# Recognition of Biometric Unlock Pattern by GMM-UBM

M Erdal Özbek, Mohamed Amine Haytom, Estelle Cherrier

# GKM-GAM ile Kilit Deseni Biyometrisi Tanıma
# Recognition of Biometric Unlock Pattern by GMM-UBM

*M. Erdal Özbek, Mohamed Amine Haytom, Estelle Cherrier*
Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, 14000 Caen, France
{erdal.ozbek,amine.haytom,estelle.cherrier}@ensicaen.fr

February 28, 2019

**Abstract**

Unlock patterns are used for authentication in mobile smart devices, yet they are vulnerable to attacks, since only the pattern draw is required. Extra biometric data of the user while drawing the unlock pattern passwords may strengthen the authentication, such as the speed of drawing, the pressure of the finger on the touch screen. Such biometric modality is referred to as behavioral biometrics. Besides, voice is also a behavioral biometric modality, as well as a physiological one. Hence, statistical models such as Gaussian mixture models (GMM) with universal background modeling (UBM) are widely used in speaker verification systems. In this work, we propose to apply and adapt a framework usually dedicated to speaker verification to recognize the unlock patterns based on users' behavior. We evaluate the performance using equal error rate for different combinations of features and varying number of mixtures. As a result of the combination of features, an equal error rate as low as 9.25% on average is obtained, which is promising for a preliminary study on GMM-UBM applied to unlock pattern based biometric recognition.

## 1 Introduction

Biometrics refers to physiological or behavioral characteristics of an individual [JRP06]. These characteristics are mainly used for authentication purpose in security systems or applications, due to their advantages over traditional systems in verification and identification steps. They are unique for each person and difficult to copy, they cannot be separable, thus they cannot be lost nor forgotten as in the case of text- or number-based passwords commonly known as Personal Identity Numbers (PINs). Moreover, biometric recognition is based on *what you are*, or on *how you do things*, like your signature, your gait, your way of typing on a keyboard, etc, therefore

it is the only authentication method that allows to authenticate the user, rather than her/his mobile phone, smart card or any secret she/he knows.

As the number of mobile smart devices is rapidly increasing, their utility and associated security issues become more vital. Frequent usage of these devices requires repeatedly entering PINs or passwords. For example, in a typical usage of smartphones, the users unlock their phones many times a day, such as on an average of 47.8 [Har+14; Col+16]. Thus, today, mobile smart devices with touchscreen have an option for securing the device using unlock patterns replacing PINs. Unlock patterns are simple recall-based graphical passwords that can be used for authentication [Liu+11; BCO12]. Generally, in a grid of $n \times m$ nodes (e.g., $4 \times 4$, see Figure 1), the user defines a graph that begins from a node and passes through other nodes. Unlocking is simply done by drawing the saved pattern made by joining four or more node points by fulfilling other rules [SWZ14].

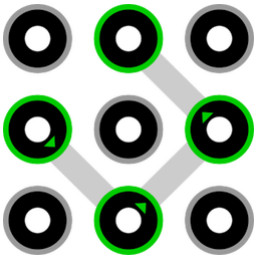

Figure 1: An example of unlock pattern shape.

However, the unlock pattern is vulnerable to (i) side-channel attacks [Nah16], where all the operations performed in the mobile device are eavesdropped by the intruder; (ii) smudge attacks [Avi+10], where the intruder takes advantage of the trace of the finger left on touchscreen device; and (iii) shoulder-surfing attacks [Wie+06], where the intruders spy the user while drawing his/her pattern, see [Col+16] for a thorough study of the different types of attacks. Therefore, the inherent biometric information gathered while drawing the unlock pattern passwords may strengthen the authentication with a good usability [AW12; BMR13]. During the enrollment phase, the user's biometrics data can be stored. These can be the location of the finger, the time elapsed to draw the pattern, the pressure of the finger or similar information. In the verification phase, the unlock pattern application compares the data with the enrollment phase in order to authenticate the user.

On the other hand, in voice biometrics, statistical models are used to represent acoustical features of people to distinguish users for authentication. The aim is to design a system that extracts user-specific features which minimizes the probability of verification errors calculated from the scores in the

testing phase. Today, Gaussian mixture model (GMM) lies at the core of the speaker recognition systems where the features are represented by Gaussian probability density functions (PDFs) [RQD00]. For a recent overview on this subject, the reader is referred to the reference [HH15]. In this work, we propose to use these statistical models for both investigation and evaluation of the user biometrics that emerge from unlock patterns collected by a developed Android application as in [BMR13].

The rest of the paper is organized as follows. In Section 2, we present a brief summary of statistical models used for the verification system. We then explain how the biometric unlock pattern is collected in Section 3. We evaluate the biometrics data and give performance results for various parameters in Section 4. In the final section, we conclude by discussing the results.

# 2 Material and method

## 2.1 Biometric systems performance evaluation

Biometric recognition systems involve two steps. The first step concerns the user enrollment: Enrollment means the capture of the biometric raw data, the extraction of features to define a model (which is stored as a reference) of each genuine user and its storage (if the template meets some quality requirements). For unlock pattern based systems, the concerned biometric data is the dynamic pattern, and the extracted features (see Section 3) are stored in the mobile phone memory. In the second step called verification, the system must decide if the user draws the expected pattern, in the expected manner: the features extracted from the present pattern are compared to the stored features.

More precisely, the performance evaluation is based on the match score between the enrolled user and the test user, where the system decides based on a decision threshold. Thus, in the verification system, two types of errors are defined. When a valid identity claim is rejected, a false rejection (miss) error occurs. Conversely, when an identity claim from an impostor is accepted, a false acceptance (false alarm) error appears. The error rates are defined as the ratios of the number of the errors to the number of attempts by False Non Match Rate (FNMR) and False Match Rate (FMR), respectively [RNJ06]. A very popular performance measure is the equal error rate (EER) where these two values (FMR and FNMR) become equal. In this work, we will use EER values for performance evaluation.

## 2.2 Unlock pattern recognition

Only a few references mention studies about unlock pattern based mobile authentication systems. We can cite [AW12], where the authors present

their initial explorations of the use of unlock pattern dynamics as a secure and user-friendly two-factor authentication based on random forest machine learning classifier, which allows them to obtain an EER of 10.39% (with 32 users). In [Col+16], an improvement of the standard biometric unlock pattern system is proposed (with 36 users). It is not analyzed in terms of EER, but in terms of security enhancement. A statistical classifier for authentication is developed in [Liu+11], where time, pressure, size, and angle features are collected from 113 participants. However, not all smartphones can provide all these features. This paper also presents a comparison with existing keystroke dynamics interactions on mobile phones (PIN, character strings). Artificial intelligence approaches are proposed in [Alp15], with 3 classifiers, namely artificial neural networks, adaptive neuro-fuzzy inference systems and histogram methods in verification phase. 35 volunteers are considered as genuine users, while 10 others imitate fraud attempts. In the different experiments, various values of EER ranging from 2.5% to 8.75% are achieved, but these experiments are based on the emulation of a smartphone touchscreen with Matlab and the touchscreen of a computer, the author does not use a real smartphone unlike other studies.

### 2.3 Statistical models for voice recognition

A GMM is a mixture of Gaussian PDFs parameterized by a number of mean vectors, covariance matrices, and mixture weights [RQD00]. Therefore, a GMM PDF, denoted by $\lambda$, is given by

$$p(\mathbf{x}|\lambda) = \sum_{i=1}^{N} P_i \mathcal{N}(\mathbf{x}|\boldsymbol{\mu}_i, \boldsymbol{\Sigma}_i), \tag{1}$$

where $N$ is the number of Gaussian components, $P_i$ is the prior probability (mixing weight) of the $i$th Gaussian component, and

$$\mathcal{N} = (2\pi)^{-\frac{d}{2}} |\boldsymbol{\Sigma}_i|^{-\frac{1}{2}} \exp\left\{ -\frac{1}{2} (\mathbf{x} - \boldsymbol{\mu}_i)^T \boldsymbol{\Sigma}_i^{-1} (\mathbf{x} - \boldsymbol{\mu}_i) \right\} \tag{2}$$

is the d-variate Gaussian density function with mean vector $\boldsymbol{\mu}_i$ and covariance matrix $\boldsymbol{\Sigma}_i$. The prior probabilities $P_i \geq 0$ are constrained to sum up to unity.

In order to estimate the model parameters from a training sample $\mathcal{X} = \{\mathbf{x}_1, \ldots, \mathbf{x}_T\}$, the basic approach is to use maximum likelihood (ML) estimation. Usually, the feature vectors of $\mathcal{X}$ are assumed to be independent. Therefore, the average log-likelihood of $\mathcal{X}$ with respect to model $\lambda$ is defined as

$$LL_{avg} = \frac{1}{T} \sum_{t=1}^{T} \log \sum_{i=1}^{N} P_i \mathcal{N}(\mathbf{x}_t|\boldsymbol{\mu}_i, \boldsymbol{\Sigma}_i), \tag{3}$$

where the expectation maximization (EM) algorithm which iteratively increases the likelihood can be used to maximize the log-likelihood.

In order to adapt to different users, dynamic operation and environment conditions, user-independent world model or universal background model (UBM) may be used. As UBM represents user-independent distribution of the feature vectors, when enrolling a new user to the system, the parameters of UBM are adapted. Thus, model parameters are not estimated each time for each user from scratch, instead they are estimated using a prior knowledge on general user data.

The adaptation of UBM parameters can be performed using maximum a posteriori (MAP) adaptation principle [RQD00; Bim+04; KL10; HH15]. Given the enrollment sample and the UBM, $\lambda_{UBM}$, the probabilistic alignment of the training vectors to the UBM parameters is obtained for the $i$th mixture by

$$P(k|\mathbf{x}_t) = \frac{P_i \mathcal{N}(\mathbf{x}_t|\boldsymbol{\mu}_i, \boldsymbol{\Sigma}_i)}{\sum_{n=1}^{N} P_n \mathcal{N}(\mathbf{x}_t|\boldsymbol{\mu}_n, \boldsymbol{\Sigma}_n)}. \tag{4}$$

Using the $P(k|\mathbf{x}_t)$ and $\mathbf{x}_t$, sufficient statistics for the weight, mean, and variance parameters are computed. These quantities are known as the zero-, first-, and second-order Baum-Welch statistics, respectively.

When the MAP-adapted GMM model and the UBM are combined, the commonly referred GMM-UBM system is obtained. Then the difference of the target ($\lambda_T$) and background ($\lambda_{UBM}$) models can be measured via the average log-likelihood ratio given by

$$LLR_{avg} = \frac{1}{T} \sum_{t=1}^{T} \{\log p(\mathbf{x}_t|\lambda_T) - \log p(\mathbf{x}_t|\lambda_{UBM})\}. \tag{5}$$

# 3 Our proposal

## 3.1 Data collection

For this work, unlock pattern data from 31 users working in the GREYC laboratory is collected using Nexus 5 Android mobile phone. This number of volunteers is not so high, but it is in the same range as in the published studies (see section 2.2). Each user is asked to enter the predefined unlock pattern at least ten times correctly. More precisely, the pattern is imposed and it is the same for each user and each session. During data acquisition, the following data have been saved for each session: time information (T), coordinates of the horizontal and vertical axes (X and Y), and pressure (P) of the finger while drawing the unlock pattern.

Figure 2 displays an example of the coordinate information (XY) collected from a single user. The shape of the unlock pattern and the variations in drawing each of the unlock pattern can be easily recognized.

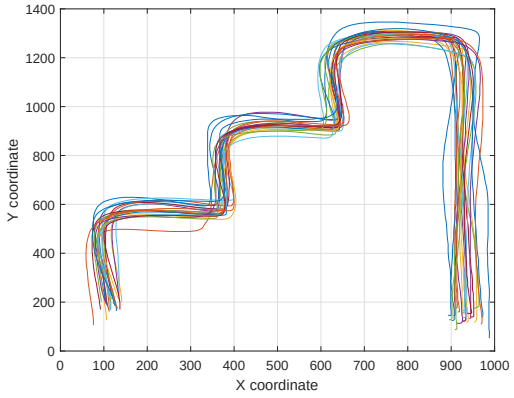


Figure 2: An example of unlock pattern coordinate information.

### 3.2 Our approach

In this paper, we propose to use a technique devoted to speaker recognition, namely GMM-UBM method, to perform unlock pattern verification. Indeed, either voice features or unlock pattern features are time-varying signals, and these two modalities are behavioral ones (more precisely, voice modality is both a physiological and a behavioral modality). Based on the method presented in section 2.3, Baum-Welch statistics have been computed for each user. The EM algorithm has been applied to maximize the log-likelihood at least with 5 iterations, which is generally accepted sufficient for convergence. The log-likelihood values have been used as scores for target (genuine) and impostor trials to determine the EER values.

In order to explore the effect of the number of mixtures on the performance, varying number of mixtures for Gaussian PDFs have been tested.

### 3.3 Evaluation

The evaluation of biometric verification system is performed by the EER measure given in percentage. For the experiments performed in this work, two thirds of the data has been used for enrollment and the remaining has been left for verification. For each of the group of features and number of Gaussian mixtures cases, an average value of EERs is obtained by computing randomly generated 100 iterations.

The performance is also investigated for different group of features which are dubbed by their initials (e.g., T for time and P for pressure).

## 4 Results

As the major information of the users' biometrics resides while plotting the unlock pattern, we first considered the XY coordinate information. We made

performance comparisons with respect to different number of mixtures in GMM-UBM. Figure 3 displays the EER percentage for increasing number of mixtures. An average of 14% EER is obtained while relatively higher EER values are due to small number of mixtures unable to sufficiently represent the data.

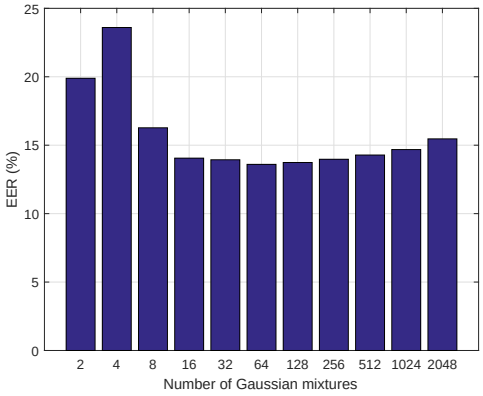


Figure 3: Performance comparison for different number of Gaussian mixtures.

Another direction of investigation was to determine which of the information collected from the unlock pattern is more useful. For this purpose, we grouped features for a fixed number of mixtures (i.e., 32) and obtained the average EER for each of the cases. The recognition performance is obtained as shown in Figure 4.

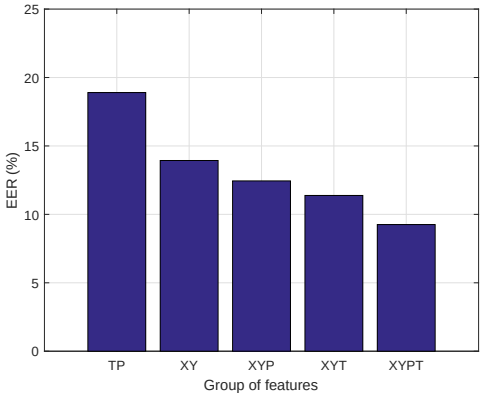


Figure 4: Performance comparison for different groups of features.

The best EER results are achieved as low as 9.25% with the features composed of the coordinates, time, and pressure information. Although the pressure data values take similar values due to the resolution of the sensor of

the Android device, they have an impact on the performance when combined with coordinate information. This can be seen from the comparison with XY and XYP, as well as with XYT and XYPT. Similarly, one can deduce the same conclusion for the time information from the comparison of XY with XYT and XYP with XYPT.

## 5 Conclusion

In this work, we investigated the biometric information hidden in the unlock pattern dynamics for better security password applications. The novelty of the paper is being the first application of the state-of-the-art speaker recognition models (GMM-UBM) to investigate and recognize the unlock pattern information.

We evaluated the performance using EER measure and obtained a recognition of as low as 9.25%. As of our knowledge there is no work using GMM-UBM for unlock pattern recognition and presenting performance less than 10% EER. Results also demonstrated that the combination of time and pressure information with coordinates have lower error rates.

Since there is no large available common dataset for unlock pattern studies, the experiment is performed with a limited number of users, like almost all the existing studies. Nevertheless, we expect better results with increasing number of users due to the performance of the GMM-UBM already shown in voice biometrics.

## References


[Col+16] Ashley Colley, Tobias Seitz, Tuomas Lappalainen, Matthias Kranz, and Jonna Häkkilä. "Extending the Touchscreen Pattern Lock Mechanism with Duplicated and Temporal Codes". In: *Advances in Human-Computer Interaction* 2016 (2016).

[Nah16] Ani Nahapetian. "Side-Channel Attacks on Mobile and Wearable Systems". In: *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. Las Vegas, NV, USA, Jan. 2016, pp. 243–247.

[Alp15] Orcan Alpar. "Intelligent biometric pattern password authentication systems for touchscreens". In: *Expert Systems with Applications* 42 (2015), pp. 6286–6294.

[HH15] J. H. L. Hansen and T. Hasan. "Speaker Recognition by Machines and Humans: A tutorial review". In: *IEEE Signal Processing Magazine* 32.6 (Nov. 2015), pp. 74–99.

[Har+14] Marian Harbach, Emanuel von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. "It's a Hard Lock Life: A Field Study of Smartphone (Un)Locking Behavior and Risk Perception". In: *Symposium on Usable Privacy and Security (SOUPS)*. Menlo Park, CA, USA, July 2014, pp. 213–230.

[SWZ14] Chen Sun, Yang Wang, and Jun Zheng. "Dissecting pattern unlock: The effect of pattern strength meter on pattern selection". In: *Journal of Information Security and Applications* 19.4-5 (Nov. 2014), pp. 308–320.

[BMR13] Michael Beton, Vincent Marie, and Christophe Rosenberger. "Biometric Secret Path for Mobile User Authentication: A Preliminary Study". In: *World Congress on Computer and Information Technology (WCCIT)*. Sousse, Tunisia, Oct. 2013.

[AW12] Julio Angulo and Erik Wästlund. "Exploring Touch-Screen Biometrics for User Identification on Smart Phones". In: *Privacy and Identity Management for Life: 7th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Trento, Italy, September 5-9, 2011, Revised Selected Papers*. Ed. by Jan Camenisch, Bruno Crispo, Simone Fischer-Hübner, Ronald Leenes, and Giovanni Russello. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 130–143. ISBN: 978-3-642-31668-5. DOI: 10.1007/978-3-642-31668-5_10.

[BCO12] Robert Biddle, Sonia Chiasson, and P. C. van Oorschot. "Graphical Passwords: Learning from the First Twelve Years". In: *ACM Computing Surveys* 44.4 (Aug. 2012).

[Liu+11] Xi-Yang Liu, Hai-Chang Gao, Li-Ming Wang, and Xiu-Ling Chang. "An Enhanced Drawing Reproduction Graphical Password Strategy". In: *Journal of Computer Science and Technology* 26.6 (Nov. 2011), pp. 988–999.

[Avi+10] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. "Smudge Attacks on Smartphone Touch Screens". In: *4th USENIX Workshop on Offensive Technologies (WOOT)*. Washington DC, USA, Aug. 2010.

[KL10] Tomi Kinnunen and Haizhou Li. "An Overview of Text-independent Speaker Recognition: From Features to Supervectors". In: *Speech Communication* 52.1 (Jan. 2010), pp. 12–40. ISSN: 0167-6393.

[JRP06] Anil K. Jain, Arun Ross, and Sharath Pankanti. "Biometrics: A Tool for Information Security". In: *IEEE Transactions on Information Forensics and Security* 1.2 (June 2006), pp. 125–143.

[RNJ06] A. A. Ross, K. Nandakumar, and A. K. Jain. *Handbook of Multibiometrics*. Ed. by Springer. 2006.

[Wie+06] Susan Wiedenbeck, Jim Waters, Leonardo Sobrado, and Jean-Camille Birget. "Design and evaluation of a shoulder-surfing resistant graphical password scheme". In: *Working Conference on Advanced Visual Interfaces (AVI)*. Venezia, Italy, May 2006, pp. 177–184.

[Bim+04] Frédéric Bimbot et al. "A Tutorial on Text-Independent Speaker Verification". In: *EURASIP Journal on Advances in Signal Processing* 2004.4 (2004), pp. 430–451.

[RQD00] Douglas A. Reynolds, Thomas F. Quatieri, and Robert B. Dunn. "Speaker Verification Using Adapted Gaussian Mixture Models". In: *Digital Signal Processing* 10.1 (2000), pp. 19–41.