Biometrics

Chandrasekhar Bhagavatula
Stephen Siena

March 18, 2014

Electrical & Computer ENGINEERING

Today's Lecture

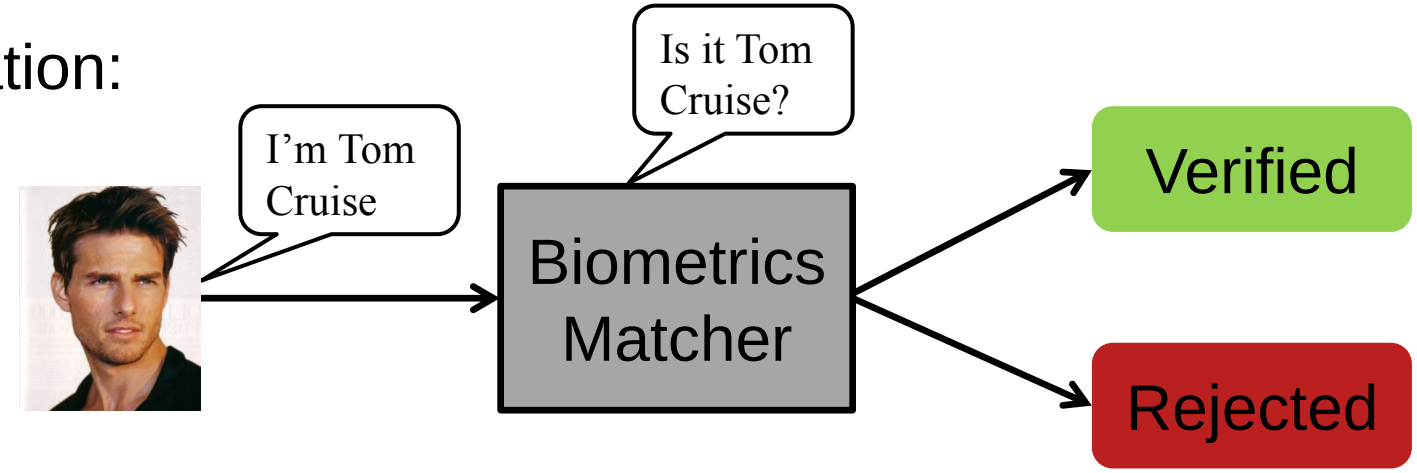
- What is a biometric?
- Strengths and weaknesses
- Challenges and concerns
- Group discussion
- Biometrics in smartphones
- Fun and thrilling demos

What is a biometric?

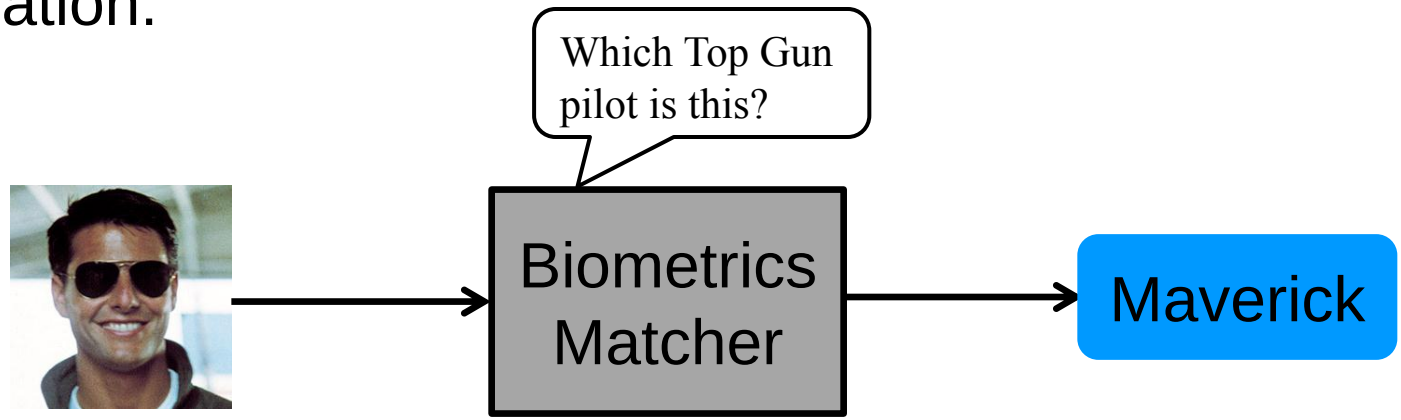
- "Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic."
  - *The Biometric Consortium*

What is the goal of biometrics?

- Verification:



- Identification:



Perception vs. Reality

- CSI
- It may not be as far-fetched as you think though.
- Some state of the art work has been able to use very low-resolution faces in facial recognition. Part 1, Part 2

Demo – Part 1

- Enrollment
  - Capturing a biometric and storing it for later comparison

Types of Biometrics

- “Physiological”

Types of Biometrics

- "Physiological"
  - Face
  - Iris
  - Fingerprint
  - Ear
  - Teeth
  - DNA
  - Heartbeat

Types of Biometrics

- “Behavioral”

Types of Biometrics

- "Behavioral"
  - Gait
  - Keystrokes
  - Mouse movements
  - Voice
  - Signature

What is important for a password?

- Hard to guess
- Quick to use
- Easy to:
  - Remember
  - Match
  - Change

Text vs. biometric passwords

	Text Passwords	Biometrics
Easy to remember	Often competing values	Easy!
Quick to use		Variable; depends on biometric
Hard to guess		
Easy to match	Easy!	
Easy to change	Easy!	Challenging!

Challenges in Biometrics

- Many biometrics are constantly changing
- **Every** biometric is measured differently each time

Challenges in Biometrics

- Environmental factors that affect biometrics

Challenges in Biometrics

- Environmental factors that affect biometrics
  - Lighting
  - Occlusion/Clothing
  - Different sensors
  - Resolution
  - Pose
  - Expression
  - Lots more…

Challenges in Biometrics

- The (good?) news:
  - Advances are being made in handling these challenges
  - Most recently: Facebook

DeepFace: Closing the Gap to Human-Level Performance in Face Verification

Yaniv Taigman, Ming Yang, Marc'Aurelio Ranzato, Lior Wolf

Conference on Computer Vision and Pattern Recognition (CVPR)

Abstract

In modern face recognition, the conventional pipeline consists of four stages: detect => align => represent => classify. We revisit both the alignment step and the representation step by employing explicit 3D face modeling in order to apply a piecewise affine transformation, and derive a face representation from a nine-layer deep neural network. This deep network involves more than 120 million parameters using several locally connected layers without weight sharing, rather than the standard convolutional layers. Thus we trained it on the largest facial dataset to-date, an identity labeled dataset of four million facial images belonging to more than 4,000 identities, where each identity has an average of over a thousand samples. The learned representations coupling the accurate model-based alignment with the large facial database generalize remarkably well to faces in unconstrained environments, even with a simple classifier. Our method reaches an accuracy of 97.25% on the Labeled Faces in the Wild (LFW) dataset, reducing the error of the current state of the art by more than 25%, closely approaching human-level performance.

Privacy Concerns

- As biometrics get easier to use, so does the ability to use biometrics covertly
- Also possibility of having your biometric stolen (compared to a password)

Group Discussion

- Scenario: A bank wants to switch their ATMs to use face recognition to replace the use of PINs.

- Would you want your bank to do this?
- What are possible advantages and disadvantages to this proposal?

Smartphone Biometrics

- Both Google and Apple have introduced some form of biometric authentication on their smartphones

Smartphone Biometrics

- Potential Advantages
  - More secure
  - Easier unlocking of phone
- Potential Problems
  - Do you want Google or Apple to have your biometrics at all times?

Smartphone Biometrics

- Both have been easily broken
- Google tried to fix it by adding a liveness checking option where they required a blink. (It doesn't really help)
- Face unlock broken
- Fingerprint unlock broken

Demo – Part 2!

- Matching (Verification)
  - User claims an identity and presents their biometric
  - System accepts or rejects them

Thank you!

17- Related Work Sections

Lorrie Cranor and Blase Ur
March 18, 2014

05-436 / 05-836 / 08-534 / 08-734
Usable Privacy and Security

Carnegie Mellon University
CyLab

institute for SOFTWARE RESEARCH

Engineering & Public Policy

Why do we cite related work?

- Lay the groundwork for our work
- Put our work in context
- Highlight advantages of our approach
- Identify shortcomings of other approaches (or our approach!)
- Identify problems that have already been solved or are out of scope
- Show that we are knowledgeable

Where do you start?

- Identify papers that might be related
  - Google Scholar
  - ACM digital library
  - IEEE online library
- Then add in papers that the most relevant papers cite (and papers that cite the most relevant papers)
- Skim the abstracts before reading

A good related work section...

- ...ties papers together into themes
- ...makes clear what other researchers have done (and have not done)
- ...makes it clear that you have chosen a good problem to work on
- ...shows what work your approach builds upon (or parallels)
- ...shows how your work is different!!!

Good practices

- Marsh et al. also investigated ponies, though they focused on pony color [4]. In a 44-pony user study, they found that purple ponies had greater privacy concern than green ponies. Instead, we focus on how hair length impacts ponies' privacy attitudes.

Good practices

- A number of groups have performed formative investigations into how pony activists use TOR. Cruise interviewed 12 ponies about their use of anonymity tools, finding that configuration errors commonly lead to a loss of anonymity [5]. We build on their work by pinpointing the precise usability flaws that cause this loss of anonymity.

Bad practices

- Other researchers [1, 4, 5, 6] have also studied pony passwords. We study pony passwords better.

Bad practices

- Bauer et al. studied 1500 ponies' passwords, finding that “Kentucky Derby” was the most popular pony password [5]. Cranor et al. studied 1400 monkeys' passwords, finding that “PonyMonkey” was a common password [6]. Kelley et al. interviewed 38 ponies and 23 horses in a lab on the campus of Carnegie Mellon University in 2003 and published the results in CCS [7].

Other bad practices

- Citing every paper you ever read
- Not grouping papers into themes
- Listing too much information about a particular paper
- Not citing something that's related because they were too similar
- Only citing yourself
- Referring to “this paper did this”