Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed Computing

Signature Recognition in Mobile Payments

Master Thesis

Cedric Waldburger

wcedric@ee.ethz.ch

Distributed Computing Group
Computer Engineering and Networks Laboratory
ETH ZÃ¼rich

Supervisors:
Christian Decker (DISCO)
Conor Wogan (SumUp)
Prof. Dr. Roger Wattenhofer

March 28, 2013

Acknowledgements

thank DISCO/Christian/Prof

thank SumUp

Abstract

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Keywords: Signature Detection, Signature Recognition, Fraud Detection, Mobile Payments, Mobile Devices

Contents

Chapter 1

Introduction

As Smartphones become more and more popular, they're being used in more and more industries and fields. An application that has seen a lot of traction recently is mobile payments where the smartphone is used to process payments - either between users or between a client and a merchant.

SquareUp (ref), SumUp (ref), iZettle (ref) and others are just some of the companies who are enabling merchants to take payments from their clients via their smartphone. This thesis was written in collaboration with SumUp, located in Berlin and Dublin. In section (ref: 1.1) we analyze the business model in more detail.[1] [2] [3] [4] [5] [6] [7] [8]

As with every area that involves financials and money transactions in particular, security becomes a very important topic. Security measures are taken on various ends but this thesis focuses on identifying card holders by their signature.

As the technical complexity and thus the cost of a Chip-and-Pin-Reader are much higher than those of Swipe- and Chip-and-Signature-Readers, identification by signature rather than a four or six digit pin remains the dominating technique.

This work is focused on automatic signature detection using a (TODO: MIXER) of Dynamic Time Warping (DTW) and Hidden Markov Models (HMM) to generate a similarity score between signatures and a reference signature in the case of DTW or the respective HMM signature model.

1.1 SumUp - Mobile Payment Company

SumUp was founded in fall 2011 in Berlin and Dublin and is today used actively by many thousand merchants in more than ten european countries. It's core business competes with traditional Credit Card Terminal companies who require their users to pay a monthly fee for their terminal.

Instead of building and selling complex hardware, SumUp's Apps make use of the fact that almost anyone owns a smartphone today. SumUp works on the

iOS and Android platform and the only additional hardware, a dongle that reads the credit cards, is sent to the customers for free. The Apps to use Sumup are available for free in both the Android and iOS store respectively.

In order to accept a credit card payment, a new user follows the steps depicted in Fig X (TODO):

- Open Account and supply documents of identification
- Plug in card reader
- Choose product or enter amount manually
- Choose Payment Method
- Put Credit Card into reader
- Let customer sign and confirm

On the server side, a variety of Fraud checks are performed and the transaction is either accepted or declined. The signature detection developed during this work will likely be implemented as an additional security measurement on the server side.

Besides it's simplicity and low setup time and cost, SumUp's advantage over its competitors is that it only collects a fixed percentage per transaction of 2.75%.

1.2 Fraud

Automatic payment systems are always interesting for attackers due to their direct monetary return and usually high scalability. SumUp is no exception and chapter 2 (TODO: ref) will list the different fraud scenarios and counter measurements.

As credit cards are historically a very unsafe payment method (todo: list to paper), special attention has to be paid when dealing with credit card information and processing credit card transactions.

The main attack vectors in credit card fraud are: (TODO: ref paper)

- Copied and stolen cards
- Money Laundry
- People transferring money under someone else's name
- Illegal money being transferrend through one's system

We will mainly focus on the first fraud case and concentrate on identifying a card holder by his signature. Our goal is that after a card has been used a certain amount of times, we can build a reliable signature model to identify whether it is the same person signing or not the next time the card is used.

Not only the pysical cards are at risk to be stolen, also the digital copy of the credit card data needs to be protected. This is one of the reasons SumUp only saves encrypted card information and does so in a PCI-DSS environment. The ensure maximum security precaution, only card numbers and not names of card holders are saved. This has one downside: We can only identify cards but not card holders and can therefore only build a signature for a card but not for a person (who might use several cards on several occasions).

1.3 Signature Recognition

Methods for signature detection is usually divded into Online and Offline Methods.

Offline Signature Detection performs recognition algorithms based on static features of a signature, mainly it's shape and length.

Online signature detection has become possible when digital tablets and touchscreens have become widely used and it became feasible to also capture the dynamic features of a signature.

In chapter X (todo: ref) we look at the common techniques in both areas to compare signatures.

Traditionally, digital signatures were captured on a digital tablet with a pen.

Signatures captured on mobile devices are different from existing work because

- they're capture by finger instead of a pen
- the sampling rate isn't constant as the finger-up/-down are event based
- the signature is captured on screen with different resolutions and densities

We discuss our strategies to overcome these challenges in chapter X (TODO ref).

Chapter 2

Fraud

2.1 Fraud Scenarios

2.2 Fraud Prevention

2.3 Fraud Detection

Chapter 3

Signature Recognition

In this chapter, we'll present an overview of existing signature detection methods and available resources.

Traditionally, detection methods can be assign to either feature- or function-based methods. We describe both approaches in (TODO ref). A combination of feature- and function-based approaches has been providing better results than the individual techniques. (TODO: Ferrez-Aguilar et al, 2005)

3.1 Previous and Related Work

During the past 3 decades, a lot of work has been done to improve offline signature detection algorithms. An overview over previous work was given in a paper by Guo et al. [9]

TODO: list a few papers and their methods. Some for online and some for offline verification. List also how well they were performing.

3.2 Features and Feature Extraction

As introduced in chapter X (TODO), all features can be classified as local or global features. Global features describe the signature as a whole and include the discrete Wavelet Transform (TODO: ref), thue Hough Transform (TODO: ref), horizontal and vertical projectsions (TODO: ref) and smoothness features (TODO: ref).

3.3 Feature-based Systems

Feature-based systems, also called global systems, are characterized by the fact that the feature vector consists of measurements on the whole signature. Exam-

ple features are the total duration, number of finger-up and finger-down events, average speed, etc.

Sequential Forward Feature Selection (SFFS) is one of the best performing methods (TODO: Jain and Zongker, 1997) but many have been proposed. The matching is usually done using statistical classifiers such as Parzen Windows (Martinez-Diaz et al, 2007), majority voting (Lee et al, 1996) Mahalanobis distancis (Galbally et al, 20007) or Guassian Mixture Models (Martinez-Diaz et al, 2007).

3.4 Function-based Systems

Function-based systems, also called local systems, are characterized by the fact that the feature vecotr consists of measurements on partial segments of the signature. Theses segments can be single points of groups of points. The most popular methods are Dynamic Time Warping (DTW) and Hidden Markov Models (HMM).

3.4.1 Comparison of time series

The first approach to compare two time signals that comes to mind, might be to use linear correlation [10] but as soon as the time signals are not of equal length or there is a non-linear distortion, this approach will not be valid anymore. As it is very likely that the same signer's signature will have different dynamics every time he signs, this is not a feasible approach.

We discuss approaches that take these limitations into account in the next two sub-chapters.

3.4.2 Dynamic Time Warping

Dynamic Time Warping is a dynamic programming algorithm to measure the similarity between two time series which may vary in time or speed. This has been used for speech recognition and can also be used for signature detection to cope with the non-linear time distortions which one might have in the signals because a signer does not always sign with the same speed. It has shown to be a much more robust distance measure than the Euclidean distance [11][4][5] due to it's ability to match similar shapes even if they are out of phase in the time axis.

Koegh et al. showed on a very large dataset that the mean error rate average over 1000 runs for DTW was an order of magnitude lower than the error rate for the Euclidian distance. However, the DTW algorithm also took approximately 230 times longer than the Euclidean distance. [12]

It has first been applied to signatures in 1977 by Yasuhara and Oka (TODO: ref).

DTW allows us to compare signatures even if the signer was signing slower at the beginning in one of the two signatures.

Training is done by computing the distance measure $dtw[n][m]$ for all signatures n, m in the set of signatures for a certain user and selecting the signature s with the smallest distance to all other signatures.

Classification is done by computing the distance DTW distance $dtw[s][t]$ between the model signature s and a signature t under test.

Listing 3.1: DTW in Pseudo-Code

```
for i:=maxint to 0 do
begin
end
```

Another short coming of the Euclidean distance is that it is only defined if both time series have equal length, as $e_k = (i, j)_k, i = j = k$. The time and space complexity of DTW is $O(nm)$

TODO: show image like 10.1007 s10115 page 362

Even though the DTW algorithm has been outperformed by more powerful algorithms like HMMs or SVMs in speech detection, it remains very effective in Signature detection as it deals well with small amounts of training data, which is typical for signature verification problems.

In general, DTW is known to have two drawbacks in signature verification:

- heavy computational load
- warping of forgeries

DTW causes heavy computational load becauseit does not obey the triangular inequality and thus indexing a set of signatures takes a lot of time. As soon as the pool of signatures for a signer get bigger, the computation costs raise because the test signature has to be compared to each of the signatures in the pool of confirmed signatures. Eamonn Keogh et al. presented a lower bounding method to index all samples without comparing each of them to each other. [12]

The second drawback can be addressed by looking at how straight or bended the warping path is. Work on this has been done [13] but made comparison between different signatures harder because it introduce another dimension and thus made computation harder.

Hao Feng et al. proposed another extension of the DTW algorithm, called extreme points warping (EPW) which proved to be more adaptive in the field of signature verification than DTW and reduced the computation time by a factor of 11. [14]

3.4.3 Hidden Markov models

A Hidden Markov Model (HMM) is a stochastic process with an underlying Markov Model of which the states can not directly be observed but the only observations can be made. Each state transition emits a certain observation with a certain probability.

While HMMs with a too small set of states and observations perform bad because they are too simple, too many states and observations make the model computational heavy and accuracy is reduced because of overfitting.

HMMs are defined by:

- Number of hidden states: N
- Number of Observations or Symbols: M
- Probability transition matrix $A = \{a_{ij}\}$ defining the probabilities fo jumping from one state to another or staying on the same state

TODO: Add Image of how HMM looks

Markov Models can be modeled as Left-to-right, ... (TODO: name all types, show graph).

3.4.4 Neural networks

Neural networks have also been used to build a system for detection of random forgeries. (TODO: explain random forgeries, list reference Baltzakis) Baltzakis uses global features, grid features such as pixel densities and texture features such as cooccurrence matrices to represent each signature. A two-stage perceptron one-class-one-network (OCON) calssification is used for each feature set. TODO: explain more when reference found

3.4.5 Template matching techniques

3.4.6 Minimum distance classifiers

3.5 Online Signature Detection

2005).

3.5.1 Feature-Based Methods

3.5.2 Function-Based Methods

3.6 Challenges in Signature Detection Specific to Mobile Payments

A lot of work has been done on signature detection on static signatures and also on dynamic signatures. However, almost all work on dynamic signatures has been done on signatures that were captured using a pen on a digital tablet. In our case, signatures were captured on a wide range of different devices and with a user's finger instead of a pen. This has several implications.

Our experiments in chapter X (TODO ref) will show to which extent known techniques are applicable to this type of signature and what future work might need to be done.

3.6.1 Signature are written with Finger

Our experience shows that people are not used to write their signature with their bare finger and the first few times they sign, their signature differs a lot. However, after just 10-15 times , the signature's shape seems to stabilize.

This means that it will be a lot harder to detect signatures based on the first few signatures than on later signatures, once a user got used to signing with his finger.

It also means that we should prefer later signatures to earlier ones as in later signatures the signer's signature might have stabilized.

3.6.2 Sparse Initial Dataset

Although SumUp is live in over 10 countries as of today, it is still only used in a relatively small set of locations and we are therefore unlikely to gather a lot of data about a certain user until the concept becomes more often deployed and used.

This means that we have to try and find a solution that works reasonably well with a small amount of initial data per user.

3.6.3 Device & Software Fragmentation

Unlike the signature's that are captured on a digital tablet, our database of signatures is captured on a variety of devices with different properties. There

are various factors that have an influence on the digital representation of the signature:

- Different Manufacturer: Both, iOS and Android devices use a variety of manufacturers for their handsets and the touch screens used. Recent studies have shown the differences of how signals are captured on different screens (TODO: link reference)
- Screen Size: the screen diagonal of current smartphones typically ranges between X and X cm, those of tablets typically ranges between X and X cm. A consequence is that the user might not only sign slightly differently but also that the signature will consist of more or less data points and it will take users a longer or shorter amount of time to sign.
- ...

We will consider these factors when applying our algorithm in Chapter X (TODO)

Chapter 4

Experiments

4.1 Database

4.1.1 Acquisition

Between 8 and 80 Signatures per person were collected from 11 people on 4 different days on four different devices. In total, a set of 487 (TODO: correct) signatures and X Forgeries were collected.

The devices used to collect the signatures are listed in Table X (TODO: ref).

Table 4.1: The four devices used to collect signatures, ordered by screen size

Device	**Software Version**	**Screen Size [cm]**	**Screen Resolution [px]**
Apple iPhone 4s	iOS 6.1.2	8.9	640x960
Apple iPhone 5	iOS 6.1.2	10	640x1136
Samsung Galaxy Note II	Android 4.1.1	14.1	720x1280
Apple iPad mini	iOS 6.1.2	20	768x1024

4.1.2 Pre-Alignment and Normalization

4.2 Databases

4.3 Forgeries

4.4 Recognition

4.4.1 Feature Extraction

4.4.2 Dynamic Time Warping

4.4.3 Hidden Markov Models

Model

Training

Evaluation/Matching

4.4.4 MLP

4.5 Evaluation

4.5.1 Computational Requirements

4.5.2 Modi

4.6 Discussion and conclusions

4.6.1 Signature Detection

4.6.2 Feedback Loop

4.6.3 Feature Work

- use lower bound proposed by Keogh et al.[12] to make DTW faster on large datasets

Chapter 5

Conclusions

Bibliography

[1] Hanmandlu, M., Yusof, M., Madasu, V.K.: Off-line signature verification and forgery detection using fuzzy modeling. In: Pattern Recognition. (March 2005)

[2] Phua, C., Lee, V., Smith, K., Gayler, R.: A comprehensive survey of data mining-based fraud detection research. Artificial Intelligence Review (2005)

[3] Camino, J.L., Travieso, C.M., Morales, C.R., Ferrer, M.A.: Signature classification by hidden markov model. (1999) 481–484

[4] Fuentes, M., Garcia-Salicetti, S., Dorizzi, B.: On line signature verification: Fusion of a hidden markov model and a neural network via a support vector machine. In: Frontiers in Handwriting Recognition, 2002. Proceedings. Eighth International Workshop on. (2002) 253–258

[5] Shafiei, M., Rabiee, H.: A new online signature verification algorithm using variable length segmentation and hidden markov models. In: Document Analysis and Recognition, 2003. Proceedings. Seventh International Conference on. (2003) 443–446 vol.1

[6] Kim, J.W., Cho, H.G., Cha, E.Y.: A study on enhanced dynamic signature verification for the embedded system. In: Proceedings of the First international conference on Brain, Vision, and Artificial Intelligence. BVAI'05, Berlin, Heidelberg, Springer-Verlag (2005) 436–446

[7] Coetzer, J., Herbst, B.M., du Preez, J.A.: Offline signature verification using the discrete radon transform and a hidden markov model. EURASIP J. Appl. Signal Process. **2004** (January 2004) 559–571

[8] Dolfing, J.G.A., Aarts, E.H.L., Van Oosterhout, J.J.G.M.: On-line signature verification with hidden markov models. In: Pattern Recognition, 1998. Proceedings. Fourteenth International Conference on. Volume 2. (1998) 1309–1312 vol.2

[9] Justino, E.J., Bortolozzi, F., Sabourin, R.: A comparison of svm and hmm classifiers in the off-line signature verification. Pattern Recognition Letters **26**(9) (2005) 1377 – 1385

[10] Plamondon, R., Lorette, G.: Automatic signature verification and writer identification - the state of the art. Pattern Recognition **22**(2) (1989) 107 – 131

[11] Keogh, E.J., Pazzani, M.J.: Scaling up dynamic time warping for datamining applications. In: Proceedings of the sixth ACM SIGKDD international conference on Knowledge discovery and data mining. KDD '00, New York, NY, USA, ACM (2000) 285–289

[12] Keogh, E.: Exact indexing of dynamic time warping. In: Proceedings of the 28th international conference on Very Large Data Bases. VLDB '02, VLDB Endowment (2002) 406–417

[13] Y Sato, K.K.: Online signature verification based on shape motion and writing pressure. Proceedings of the 6th ICPR (1982) 823–826

[14] Feng, H., Wah, C.C.: Online signature verification using a new extreme points warping technique. Pattern Recogn. Lett. **24**(16) (December 2003) 2943–2951

Appendix A

Appendix Chapter