

# Survey Explanation Sheet

- **Important information before survey**

This survey is part of a research project conducted at **LaBRI, University of Bordeaux**. This survey is anonymous. Your personal information will be kept strictly confidential. Age and gender information will only be used for statistical purposes. **By starting the survey, you confirm that you have read and agreed to the above information.**

- **What is a Biometric Authentication System?**

A Biometric Authentication System is a system used to verify that you are who you claim to be. For example, when you use facial recognition to unlock your phone, we need to confirm that it's really you using it. The phone's system will retrieve your stored biometric data and compare it with your current face scan. Typically, this comparison yields a similarity score ranging from 0 to 100, where 0 means completely different and 100 means identical. If the score in this authentication attempt exceeds a threshold—say, 80—you successfully unlock your phone.

- **How is a Biometric Authentication System evaluated?**

Biometric Authentication Systems vary in quality. A perfect system would always correctly verify you and never allow an imposter. Continuing with the phone-unlock example, a perfect system would successfully unlock your phone with your own face every time, and no one else could ever unlock it with their face. In reality, no system is perfect, so we use two metrics to assess performance: FNMR and FMR. FNMR (False Non-Match Rate) is the proportion of times you try to authenticate with your own identity but are incorrectly rejected. FMR (False Match Rate) is the proportion of times someone else tries to authenticate with their own identity but is incorrectly accepted. For each user, there are actually two kinds of FMR situations: One is when someone else tries to unlock your device and succeeds — this error rate is called **FMR In**. The other is when you try to unlock someone else's device and succeed — this error rate is called **FMR Out**. FMR is the average of FMR In and Out.

You may notice that choosing different thresholds yields different error rates. For example, suppose your own match scores are 90, 75, and 60, and an imposter's scores are 30, 50, and 65. No matter where you set the threshold, some errors occur: a threshold of 55 lets the imposter's 65 through, while a threshold of 70 wrongly rejects your 60. Selecting an appropriate threshold is crucial; in our experiment, we choose the threshold where  $FMR = FNMR$ . To accurately evaluate a system, we need to understand its FNMR and FMR characteristics. A simplified example: we have 10 users' phones, all using the same Biometric Authentication System under test. We attempt to unlock each phone with User 1's face, then each with User 2's face, and so on, recording every similarity score. From these data, we derive the system's performance metrics.

- **What is the Biometric Menagerie?** Similar to the biometric system different perform differently. Some users are often wrongly rejected, and some are easily impersonated. We want to identify the worst-performing users in the Biometric Authentication System. Researchers classify these users using animal nicknames. Starting with the poorest performers:

- **Goat:** Users with the worst FNMR performance; they frequently fail to be recognized with their own biometric (e.g., Goat users often cannot unlock their phones).
- **Lamb:** Users with the worst FMR In performance; they are easily impersonated by others (e.g., Lamb users' phones are frequently unlocked by someone else).
- **Wolf:** Users with the worst FMR Out performance; they can easily unlock other people's phones with their own biometric (e.g., Wolf users often unlock others' phones with their face).

These categories are not mutually exclusive; a user can be both a Wolf and a Lamb, for example. Users who do not fall into any of the above "animal" categories are considered to perform well:

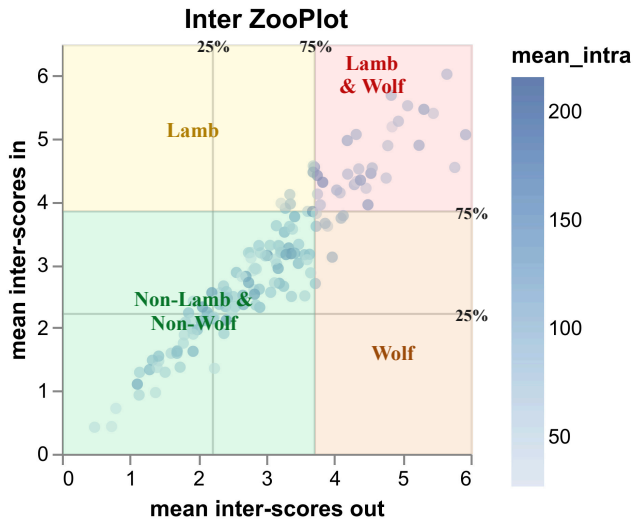
- **Sheep:** Well-performing users, making up the vast majority of the Biometric Authentication System.

- **What should I do in this survey?**

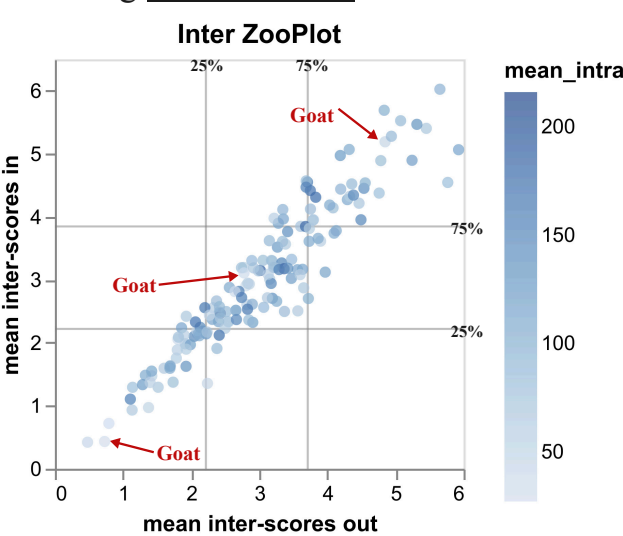
We wish to investigate how two types of Biometric Authentication System evaluation tools perform. You are invited to participate in this survey. In the questionnaire, you will classify users according to these categories using two different tools. Before you begin, you will first complete 5 pretest questions before starting the actual survey to help you understand the testing process. At the end of the experiment, you will be asked to rate the tools based on two aspects: ease of use and confidence in your decisions.

# How to use ZooPlot/Inter ZooPlot ?

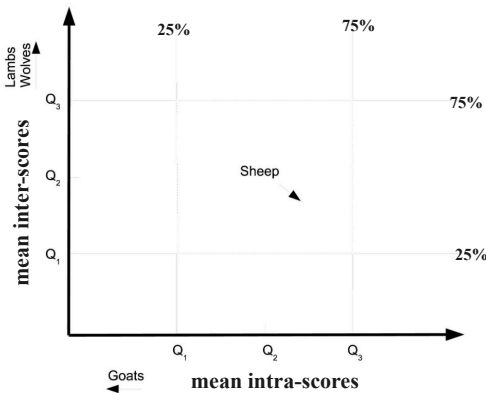
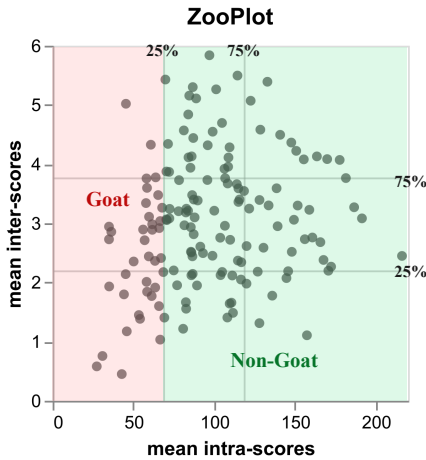
- How to determine whether it is a **Lamb** or a **Wolf** using **Inter ZooPlot**?



- How to determine whether it is a **Goat** using **Inter ZooPlot**?



- How to determine whether it is a **Goat** using **ZooPlot**?



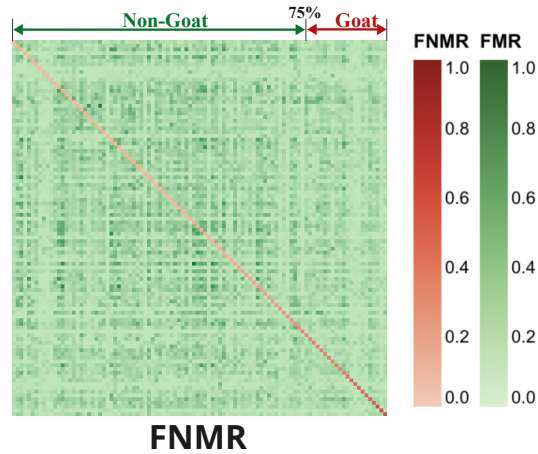
- How to determine what kind of **animal** the user is?

Intra Score (FNMR Performance)	Inter-score In (FMR IN Performance)	Inter-score Out (FMR Out Performance)	Menagerie
High (Good)	Low (Good)	Low (Good)	Sheep
High (Good)	Low (Good)	High (Bad)	Wolf
High (Good)	High (Bad)	Low (Good)	Lamb
High (Good)	High (Bad)	High (Bad)	Wolf & Lamb
Low (Bad)	Low (Good)	Low (Good)	Goat
Low (Bad)	Low (Good)	High (Bad)	Goat, Wolf
Low (Bad)	High (Bad)	Low (Good)	Goat, Lamb
Low (Bad)	High (Bad)	High (Bad)	Goat, Wolf & Lamb

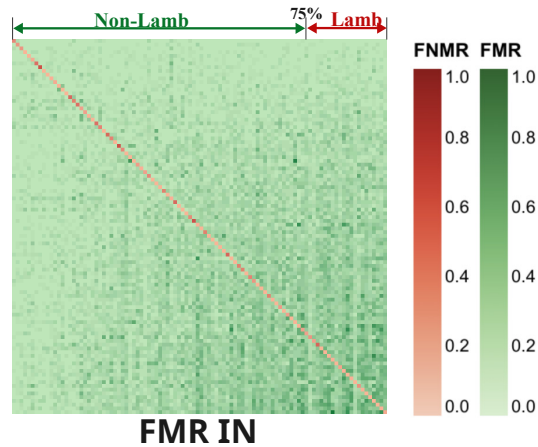
**Note:** If the user is a **Wolf**, **Lamb**, or **Goat** (Poor performing users), then they cannot be a **Sheep** (Well performing user).

# How to use BCM ?

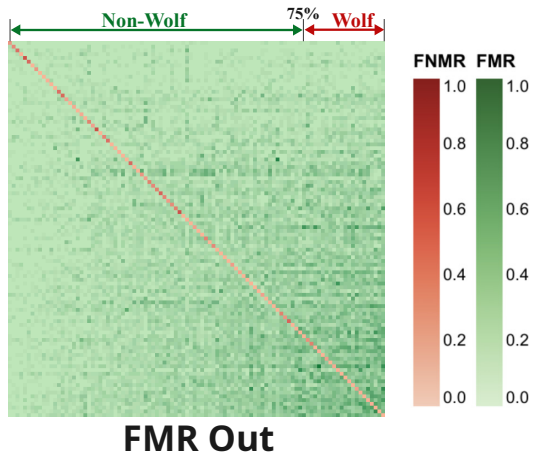
- How to determine whether it is a **Goat** using **FNMR BCM**?



- How to determine whether it is a **Lamb** using **FMR IN BCM**?



- How to determine whether it is a **Wolf** using **FMR Out BCM**?



**Note:** If the user is a **Wolf**, **Lamb**, or **Goat** (Poor performing users), then they cannot be a **Sheep** (Well performing user).