

Algorithm Design for Grip-Pattern Verification in Smart Gun

X. Shang, R.N.J. Veldhuis, A.M. Bazen and W.P.T. Ganzevoort
University of Twente, EEMCS-SAS
P.O. Box 217, 7500 AE Enschede, the Netherlands
Phone: +31 (0)53 4892 842 Fax: +31 (0)53 4891 060
E-mail: x.shang@el.utwente.nl

Abstract— The Secure Grip project¹ focuses on the development of a hand-grip pattern recognition system, as part of the smart gun. Its target customer is the police. To explore the authentication performance of this system, we collected data from a group of police officers, and made authentication simulations based on a likelihood-ratio classifier. This smart gun system has been proved to be useful in the authentication of the police officers. However, its authentication performance needs some further improvement, especially when data for training and testing were collected with some time in between. We present and analyze the simulation results of the authentication experiment. Based on the analyses, we propose some methods to improve the system's authentication performance.

Keywords— grip pattern recognition, smart gun, likelihood-ratio, support vector machine

I. INTRODUCTION

In grip pattern recognition the main research question is, whether the pressure pattern exerted while holding an object can be used to reliably authenticate a person. The Secure Grip project focuses on the development of a prototype recognition system, as part of the smart gun, where the grip-pattern recognition ensures that it can only be fired by its rightful user. This application is intended for use by the police, since carrying a gun in public brings considerable risks. In the US vital statistics show that about 8% of the law-enforcement officers, who are killed in a shooting incident, are shot by their own weapon [1].

The first prototype of this smart gun system (see Fig. 1) was described in [2], in terms of its design, implementation and evaluation. A collection of grip patterns was gathered from a group of mostly untrained subjects with no experiences in shooting. The simulation results indicated that

¹This research is supported by the Technology Foundation STW, applied science division of NWO and the technology programme of the Ministry of Economic Affairs.

the grip pattern contains sufficient information to use for authentication. To explore the authentication performance of the smart gun system when used by its target customer, the police, we collected new data from a group of police officers. With the new data we made authentication simulations, by using the same algorithm as was used in [2].



Fig. 1. Prototype of the smart gun

This paper presents and analyzes the authentication performance of the smart gun system, with the grip patterns collected from the police officers. Section 2 describes the authentication algorithm. The procedure of data collection is reviewed in Section 3. Subsequently, Section 4 presents and analyzes the simulation results of the authentication experiment. Finally, the conclusions are given in Section 5.

II. AUTHENTICATION ALGORITHM

The authentication algorithm is based on a likelihood-ratio classifier for Gaussian probability densities. The likelihood-ratio classifier has been proved to be optimal, in terms of the expected overall error rates if the data has a known probability density function [3], [4]. We assume that both the overall data, and that of each individual subject, are Gaussian distributed. The pixel values of each grip pattern image are aligned into a column vector, and are used as the features in the algorithm. In our system the feature space has the dimension of 1936, since each grip

pattern was recorded as a 44 by 44 image.

In practice, the exact probability density function of neither the overall data, nor the data of each individual subject is known, and therefore needs to be estimated from the training data. In total, four parameters need to be estimated. They are the mean vector of the overall data, the mean vector and the covariance matrix of each individual subject's data, and the transformation matrix. In our case, the number of training samples from each subject should be much more than 1936. This is to prevent the estimated covariance matrices from being singular, and to prevent the classifier suffering from overtraining. Otherwise, the algorithm would suffer from the so-called small-sample-size problem. However, we can not make this large number of measurements, since it would be rather impractical for the user enrollment.

To solve the small-sample-size problem, we assume that each subject has the same within-class covariance matrix. Thus, this common covariance matrix can be estimated more accurately, by using data from all the subjects. As a further step to relieve the effect of the small-sample-size problem, we reduce the dimension of the feature space. Firstly, we apply a PCA (Principal Component Analysis) to project the overall data to a subspace with the biggest variances. In this new space, the directions contributing to the authentication, are not more than the number of subjects minus one. And, these directions have the smallest variances of each individual subject's data [3]. Accordingly, a further dimension reduction is achieved, by applying a PCA to each individual subject's data, and discarding all the directions, except only 40 ones (41 subjects in total) with the smallest variances.

III. DATA COLLECTION

We collected grip patterns from a group of 41 police officers, in three sequential sessions. The three sessions had approximately one month and four months in between. All subjects in the group participated in both the first and the second session, with 25 grip pattern images recorded from each. In the third session, however, data was collected from 22 subjects from the same group; and each subject contributed 50 grip pattern images.

In both the first and the second session, we asked each subject to pick up the gun, aim it at an assumed target, hold it still, say "ready" as a signal for us to record the image of his hand-grip pattern (see Fig. 2), and then release the gun after we finished recording. This whole procedure was repeated by the subject until enough data was collected from him. We observed afterwards, that most of the subjects' hand-grip pattern, varied greatly on average from one session to the other.

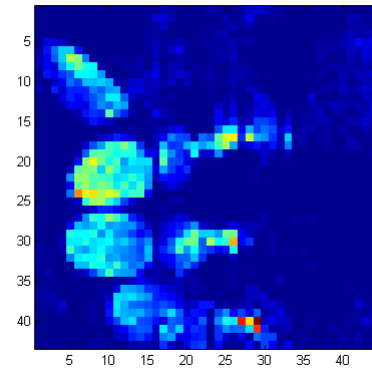


Fig. 2. An example of the hand-grip pattern image

To reduce this type of variation, in the third session, we sounded a beep each time that we finished recording one image. This was to rule out the inaccuracies in the data, caused by the possibility that the subject released the gun, before his hand-grip pattern was recorded. In addition, for each subject, each time when he picked up the gun, we started recording his grip patterns until he released the gun. This type of movie-like recording is for further study of the grip patterns' characteristics in the future. Apart from these, the data was collected in exactly the same way as in the previous two sessions.

IV. EXPERIMENT, RESULTS AND DISCUSSION

In this section, simulation results of the authentication experiment are presented. Subsequently, these results are analyzed from both the view point of the data characteristics and that of the algorithm limitations. Given these analyses, some methods are proposed to improve the authentication performance of the system.

A. Experiment set-up and results

We made two types of simulations in order to evaluate the authentication performance. One was the within-session simulation, where data for both training and testing came from the same session; the other was the across-session simulation, where data collected in two different sessions was used for training and testing, respectively. The authentication performance was assessed by the overall Equal-Error Rate (EER) of all the subjects. This was calculated by taking into account all the likelihood-ratios, of both the genuine subjects and the impostors. In the within-session case, we averaged the overall EERs obtained from 20 runs of simulation as the final result. In each single run, 75% of the data was randomly chosen for training, and thus the rest 25% for testing. The simulation results are presented in Table I and Table II. For easy

comparison, the simulation result by using data collected from the untrained subjects, is also presented in Table I, as Session 0.

Session	EER(%)
0	1.41
1	0.63
2	1.01
3	0.38

TABLE I
WITHIN-SESSION SIMULATION RESULTS

Training session	Testing session	EER(%)
1	2	8.78
2	1	7.02
1	3	23.18
3	1	15.82
2	3	19.36
3	2	19.09

TABLE II
ACROSS-SESSION SIMULATION RESULTS

One can see that when data for training and testing came both from the same session, the reference algorithm worked fairly well, and gave fewer authentication errors, compared to the case where data collected from the untrained subjects was used; while the same algorithm shows relatively worse results, when data collected in two different sessions was used for training and testing, respectively.

Also, we found out that, both the false reject rate (FRR) and the false acceptance rate (FAR) became bigger in the across-session simulation, in comparison with their counterparts in the within-session simulation. Besides, the FRR increased more than the FAR. To give an example, we take the first and the second session for training and testing, respectively, and present these four curves in Fig.3.

A police gun must have a very low FRR, to make it highly unlikely, that the rightful user could not able to fire it. The current official requirement in The Netherlands, for example, is that the FRR of a police gun must be lower than 0.01%. Under this condition, the FAR should be as low as possible. One can see from Fig.3, that in the within-session simulation, the FAR is expected to be less than 10%, when FRR equals 0.01%. However, the FAR is more than 90% under the same condition, in the across-session simulation.

Since in practice, there will always be a time interval between the user enrolment and the live authentication, the

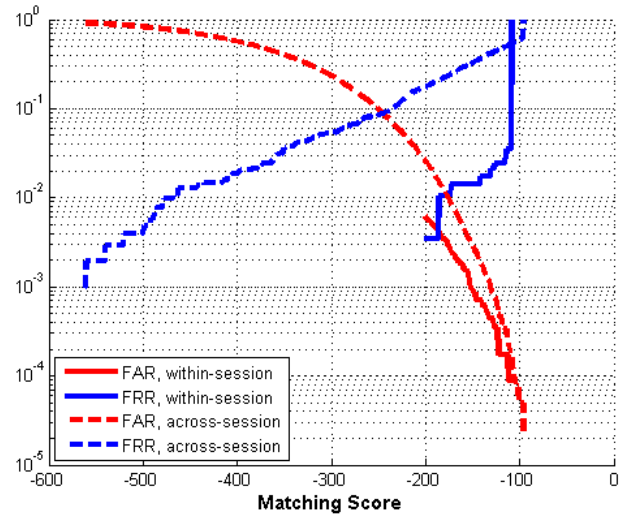


Fig. 3. FAR and FRR curves obtained from the within-session and the across-session simulation

across-session simulation results make more sense. To improve the across-session authentication performance, we need to first find out the reasons for the unsatisfactory simulation results.

B. Data characteristics

Comparing the data recorded from different sessions, we discovered big variations in most of the individual subjects' hand-grip pattern images. That is, for a certain subject, his hand-grip pattern varied greatly on average from one session to another.

Two main factors may contribute to the across-session variations of the same subject. One is the intrinsic factor. That is, for some biological reason, after a certain amount of time, a person's hand-grip pattern tends to change within some certain range. The other one is the extrinsic factor. Since the data acquisition conditions in these three sessions were slightly different, this may also cause the variations of across-session data. Specifically, in the third session we used a beep, while not in the other two sessions. As mentioned in Section 2, this may affect the recording time, and consequently the grip pattern image. Also, two different experimenters were recording data by pressing a button on the laptop, in the first and the second session, respectively. This may also result in different recording times of images, from even the same subject. Because it is very likely, that these two experimenters need different amounts of time, to respond to the subject's "ready" signal, or to press the button.

To find out statistically, how a certain subject's data varies from one session to another, we did an experiment as follows. We first randomly split the test set into two

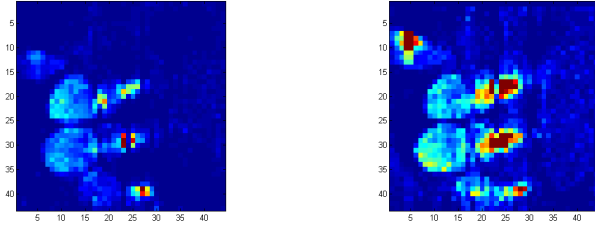


Fig. 4. Hand-grip pattern images of the same subject recorded in two different sessions

equal-sized subsets, namely subset A and subset B; and then used, for example, subset A for testing. Among those four parameters to estimate in the algorithm, we estimated three of them from the training set, yet the fourth one from subset B. We averaged the overall EERs obtained from 50 runs of this type of simulation as the final result. This gives an insight on how much the across-session variation in a certain parameter, affects the authentication performance. For example, we may plug in the mean vector of overall subjects, estimated from the test set B; while use the other three parameters, estimated from the training set.

Table III gives the simulation results. TrSe and TeSe represent the training session and testing session, respectively; *LM* and *LC* represent the mean vector and the covariance matrix of each individual subject's data, respectively; *GM* represents the mean vector of the overall data; and *TM* represents the transformation matrix. To make comparison easier, the across-session simulation results are shown in the third row, represented by *RF*.

TrSe	1	2	1	3	2	3
TeSe	2	1	3	1	3	2
<i>RF</i>	8.78	7.02	23.18	15.82	19.36	19.09
<i>LM</i>	2.95	1.53	2.70	2.95	3.10	3.36
<i>LC</i>	9.09	7.66	23.63	15.56	20.85	18.18
<i>GM</i>	8.89	6.99	23.27	15.79	19.66	19.36
<i>TM</i>	5.46	4.92	14.30	22.20	16.66	19.16

TABLE III

SIMULATION RESULTS IN EER(%) WITH ONE PARAMETER ESTIMATED FROM SUBSET B

Obviously, the across-session variation in the mean value of each individual subject's data, affects the authentication performance the most. When this type of variation is reduced, the authentication performance will be improved dramatically. Fig.5 gives further information about the changes, of the FRR and the FAR, in this type of simulation. Still, we take the first and the second session for training and testing, respectively.

Specifically, for most of the subjects, the pressure of their hand-grip patterns is distributed differently in different sessions (see Fig.4 for an example). Besides, for some subjects, shifts in position of their hands in different sessions have been observed.

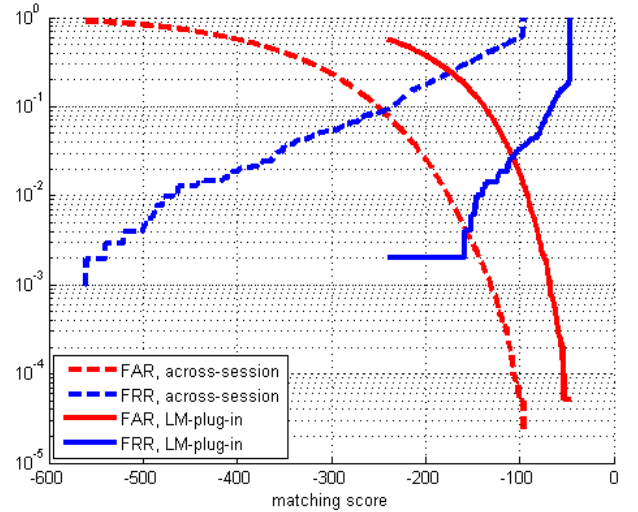


Fig. 5. FAR and FRR curves obtained from the across-session simulation and the *LM*-plug-in simulation

C. Algorithm limitations

The reference likelihood-ratio classifier is probability-density-based, which thus requires estimating the density function (Gaussian density function in our case) from the training data, before classification. In our case it suffers from the small-sample-size problem, since the available training set is relatively small, in comparison with the dimension of the original feature space. We therefore applied PCA twice to reduce the dimension of the feature space. However, this strategy may not suppress the small-sample-size problem well enough. Recently it has been proposed, that the small-sample-size problem and consequently the danger of overtraining, result from the high complexity of the classifier. In addition, the dimension of the feature space by itself, is not a good measure of a classifier's complexity [5]. Thus, even in the space with a lower dimension, the likelihood-ratio classifier may still suffer from overtraining, and thus not have good generalization performance.

Another limitation of the reference classifier is the assumption of Gaussian distributed data. The use of PCA, implicitly assumes that the data has Gaussian probability distribution. Also, the likelihood-ratio classifier is optimal in terms of the expected overall error rates, only when the probability density function of the data is known. Thus, if

this assumption is violated, the reference classifier is sub-optimal.

D. Possible Strategies to Improve the Performance

To improve the authentication performance of the system, we may first consider reducing the across-session variation in each individual subject's mean value. Consequently, we believe, the variations in the other three parameters will be further reduced as well. Some preprocessing of the grip pattern images may help to achieve that. For example, in a hand-grip pattern image, we may try equalizing the local pressure values. This may help to reduce the difference in pressure distribution between two images, of the same subject. Also, registration may help to align those grip patterns, which suffer from shifts in different sessions. In addition, a method useful for face recognition, Elastic Bunch Graph Matching, may be worth trying. It proves especially efficient in coping with variations in the face position, size, pose, and expression [6]. These variations are, at least to some extent, similar to the across-session variations of the same subject in our problem. Thus, this method may bring some improvement in the authentication performance of our system.

Also, we may turn to some other type of classifier. Taking into account the limitations of the reference classifier, the Support Vector Machine (SVM) seems a promising choice. The SVM builds an optimal classifier, and meanwhile controls its complexity to gain the generalization power. Further more, the SVM does not rely on any assumption specifically about data's characteristics [5]. Besides, in some preliminary simulation results with the grip pattern data, the SVM has been proved to be more robust to overtraining, compared to the reference classifier.

Certainly, these two solutions could be combined. Any proper preprocessing methods would also be helpful to a new type of classifier. Besides, it is very likely, that no classifier could solve the overtraining problem in question by itself, even if it has good generalization performance.

V. CONCLUSIONS

This smart gun system has been proved to be useful for authentication, with hand-grip pattern data collected from the police officers. This certainly ensures its potential to be used by the police in the future. However, its authentication performance needs to be further improved to meet the safety requirement of a real police gun.

Simulation results of authentication experiment have been analyzed, in terms of both the data characteristics, and the algorithm limitations. We discovered a big variation in the mean value of each individual subject's data, in different sessions. This type of variation is the main reason

for the unsatisfied performance of the current algorithm. Accordingly, we may apply some proper preprocessing methods to reduce this variation. Also, improvements may be expected, by using some other classifier, especially one with better generalization performance. SVM, for example, may be a good choice.

REFERENCES

- [1] The national Uniform Crime Reporting Program, "Law Enforcement Officers Killed and Assaulted", tech. rep., Federal Bureau of Investigation, 2001.
- [2] Raymond Veldhuis, Asker Bazen and Joost Kauffman, "Biometric verification based on grip-pattern recognition", presented at *SPIE*, 2004.
- [3] Asker Bazen and Raymond N.J. Veldhuis, "Likelihood-Ratio-Based Biometric Verification", *IEEE Transactions on circuits and systems for video technology*, vol. 14, no. 1, January, 2004.
- [4] H.L. Van Trees, *Detection, Estimation, and Modulation Theory*, New York: Wiley, 1968.
- [5] V.N. Vapnik, *The Nature of Statistical Learning Theory*, Springer, 1995.
- [6] Laurenz Wiskott, Jean-Marc Fellous, Norbert Krüger, and Christoph von der Malsburg, "Face recognition by Elastic Bunch Graph Matching", *IEEE Transactions on pattern analysis and machine intelligence*, vol. 19, no. 7, July, 1997.