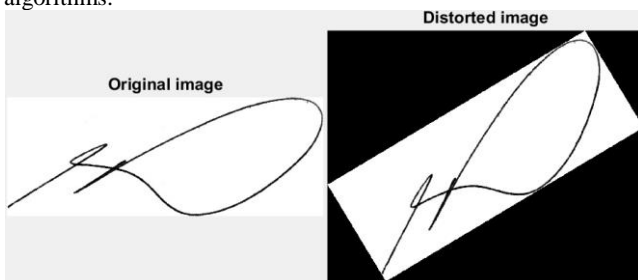


Fig. 5: Original and Destroyed image used in the comparison process

Figure 6 shows the result of BRISK algorithm, for detection features process and matching features process.

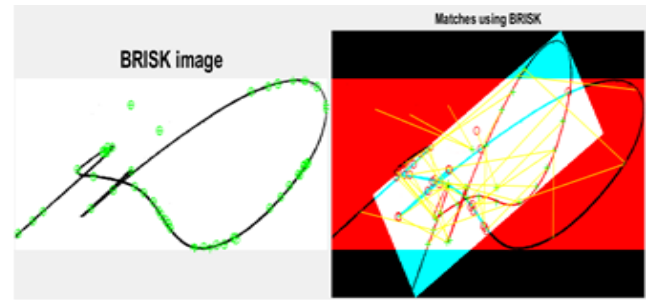


Fig. 6: Detection and matching features process for brisk algorithm

Figure 7 shows the result of FAST algorithm for detection features process and matching features process.

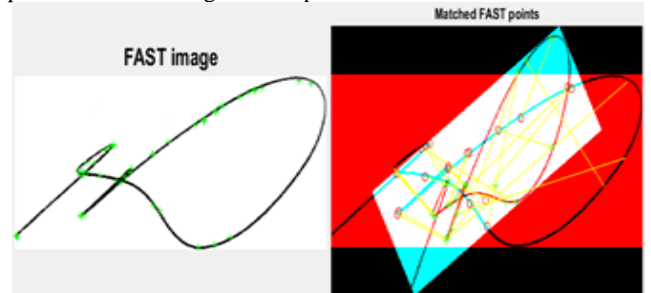


Fig. 7: Detection and matching features process for fast algorithm

Figure 8 shows the result of HARRIS algorithm, for detection features process and matching features process.

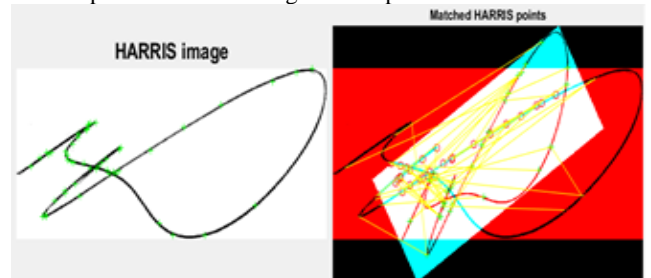


Fig. 8: Detection and matching features process for harris algorithm

From the above table, we can note that when the comparison process has been done on all cases (one, four, eight and ten) images, the accuracy of BRISK algorithm is better than the other two algorithms (HARRIS and FAST) as in Figure 9.

In addition, for the run time we can note that the best run time was for FAST algorithm when the comparison process has been done on all cases (one, four, eight and ten) images as in Figure 10.

Also, we can note that, BRISK algorithm got the second best run time and the best accuracy among three algorithms that's mean BRISK algorithm best than other algorithms. In addition, we point that the accuracy of BRISK algorithm has a positive relationship with the number of the image where we note that increasing the number of images each time leads to increased accuracy ratio of BRISK algorithm, in contrast to other algorithms where accuracy has increased in some cases and in other cases has decreased.

On the other hand, the FAST algorithm and BRISK algorithm got their highest run time when the comparison process has been done on (one) image. After that, the run time for both algorithms dropped once in the case of (four) images and then remained constant.

Table 1: Comparison of different feature detection algorithm

No. of Images	Algorithm	Extracted Features		Matched Features		Run Time (sec)	Accuracy (%)
		Original Image	Distorted Image	Original Image	Distorted Image		
1	HARRIS	527	944	29	29	0.44	5.50
	BRISK	337	260	39	39	0.15	11.57
	FAST	452	979	17	17	0.13	3.76
4	HARRIS	329	948	21	21	0.43	13.30
	BRISK	180	152	27	27	0.14	31.25
	FAST	245	725	20	20	0.12	17.01
8	HARRIS	485	699	45	45	0.40	25.22
	BRISK	160	182	21	21	0.14	35.67
	FAST	240	729	15	15	0.12	16.99
10	HARRIS	544	764	26	26	0.39	14.0
	BRISK	196	119	36	36	0.14	53.80
	FAST	275	640	24	24	0.12	25.56

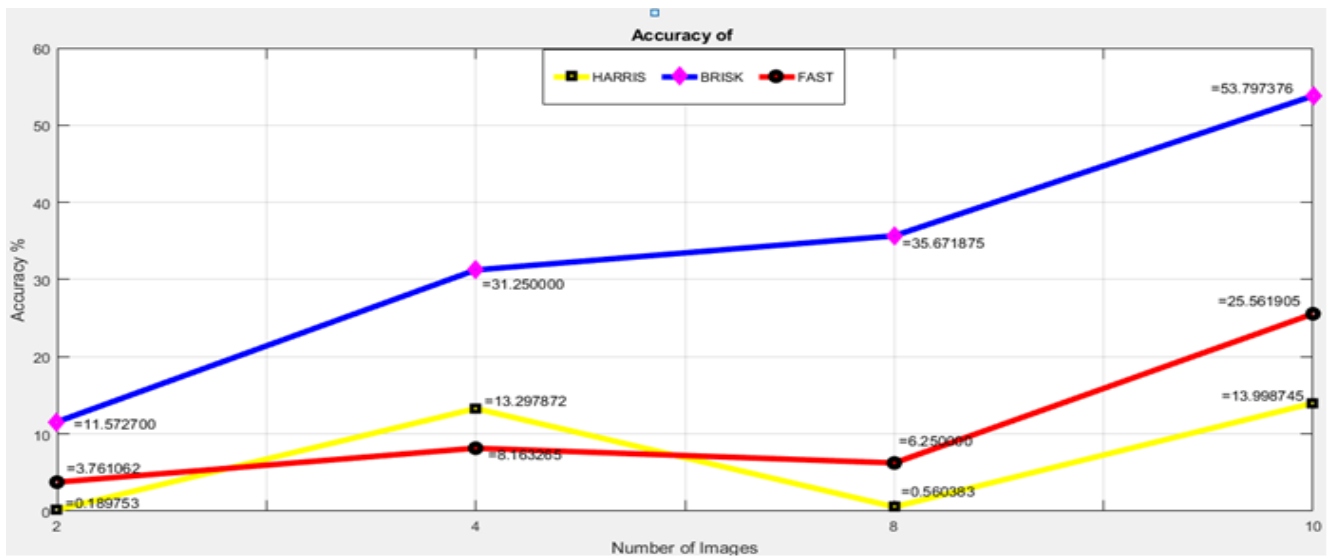


Fig. 9: Accuracy versus number of images

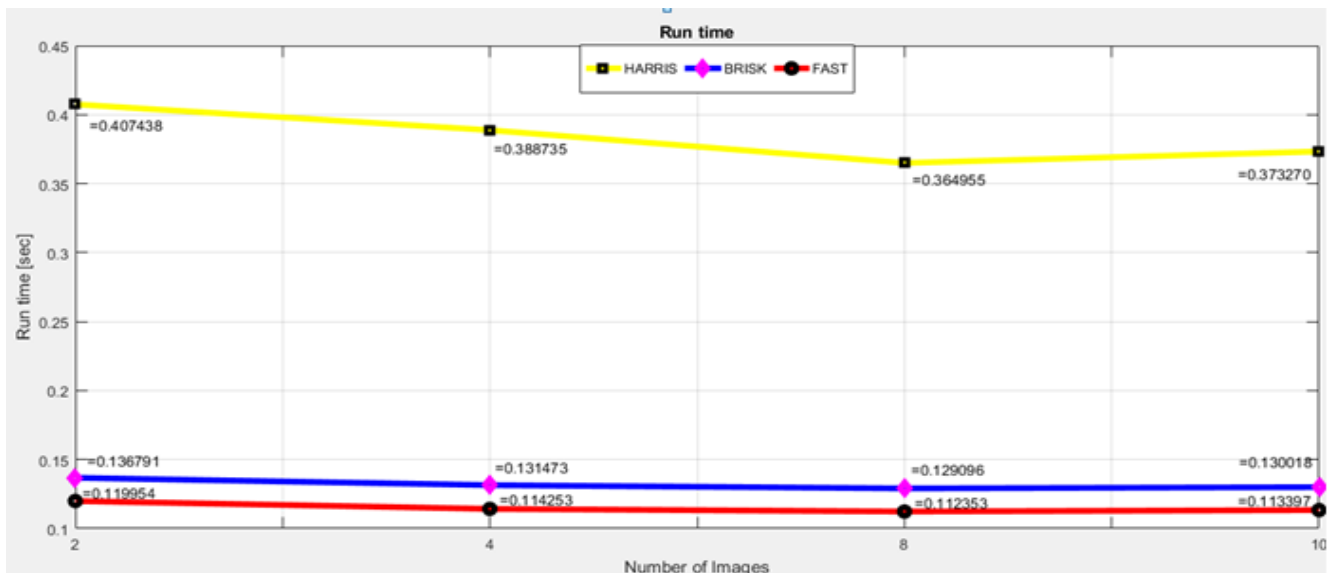


Fig. 10: Run time versus number of images

4. Conclusion and Future Works

In this paper, the comparison process of HARRIS, BRISK and FAST feature detection algorithms have 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 origi-

nal 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.

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.

References

- [1] Fotak T, Baca M, Koruga P. Handwritten signature identification using basic concepts of graph theory. *WSEAS Transactions on Signal Processing*. 2011, 4(7): 117-129.
- [2] Daqrouq K, Sweidan H, Balamesh A, Ajour M. Off-Line Handwritten Signature Recognition by Wavelet Entropy and Neural Network. *Entropy*. 2017, 19(6): 1-20.
- [3] Jahan T, Anwar S, Al-Mamun A. A Study on Preprocessing and Feature Extraction in offline Handwritten Signatures. *Global Journal of Computer Science and Technology: F Graphics and Vision*. 2015, 15(2): 1-7.
- [4] Gunjal S, Dange B, Brahmane A. Offline Signature Verification using Feature Point Extraction. *International Journal of Computer Applications*. 2016, 141(14): 6-12.
- [5] Hafemann L, Sabourin R, Oliveira L. Learning features for offline handwritten signature verification using deep convolutional neural networks. *Pattern Recognition*. 2017, 70(1): 163-176.
- [6] Ghosh P, Pandey A, Pati U. Comparison of Different Feature Detection Techniques for Image Mosaicing. *ACCENTS Transactions on Image Processing and Computer Vision*. 2015, 1(1): 1-7.
- [7] Trajkovic M, Hedley M. FAST corner detector. *Image and Vision Computing*. 1998, 16(2): 75-87.
- [8] Leutenegger S, Chli M, Siegwart R. BRISK: Binary Robust Invariant Scalable Key points. *Proceedings of the IEEE International Conference on Computer Vision*, 2011.
- [9] Uliyan D, Jalab H, Abdul Wahab, A, Sadeghi S. Image Region Duplication Forgery Detection Based on Angular Radial Partitioning and Harris Key-Points. *Symmetry*. 2016, 8(62): 1-19.
- [10] Patil P, Chavan M. A Comparative Analysis of Image Stitching Algorithms Using Harris Corner Detection and SIFT Algorithm. *International Journal of Engineering Research and Technology*. 2017, 10(1): 482-486.
- [11] Soleimani A, Fouladi k, Araabi B. UTSig: A Persian offline signature dataset. *IET Biometrics*. 2016, 6(1): 1-8.