

Online Signature Verification: A Review

Urvashi Chaudhary, Chandra Kanta Samal², Vinesh Kumar³

[#]Department of Electrical Engineering, IIT Delhi, Department of Computer Science, Acharya Narender Dev College University of Delhi, Delhi

Abstract: In past few decades Online Signature Verification have been employed in many applications such as security control, banking, law enforcement etc. A number of techniques have been proposed in the realization of reliable signature verification system such as Dynamic Time Wrapping (DTW), Hidden Markov Model (HMM), Support Vector Machine (SVM) and Neural Networks (NN) In this paper we have presented a review of research carried out in recent field of online signature verification and made a qualitative analysis of these state-of-the-art approaches.

Keywords: Signatures, Verification, fraudulence, feature Extraction, training, Forgery

I. Introduction

Biometrics is the utilization of physiological traits (face, iris, and fingerprint) or behavioral traits (signature, voice) for the verification of an individual identity. Biometric based authentication system is a trustable alternative to the password-based security systems as it is relatively hard to be forgotten, stolen, or guessed.

Signature being a behavioural biometric it is mainly used in the banks to verify the checks and accounts. Unlike physiological biometrics, it is fraught with problem of change over a time and it is not difficult to forge. One of the main challenges in signature verification is related to the signature variability. While signatures from the same user show considerable differences between different captures (high intra-class variability), skilled forgers can perform signatures with high resemblance to the user's signature (low intra- class variability). Signature verification aims at using such properties for making reliable authentication. However the wide spread acceptance of the signature by the public makes it more suitable for certain lower-security authentication needs. However, signature verification is a challenging task due to practical constraints. For instance, MasterCard estimates a \$450 million loss each year due to credit card fraud, likewise some billions of dollars being lost because of fraudulent encashment of checks. Reliable automatic signature verification could be a proper solution to reduce such losses since handwritten signatures are already involved in the credit card transactions and bank checks encashment.

1.1 The Signature Verification Modes

There are two modes to the signature verification depending on how the signatures are collected from a user.

Offline (static) Signature Verification: In this mode data is acquired by scanning handwritten signatures which are then processed as static images. The verification is based on these static signature images. This mode is useful in automatic verification of signatures obtained from bank checks and other paper documents.

Online (dynamic) Signature Verification: In this mode the signatures are captured by social hardware (e.g. smart pens or pressure sensitive tablets) which is capable of measuring dynamic properties of a signature in addition to the shape, while shape is the only information in offline signatures. Dynamic information (e.g. pen pressure) makes the signature more unique and more difficult to forge.

Applications of online signature verification include identity verification in payments using a credit card; authorization of computer users for accessing sensitive data or programs, authentication of individuals for accessing physical devices or buildings, and protection of small personal devices from unauthorized usage.

Online signature verification is more robust, reliable and accurate than offline signature verification as its dynamic properties make the process of forging an online signature more difficult. Therefore online signature has become an attractive biometric method as it facilitates the authentication of the internet transactions and contracts (e-commerce, e-banking, e-business, e-contract).

Need

Signature is a special characteristic of any person. By the help of signature we can identify the person. In today day to day life as we talk about the verification of any person, we normally verify them by two ways firstly by face and secondly by signature. In banking or security system the person is normally verified by his or her signature. Hence we can say that the signature is alternate way to identify the person. In most of the organizations, the signature is normally verified by their experts by matching old signature's samples.

So, Online Signature will give the more accurate way to verify the signature because sometimes the person can copy the signature of others. As online signature is based on real time so there is very less chance (0.01%) that the person can copy the signature. We don't need any regular expert who always needs to verify the signature of the person.

II. Image Matching

Image matching is a fundamental aspect of many problems in computer vision, including object or scene recognition, solving for 3D structure from multiple images, stereo correspondence, and motion tracking. Image features that have many properties that make them suitable for matching differing images of an object or scene. The features are invariant to image scaling and rotation, and partially invariant to change in illumination and 3D camera viewpoint. They are well localized in both the spatial and frequency domains, reducing the probability of disruption by occlusion, clutter, or noise. Large numbers of features can be extracted from typical images with efficient algorithms. In addition, the features are highly distinctive, which allows a single feature to be correctly matched with high probability against a large database of features, providing a basis for object and scene recognition.

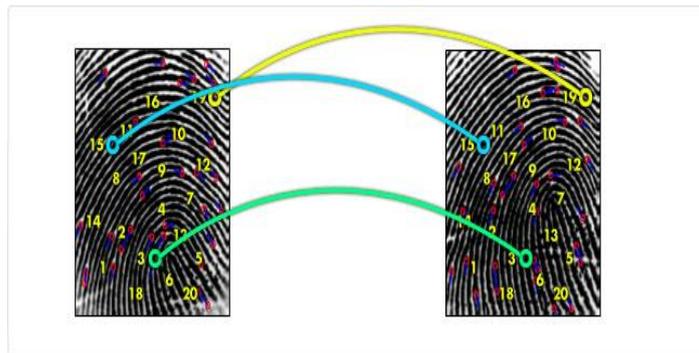


Figure 1.1: Image Points Matching of figure

The cost of extracting these features is minimized by taking a cascade filtering approach, in which the more expensive operations are applied only at locations that pass an initial test.

Following are the major stages of computation used to generate the set of image features:

- Scale-space extreme detection: The first stage of computation searches over all scales and image locations. It is implemented efficiently by using a difference-of-Gaussian function to identify potential interest points that are invariant to scale and orientation.
- Keypoint localization: At each candidate location, a detailed model is fit to determine location and scale. Keypoints are selected based on measures of their stability.
- Orientation assignment: One or more orientations are assigned to each keypoint location based on local image gradient directions. All future operations are performed on image data that has been transformed relative to the assigned orientation, scale, and location for each feature, thereby providing invariance to these transformations.
- Keypoint descriptor: The local image gradients are measured at the selected scale in the region around each keypoint. These are transformed into a representation that allows for significant levels of local shape distortion and change in illumination.

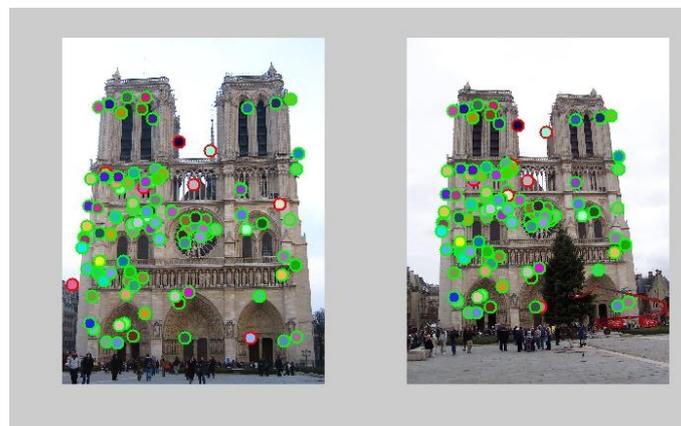


Figure 1.1: Image Points Matching of building

This approach has been named the Scale Invariant Feature Transform (SIFT), as it transforms image data into scale-invariant coordinates relative to local features. An important aspect of this approach is that it generates large numbers of features that densely cover the image over the full range of scales and locations. A typical image of size 500x500 pixels will give rise to about 2000 stable features (although this number depends on both image content and choices for various parameters). The quantity of features is particularly important for object recognition, where the ability to detect small objects in cluttered backgrounds requires that at least 3 features be correctly matched from each object for reliable identification.

For image matching and recognition, SIFT features are first extracted from a set of reference images and stored in a database. A new image is matched by individually comparing each feature from the new image to this previous database and finding candidate matching features based on Euclidean distance of their feature vectors.

The key point descriptors are highly distinctive, which allows a single feature to find its correct match with good probability in a large database of features. However, in a cluttered image, many features from the background will not have any correct match in the database, giving rise to many false matches in addition to the correct ones. The correct matches can be filtered from the full set of matches by identifying subsets of key points that agree on the object and its location, scale, and orientation in the new image. The probability that several features will agree on these parameters by chance is much lower than the probability that any individual feature match will be in error. The determination of these consistent clusters can be performed rapidly by using an efficient hash table implementation of the generalized Hough transform. Each cluster of 3 or more features that agree on an object and its pose is then subject to further detailed verification. First, a least-squared estimate is made for an affine approximation to the object pose. Any other image features consistent with this pose are identified, and outliers are discarded. Finally, a detailed computation is made of the probability that a particular set of features indicates the presence of an object, given the accuracy of fit and number of probable false matches. Object matches that pass all these tests can be identified as correct with high confidence.

III. Literature Review

In this paper, Prathiba M.K. and Dr. L. Basavaraj proposed an online handwritten signature verification system is one of the most reliable, fast and cost effective tool for user authentication. This work examines the online handwritten signature verification system methodologies. Signatures are acquired from devices such as pressure sensitive tablets, digitizer, etc. The aim of this paper is to review the signature feature extraction algorithms, techniques and methodologies [21]. In this paper, Liang Wan proposed a new two-stage statistical system for automatic on-line signature verification. System is consists of a simplified GMM model for global signature features and a discrete HMM model for local signature features. He explained specific simplification strategies for system building and training. The system requires only 5 genuine samples for new users and depends on only 3 global parameters for quick and efficient system tuning. Experiments are conducted to verify the effectiveness of this system [13]. In this paper a system proposed by F.A. Afsar, U. Farukh and M Arif. They worked in such a way that first the global features are extracted from the spatial coordinates and these features are obtained during the data acquisition stage. The method used here is one dimensional wavelet transform. Then the results are obtained using K-NN classifier and proved the accuracy of the proposed technique better. It is global feature based approach signature verification. The signature patterns are matched based on wavelet domain features that are extracted from the normalized spatial coordinates of the signatures obtained during data acquisition. The differences between the spatial coordinates of consecutive points in the signature are also subjected to both wavelet decomposition and feature extraction. The total temporal duration of the signature used as a distinguishing feature during classification. The Figure 2.2 shows the block diagram of the system. The system is described in these stages 1) Acquisition 2) Pre-processing 3) Feature Extraction 4) Template Generation 5) Feature Matching [12]. In this paper, Pippin proposed two verification filters, each filter employing different techniques commonly used in the literature. The first filter extracts high-level global features of a signature and compares these features with stored signature templates using KNN classification. The second filter uses velocity based stroke segmentation to encode the signature as a series of strokes and then uses dynamic time warping to find the closest distance between test and template signatures [10]. In this paper, Feng proposed a new warping technique for the functional base approach in signature verification. Dynamic time warping (DTW) is the commonly used warping technique. There are two common methodologies to verify signatures: the functional approach and the parametric approach so the functional based approach was originally used in application speech recognition and has been applied in the field of signature verification with some successful accuracy since two decades ago. The new warping technique he proposed, named as extreme points warping (EPW). It was proved that this method is adaptive in the field of signature verification than DTW in the presence of the forgeries. In the functional approach, a straightforward way to compare two signal functions is to use a linear correlation. It has the following two problems: Due to difference of overall signal duration and due to existence of non-linear distortions within signals. A new warping technique called EPW replaced the

commonly used DTW. Instead of warping the whole signal as DTW does, EPW warps a set of selective points [11].

In his paper, Alisher, proposed a system for on-line signature verification. Here approaching the problem as a two-class pattern recognition problem. During enrollment, reference signatures are collected from each registered user and cross aligned to extract features about that user signature. A test signatures authenticity is established by first comparing it with each reference signature for the claimed user. The signature is then classified as genuine or forgery based on the alignment scores which are normalized by reference statistics, using standard pattern classification techniques. He experimented with the Bayes classifier on the original data as well as a linear classifier used in conjunction with Principal Component Analysis (PCA). The system has following phases: 1) Data Acquisition 2) Feature Extraction 3) Signature Alignment. An online signature identification system is presented in [18] based on global features. The information is extracted as time functions of various dynamic properties of the signatures [14].

In this paper, Kashi proposed a method for the automatic verification of on-line handwritten signatures using both global and local features. The global and local features indicate various aspects of signature shape and dynamics of signature production. He explained that with the addition to the global features of a local feature based on the signature likelihood obtained from Hidden Markov Models (HMM), the performance of signature verification method improved significantly. In this paper, he models the signing process with many states that constitute a Markov chain, each of them corresponding to a segment of signature. The states are not directly observable (hidden); one can only observe the signature local features here as tangent angles. In this signature verification, the handwriting tangent and its derivative as an observation vector in equal length segmentation is used [9].

IV. Research Methodology

Research Methodology provides the scientific way for the analysis and solution of the problem. I will collect the latest study material from the various heterogeneous sources for the extraction of features using structural parameters and evaluate the membership functions using interactive entropy model. The simulation and testing of algorithms using Matlab to verify their signature structural parameters.

V. Conclusion

This Paper gives the depth review of handwritten signature verification system which includes the basic concept regarding the process including the process, types of forgeries etc. The basics concern of this paper is understand the basics of online signatures verification system, that now it works and types of forgeries it can be affected by.

REFERENCES

- [1]. D.Muramatsu, M. Kondo, M. Sasaki, S. Tachibana, and T. Matsumoto, "A markov chain monte carlo algorithm for bayesian dynamic signature verification". IEEE Transactions on Information Forensics and Security, March, 2006, 1(1):22-34
- [2]. K. Yasuda, D. Muramatsu, and T. Matsumoto, "Visual-based online signature verification by pen tip tracking", Proc. CIMCA 2008, pp. 175-180
- [3]. Satoshi Shirato, D. Muramatsu, and T. Matsumoto, "camera-based online signature verification: Effects of camera positions", World Automation congress 2010 TSI press
- [4]. D. Muramatsu, K. Yasuda, S. Shirato, and T. Matsumoto. "Visual-based online signature verification using features extracted from video", Journal of Network and Computer Applications **Volume 33**, Issue 3, May 2010, Pages 333-341
- [5]. R. Plamondon and G. Lorette. "Automatic signature verification and writer identification - the state of the art". Pattern Recognition, 22(2):107-131, 1989
- [6]. M. E. Munich and P. Perona. "Visual identification by signature tracking", IEEE Trans. Pattern Analysis and Machine Intelligence, 25(2):200-217, February 2003
- [7]. F.A.Afsar, M. Arif and U. Farrukh, "Wavelet Transform Based Global Features for Online Signature Recognition", Proceeding of IEEE International Multi-topic Conference INMIC, pp. 1-6, Dec. 2005
- [8]. Mohammad M. Shafiei, Hamid R. Rabiee, "A New On-Line Signature Verification Algorithm Using Variable Length Segmentation and Hidden Markov Models", Seventh International Conference on Document Analysis and Recognition (ICDAR'03), **vol. 1**, pp. 443
- [9]. 9.R. S. Kashi , J. Hu & W. L. Nelson, "On-line Handwritten Signature Verification using Hidden Markov Model Features", Fourth International Conference Document Analysis and Recognition (ICDAR'97), pp. 253 - 257
- [10]. Charles E. Pippin, "Dynamic Signature Verification using Local and Global Features", Georgia Institute of Technology, July 2004
- [11]. Hao Feng and Chan Choong Wah, "Online Signature Verification Using New Extreme Points Warping Technique", Pattern Recognition Letters, **vol. 24**, pp. 2943-2951, Dec. 2003
- [12]. F.A. Afsar, M. Arif and U. Farrukh, "Wavelet Transform Based Global Features for Online Signature Recognition", Proceeding of IEEE International Multi-topic Conference INMIC, pp. 1-6, Dec. 2005
- [13]. Liang Wan, Bin Wan, Zhou-Chen Lin, "On-Line Signature Verification with Two-Stage Statistical Models", Eighth International Conference on Document Analysis and Recognition (ICDAR'05), pp. 282 - 286
- [14]. Alisher Kholmatov, "Biometric Authentication Using Online Signatures", MS Thesis, Sabanci University, June 2002
- [15]. Chan F. Lam, David Kamins and Kuno Zimerann, "Signature Recognition through Spectral Analysis", Pattern Recognition, **vol. 22**, pp.39-44, Jan.1989

- [16]. Liang Wan, Bin Wan, Zhou-Chen Lin, “On-Line Signature Verification with Two-Stage Statistical Models”, Eighth International Conference on Document Analysis and Recognition (ICDAR'05), pp. 282 – 286
- [17]. Chan F. Lam, David Kamins and Kuno Zimerann, “Signature Recognition through Spectral Analysis”, *Pattern Recognition*, **vol. 22**, pp.39-44, Jan.1989
- [18]. <http://www.cse.ust.hk/svc2004/download.html>
- [19]. V. Ramana Murty, M, “Hanmandlu, Interactive Fuzzy Model based Recognition of the handwritten characters”, *Journal of Pattern Recognition Research* 2, 154-165, 2011
- [20]. J-S.R.Jang, C-T.Sun,E.Mizutani, “Neuro- Fuzzy and soft computing”, Person Prentice Hall
- [21]. Prathiba M.K. and Dr. L. Basavaraj, “Online handwritten signature verification system: A Review”, *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, **Volume 3**, Issue 2, March – April 2014