Off-line Signature Verification using G-SURF

Author

Pal, Srikanta, Chanda, Sukalpa, Pal, Umapada, Franke, Katrin, Blumenstein, Michael

Published

2012

Conference Title

Proceedings of the 2012 12th International Conference on Intelligent Systems Design and Applications (ISDA)

DOI

https://doi.org/10.1109/ISDA.2012.6416603

Off-line Signature Verification using G-SURF

Srikanta Pal[a], Sukalpa Chanda[b], Umapada Pal[c], Katrin Franke[b], Michael Blumenstein[a]

[a] School of Information and Communication Technology, Griffith University, Gold Coast Australia;
[b] Department of Computer Science and Media Technology, Gjøvik University College, Norway.
[c]Computer Vision and Pattern Recognition Unit, Indian Statistical Institute, Kolkata, India
Email id: srikanta.pal@griffithenu.edu.au

Abstract— **In the field of biometric authentication, automatic signature identification and verification has been a strong research area because of the social and legal acceptance and extensive use of the written signature as an easy method for authentication. Signature verification is a process in which the questioned signature is examined in detail in order to determine whether it belongs to the claimed person or not. Signatures provide a secure means for confirmation and authorization in legal documents. So nowadays, signature identification and verification becomes an essential component in automating the rapid processing of documents containing embedded signatures. Sometimes, part-based signature verification can be useful when a questioned signature has lost its original shape due to inferior scanning quality. In order to address the above-mentioned adverse scenario, we propose a new feature encoding technique. This feature encoding is based on the amalgamation of Gabor filter-based features with SURF features (G-SURF). Features generated from a signature are applied to a Support Vector Machine (SVM) classifier. For experimentation, 1500 (50x30) forgeries and 1200 (50x24) genuine signatures from the GPDS signature database were used. A verification accuracy of 97.05% was obtained from the experiments.**

Keywords- Part-based character recognition, Document Analysis, Signature Verification, SURF, Support Vector Machine, Off-line system.

I. INTRODUCTION

The field of biometrics is a significant area of study as it offers many advantages over more commonly-used authentication methods such as photo ID cards, magnetic strip cards etc. Nowadays, biometric technologies are increasingly and more frequently being used to ensure identity verification. Signatures often include complex geometric patterns that construct them a relatively secure means for authorization in high security environments. For historical reasons, the handwritten signature continues to be the most commonly accepted form of transaction confirmation, as well as being used in civil law contracts, acts of volition, or authenticating one's identity. Signature verification has been a topic of intensive research during the past several years due to the important role it plays in numerous areas, including in financial applications.

The goal of a signature authentication system is to verify the identity of an individual based on an analysis of his or her signature through a process that discriminates a genuine signature from a forgery. The verification of human signatures is particularly concerned with the improvement of the interface between human-beings and computers. Signature verification has been extensively studied because of its various important applications in banking, credit card validation, security systems etc. In general, handwritten signature verification can be categorized into two kinds: on-line verification and off-line verification. On-line verification requires a stylus and an electronic tablet connected to a computer to capture dynamic signature information [10]. Off-line verification, on the other hand, deals with signature information which is in a static format [14-15]. Since the on-line approach can acquire more information than the off-line one, the latter is certainly more difficult to deal with.

Handwritten signatures are considered as complete images with a special distribution of pixels, and a particular writing style. They are not considered as collections of letters and words [16]. A person's signature may change radically during their lifetime. Great inconsistency can even be observed in signatures according to country, habits, psychological or mental state, physical and practical conditions [17].

There has been a substantial amount of work in the area involving off-line signature verification. In [18], Plamondon and Lorette provided a thorough survey of automatic handwritten signature verification and writer identification. Their survey covered both on-line and off-line approaches, and especially focused on preprocessing techniques, feature extraction methods, comparison processes and performance evaluation. Ramachandra et al. [7] proposed an off-line signature verification system based on a cross-validation principle and graph matching. Schafer and Viriri [12] presented an off-line signature verification system based on the combination of feature sets. Some extracted features were: Aspect ratio, centroid feature, four surface features, six surface features, number of edge points, transition features etc. The verification of signatures was accomplished using the Euclidean distance classifier. Justino et al. [13] also introduced an off-line signature verification system based on Hidden Markov Models (HMMs) to detect random, casual, and skilled forgeries. Three features: a pixel density feature, a pixel distribution feature and an axial slant feature were extracted from a grid segmentation scheme. Though a lot of work has been undertaken on signature verification, the research in the

978-1-4673-5119-5/12/$31.00 ©2012 IEEE

literature primarily assumes that the whole signature image is available, which might not be the case when dealing with signatures on document fragments. This problem could be addressed using a key-point based feature extraction technique. In this paper we propose a system for signature verification using a novel G-SURF based feature extraction method. Our feature extraction method is an amalgamation of Gabor-filter based features along with SURF (Speeded Up Robust Feature) features.

The rest of the paper is arranged as follows. The signature verification concept is discussed in Section II. The different types of verification errors and forgeries are described in Section III. In Section IV, we describe our feature extraction method along with a logical explanation of its utility for our objective. We describe our experimental setup with some information on our dataset in Section V. In Section VI, we provide a brief discussion on the classifier employed. Results and discussion on various experiments undertaken are reported in Section VII. Finally, Section VIII provides a comparison of the techniques and conclusions are drawn in Section IX.

II. SIGNATURE VERIFICATION CONCEPT

In general to deal with the problem of off-line/on-line signature verification, researchers have investigated a commonly used approach which is based on two different patterns of classes: class 1 and class 2. Here class 1 represents the genuine signature set, and class 2 represents the forged signature set.

Usually two types of errors are considered in a signature verification system. The False Rejection, which is called a Type-1 error and the False Acceptance, which is called a Type-2 error. So there are two common types of error rates: False Rejection Rate (FRR) which is the percentage of genuine signatures treated as forgeries, and False Acceptance Rate (FAR) which is the percentage of forged signatures treated as genuine.

III. TYPES OF FORGERIES

There are usually three different types of forgeries to take into account. According to Coetzer et al. [19], the three basic types of forged signatures are indicated below:

1. Random forgery. The forger has no access to the genuine signature (not even the author's name) and reproduces a random one.
2. Simple forgery. The forger knows the author's name, but has no access to a sample of the signature.
3. Skilled forgery. The forger has access to one or more samples of the genuine signature and is able to reproduce it.

But based on the various skilled levels of forgeries, it can also be divided into six different subsets. The paper [20] shows various skill levels of forgeries and these are shown below.

1. A forged signature can be another person's genuine signature. Justino et al. [21] categorized this type of forgery as a Random Forgery.
2. A forged signature is produced with the knowledge about the genuine writer's name only. Hanmandlu et al. [22] categorized this type as a Random Forgery whereas Justino et al. [21] categorized this type as a Simple Forgery. Weiping et al. categorized this type as a Casual Forgery [23].
3. A forged signature imitating a genuine signature's model reasonably well is categorized as a Simulated Forgery by Justino et al. [21].
4. Signatures produced by inexperienced forgers without the knowledge of their spelling after having observed the genuine specimens closely for some time are categorized as Unskilled Forgeries by Hanmandlu et al. [22].
5. Signatures produced by forgers after unrestricted practice by non-professional forgers are categorized as Simple Forgery/Simulated Simple Forgery by Ferrer et al. [24], and a Targeted Forgery by Huang and Yan [25].
6. Forgeries which are produced by a professional imposter or person who has experience in copying Signatures are categorized as Skilled Forgeries by Hanmandlu et al. [22].

IV. FEATURE EXTRACTION USING G-SURF

Key-point based techniques can be used for signature matching/verification, when a part of the query signature is missing. Most prominent key-point based feature encoding techniques are SIFT and SURF. But the inherent property of very local shape description of those methods makes it less effective if applied directly to a signature verification scenario. This is due to the fact that none of the key-point descriptors will take into account the global shape of the whole signature; neither do they consider their relative locations with respect to other key-points in the same character image. Earlier research shows that a global shape description should be added to each of the key-point feature descriptors in order to increase performance in character recognition [3, 6]. We propose to use Gabor filter-based features to accomplish the task of adding global shape context with SURF feature descriptors. This technique enables us to embed global shape information with every key-point by simply using one of the pieces of information (dominant orientation) about the key-point.

A. Feature computation for SURF

SURF (Speeded Up Robust Feature) is a robust feature extraction method, first presented by Bay et al. [1][27]. The SURF algorithm is composed of mainly two parts: first, we detect key-point. Second, we perform key-point description. Both of these parts rely on a scale-space representation and first and second order differential operators. The originality

of the SURF method is that these operations are speeded-up by the use of an *integral image* and *box filters* techniques [28]. Details about SURF can be found in [1]. Using SURF we can get a fast interest point detector and descriptor and at the same time (a) maintain comparable performance with other detectors; (b) with higher chances of finding same key-points under different viewing conditions. The basic algorithm to compute SURF features can be described in following steps [28]:

- First, we need to compute an integral image with respect to an input image.
- Key-points detection :
  - Then using box-filters we need to compute the discrete Hessian operator at several scales.
  - After that we need to compute the local *maxima* of the Hessian determinant operator applied to the scale-space in order to select key-point candidates.
  - Using quadratic interpolation, we need to refine corresponding key-points location.
  - We should store all key-points along with its Laplacian sign.
- Finally, constructing the local feature descriptor involves:
  - Calculating the dominant orientation of each key-point.
  - Final computation of the descriptor corresponding to the scaled and oriented neighborhood of the key-points.

Essentially the Haar wavelet responses in a square area centering at key-point coordinate are computed, which is used as final feature descriptor [27]. The orientation of the square area is set to be aligned with the dominant orientation of the key-point.

An example of key-points generated in one of our sample signature images is shown in Figure 1.

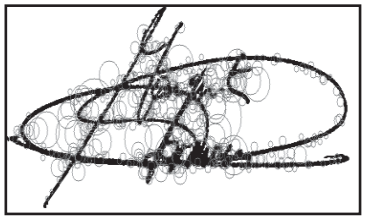


Figure 1. Example of a processed signature with key-points marked in circles.

B. Gabor features

A two-dimensional Gabor filter in the spatial and frequency domain can be defined by the following formula:

$$G(x, y, \lambda, \theta, \psi, \sigma, \gamma) = \exp\{(x'^2 + \gamma^2 y'^2)/2\sigma^2\} \cos(2\pi x'/\lambda + \psi)$$

Where,

$$x' = x\cos\theta + y\sin\theta$$

$$y' = -x\sin\theta + y\cos\theta$$

In this equation, λ represents the wavelength of the cosine factor, θ represents the orientation of the normal to the parallel stripes of a Gabor function, ψ is the phase offset, σ is the sigma of the Gaussian envelope and γ is the spatial aspect ratio, and specifies the ellipticity of the support of the Gabor function. We obtained the best results with σ set to $2*\pi$ and spatial frequency set to $2^{1/2}$.

C. G-SURF feature computation

After the key-points are detected from a signature we perform a size normalization of the signature image into 50 x 50 pixels. Then for every key-point we do the following:

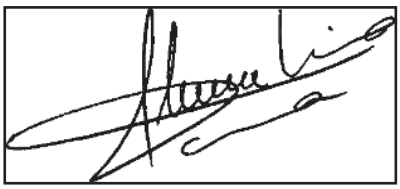
a) Compute the Gabor filter response on that size normalized image (50 x 50) with orientation of the Gabor's filter set equal to the dominant orientation of that key-point. As a result we obtained 2500-dimensional Gabor filter-based features from each key-point.

b) Concatenate the 2500 dimension (50 x50) Gabor filter response with the original SURF feature descriptor (128 dimension) of that key-point to get the final G-SURF feature vector of dimension 2628 (2500+128). We used OPENCV package for SURF computation.

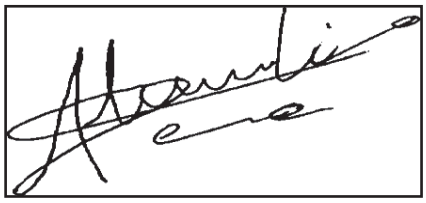
V. DATASET DETAILS AND EXPERIMENTAL DESIGN

In the field of signature verification, there is lack of a publicly available signature database. The quality of available databases also varies, as there has been no standard collection protocol. Besides, it is very costly to create a large corpus with different types of forgeries, especially skilled forgeries. So, the research in automatic signature verification has long been constrained by the unavailability of a standard database.

The signatures of English script were considered for this signature verification approach. Our entire dataset is comprised of 50 signatures from the GPDS database. Each signature has 24 original samples and 30 skilled forged samples. A total number of 1200 (50*24) genuine signatures and 1500 (50*30) forged signatures were employed for experimentation. For training, we considered 12 samples of both original and forged sample types. The remaining 12 original signatures and 18 forged signatures were kept for testing. One genuine signature samples with the corresponding forgery are displayed in Figure 2.



(a)



(b)

Figure 2. Example of an original (a) and corresponding forged signature (b).

We mainly performed 4 different experiments, which are as follows: (i) key-point level signature identification based only on the SURF descriptor, (ii) key-point level signature identification using only the G-SURF feature descriptor, (iii) Signature identification for a full signature image with only SURF descriptors based on training the classifier with the training dataset, followed by evaluating the test dataset and (iv) Signature identification for a full signature image with G-SURF feature descriptors based on training the classifier with the training dataset, followed by evaluating the test dataset.

VI. CLASSIFIER

We used Support Vector Machines (SVMs) as the classifier for this research. SVMs are defined for two-class problems and they look for the optimal hyper-plane which maximizes the distance, the *margin*, between the nearest examples of both classes, named *support vectors* (SVs). Given a training database of M data: $\{x_m|m=1,...,M\}$, the linear SVM classifier is then defined as:

$$f(x)=\sum_j \alpha_j y_j x_j \cdot x + b$$

where $\{x_j\}$ are the set of support vectors and the parameters α_j and b have been determined by solving a quadratic problem. The linear SVM can be extended to a non-linear classifier by replacing the inner product between the input vector x and the SVs, x_j, to a kernel function k defined as:

$$k(x,y)=\phi(x)\cdot\phi(y)$$

This Kernel function should be square integrable and should verify Mercer's Condition [9]. The Gaussian kernel is of the form:

$$[k(x,y)=\exp(-\frac{\| x-y \|^2}{2\sigma^2})]$$

To get best optimized results for all signatures we noticed that the gamma parameter ($1/2\sigma^2$) needs to be set to different values (0.5, 0.07, 0.005 etc) and the penalty multiplier parameter 'C' is set to 1. Further details of SVM may be found in [8, 9]. We used OPENCV SVM library in our experiment.

VII. RESULTS AND DISCUSSIONS

Different results of our experiments are shown in following sections.

A. Identification accuracy at the key-point level

Here we compare the average key-point level accuracy of our scheme using SURF and G-SURF in a 5-fold cross validation scheme. For each signature class we extracted the key-point features from all samples of both original and forged types. The total number of key-point descriptors obtained from all samples is divided into 5 sets, each of those sets consists of samples of key-point descriptors obtained from original and forged class signature image. Out of those 5 sets, 4 sets were used for training and remaining set is used for testing. This process is repeated 5 times so that each set is treated as a test set once. Each key-point feature descriptor from the test set is passed on to the SVM to determine the class (original/forged) of the key-point descriptor. The G-SURF features outperform SURF features for all signatures. It can be noted from Figure 3 that in most of the cases the SURF feature detectors attained an accuracy around 50%, whereas with G-SURF it increased in the range of 80%-90%.

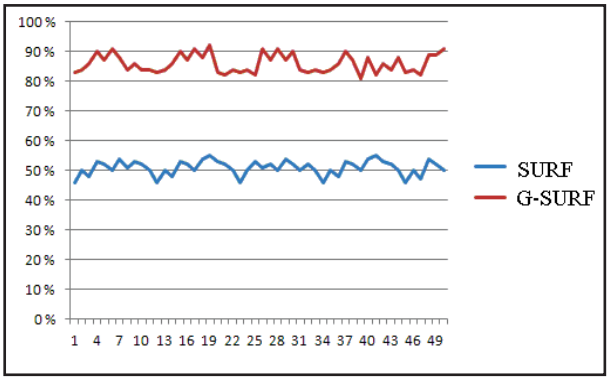


Figure 3. Comparison on percentage of key-point classification using SURF and G-SURF

B. Identification accuracy on signature image

Here we report the accuracy of our system in terms of False Acceptance Rate (FAR) and False Rejection Rate (FRR) of signature verification at the image level. We manually divided 24 original signatures and 30 forged signatures from one writer into 6 different sets. Each set consists of 4 original signatures and 5 forged signatures. We deployed a 6-fold cross validation scheme on these sets. 5 sets were used for training and one set is used for testing. This is repeated 6 times such that every set is treated once as a test dataset. For each test image, the following steps were followed in this experiment: (i) Feature computation for all key-points found in a signature image are undertaken based

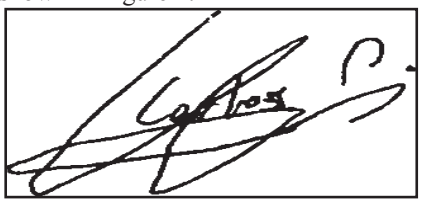
on the technique discussed in sub-section iv (c), (ii) a feature descriptor of dimension 2628(discussed in sub-section iv (c)) for each individual key-point is applied to the classifier, (iii) the classifier decides the class (original signature or forged signature) for each key-point, (iv) a majority voting scheme amongst the selected key-point descriptor classes is deployed to deduce the class for that test signature image, (v) in case of a tie (when the classifier assigns an equal number of key-point descriptors to original and forged types), then the class for the character is determined in the following way: we sum the respective confidence score obtained from the classifier of all key-point descriptors for both original and forged signature classes separately. The signature class with the maximum sum for the confidence score is assigned as the class for the signature image. The detailed results of our experiments are shown in Table 1.

Table 1. Comparative results of SURF and G-SURF

Feature	FAR (%)	FRR (%)
SURF	23.25	26.75
G-SURF	2.35	3.55

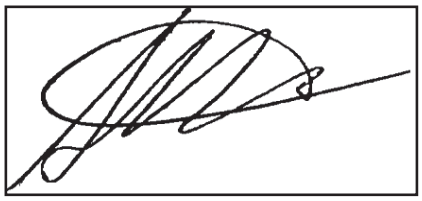
C. Error Analysis

We analyzed errors at the whole signature image level and found most of the errors came out of the images where the number of key-points detected was low. Also, certain errors came out of some very confusing signature images where even a human eye could be deceived. We noticed that in cases of miss-classification with some forged signatures, the system has been trained by an original signature which looks very much like the forged signature. Examples of such errors are shown in Figure 4.

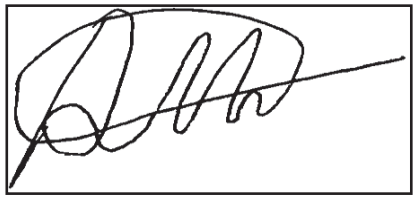


(G-I)

(G-II)



(F-I)



(F-II)

Figure 4. Examples of original signature (G-I), (G-II) with their corresponding forged signature (F-I), (F-II)

VIII. COMPARISION

Using the G-SURF feature, an average error rate (AER) as low as 2.95% was obtained. At this operational point, the FRR, FAR were 2.35%, and 3.55%, respectively. The AER (2.95 %) obtained in this research is lower than the AER obtained with the GPDS-160 database reported in [17] and [11]. GPDS database is widely used for experimentation in signature verification field. In this experiment using GPDS data sets, the G-SURF outperformed other works [20], [26] with same data sets.

IX. CONCLUSIONS

This paper presents an investigation of the performance of a signature verification system involving English off-line signatures. We proposed a novel feature extraction method combining SURF and Gabor-filter based methods to classify 50 pairs of original and forged signatures from the GPDS database. This method can be used even when a part of the signature is missing. Here the dimension of our feature vector is 2628, however in future we plan to reduce the feature dimensions using PCA or some other feature selection methods. As mention earlier in this research we experimented with Roman script signatures only. In the future we plan to extend our experiments considering Indian scripts such as Bangla and Hindi, and also using a larger dataset.

REFERENCES

[1] H. Bay, T. Tuytelaars, L. V. Gool, "SURF: Speeded Up Robust Features", ECCV (1), 2006, pp.404-417.).

[2] S. Belongie, J. Malik, J. Puzicha, "Shape Matching and Object Recognition Using Shape Contexts", IEEE Trans. Pattern Anal. Mach. Intell. 24(4) pp.509-522. (2002)

[3] Z. Zhang, L. Jin, K. Ding, X. Gao, " Character-SIFT: A Novel Feature for Offline Handwritten Chinese Character Recognition", In Proc. ICDAR 2009, pp. 763-767.
[4] M. Diem and R. Sablatnig, "Recognition of Degraded Handwritten Characters Using Local Features," Proc. ICDAR, pp. 221–225, 2009.
[5] S. Uchida and M. Liwicki: Analysis of Local Features for Handwritten Character Recognition. In Proc. ICPR 2010, pp. 1945-1948. 2010.
[6] Z. Jin, K. Qi, Y. Zhou, K. Chen, J. Chen and H. Guan, "SSIFT: An Improved SIFT Descriptor for Chinese Character Recognition in Complex Images", In Proc.
[7] A. C. Ramachandra, K. Pavithra, K. Yashasvini, K. B. Raja, K. R. Venugopal and L. M. Patnaik, "Off-line Signature Verification based on Cross-Validation for Graph Matching," IEEE International Conference on Electrical and Electronics (INDICON-2008), pp. 17-22, 2008.V. Vapnik, The nature of statistical learning theory, Springer Verlag, 1995.
[8] V. Vapnik, The nature of statistical learning theory, Springer Verlag, 1995.
[9] C. Burges, "A Tutorial on support Vector machines for pattern recognition", Data-mining and knowledge discovery, vol.*2*, no.2, 1998, pp. 1-47.
[10] H. Chang, J. Wang and H. Suen, ''Dynamic Handwritten Chinese Signature Verification," in Proc. 2nd Int. Conf. on Docu. Analysis and recognition, pp. 258–261, Oct. 1993.
[11] V. Nguyen, Y. Kawazoe, T. Wakabayashi, M. Blumenstein, and U. Pal, "Performance Analysis of the Gradient Feature and the Modified Direction Feature for Off-line Signature Verification" in proc. ICFHR 2010. pp. 303-307.
[12] B.Schafer and S.Viriri, "An Off-Line Signature Verification System", 2009, (ICSIPA- 2009), pp.95-100.
[13] E. Justino, E. Bortolozzi, R Sabourin, "Off-line Signature Verification Using HMM for Random, Simple and Skilled Forgeries," Proceedings of 7th ICDAR, pp. 105-110, 2001. [1]
[14] A. M. Darwish and G. A. Auda , ''A New Composite Feature Vector for Arabic Handwritten Signature Recognition, " in Proc. 1994 IEEE Int. Conf. on ASSP, pp. 613–616, April 1994. [2]
[15] R. Sabourin and J. Drouhard, ''Off–line Signature Verification Using Directional PDF and Neural Networks, " in Proc. 11th IAPR Int. Conf. on Pattern Recognition,, pp. 321–325, Sept. 1992. [3]
[16] B. Fang, C.H. Leung, Y.Y. Tang, K.W. Tse, P.C.K. Kwok and Y.K. Wong, "Off-line signature verification by the tracking of feature and stroke positions", Pattern Recognition, 36, pp. 91-101, 2003.
[17] K. Franke, "Analysis of Authentic Signatures and Forgeries" In Proc. IWCF, pp 150-164, 2009.
[18] R. Plamondon and G. Lorette, ''Automatic Signature Verification and Writer Identification – The State of the Art," Pattern Recognition, vol. 4, no. 2, pp. 107–131, 1989.
[19] J. Coetzer, B. Herbst, and J. D. Preez, "Off-line signature verification using the discrete radon transform and a hidden markov model", EURASIP Journal on Applied Signal Processing, 2004, 4, 559–571.
[20] V. Nguyen, M. Blumenstein, V. Muthukkumarasamy and G. Leedham, "Off-line Signature Verification Using Enhanced Modified Direction Features in Conjunction with Neural Classifiers and Support Vector Machines" ICDAR-2007, pp. 734 – 738.
[21] E. J. R. Justino, F. Bortolozzi, and R. Sabourin, "A comparison of SVM and HMM classifiers in the off-line signature verification," Pattern Recognition Letters, vol. 26, pp. 1377-1385, 2005.
[22] M. Hanmandlu, M. H. M. Yusof, and V. K. Madasu, "Off-line signature verification and forgery detection using fuzzy modelling," Pattern Recognition, vol. 38, pp. 341-356, 2005.
[23] H. Weiping, Y. Xiufen, W.Kejun,"A survey of off-line signature verification," Intelligent Mechatronics and Automation, 04,pp. 536 - 541.
[24] M. A. Ferrer, J. B. Alonso, and C. M. Travieso, "Offline geometric parameters for automatic signature verification using fixed-point arithmetic," PAMI, vol. 27, pp. 993-997, 2005.
[25] K. Huang and H. Yan, "Off-line signature verification using structural feature correspondence," PR, vol. 35, pp. 2467-2477, 2002.
[26] S. Armand, M. Blumstein and V. Muthukkumarasamy, "Off-line signature verification based on the Modified Direction Feature", 18th International Conference on Pattern Recognition, 2006, Vol. 4, pp. 509-512.
[27] H. Bay, A. Ess, T. Tuytelaars, L. V. Gool, "Speeded-Up Robust Features (SURF)", *Computer Vision and Image Understanding*, vol. 110, pp. 346-359 2008.
[28] www.iopl.im/pub/pre /H2/