Southern Connecticut State University

SC SU

Open Code Biometric Tap Pad

A solution to the problem of weak smartphone security practices

Presenter:
Md Shafaeat Hossain, PhD
Associate Professor, Computer Science Department
Southern Connecticut State University

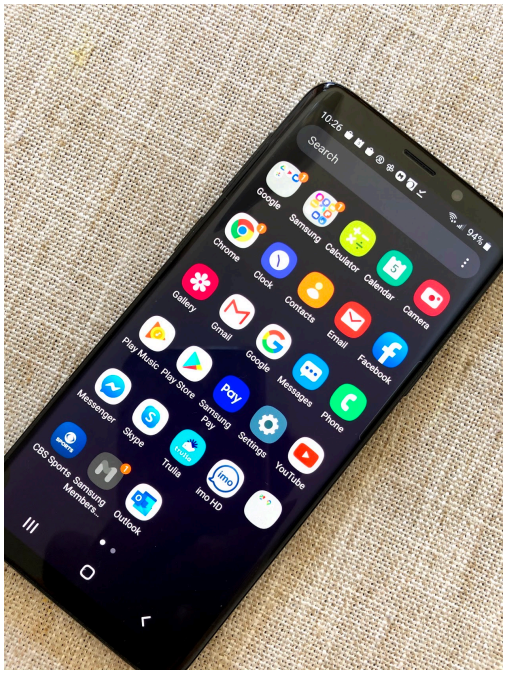
Mohamed Rilvan

- Undergraduate student
- Started research with me in the 2nd semester, while taking CSC153
- Publication:
  - M. A. Rilvan, K. I. Lacy, M. S. Hossain and B. Wang, "**User authentication and identification on smartphones by incorporating capacitive touchscreen**,"IEEE International Performance Computing and Communications Conference (IPCCC), Las Vegas, NV, USA, 2016, pp. 1-8.

  - M. A. Rilvan, J. Chao and M. S. Hossain, "**Capacitive Swipe Gesture Based Smartphone User Authentication and Identification**," 2020 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA), Victoria, BC, Canada, 2020, pp. 1-8.

Mohamed's Research: Smartphone User Authentication

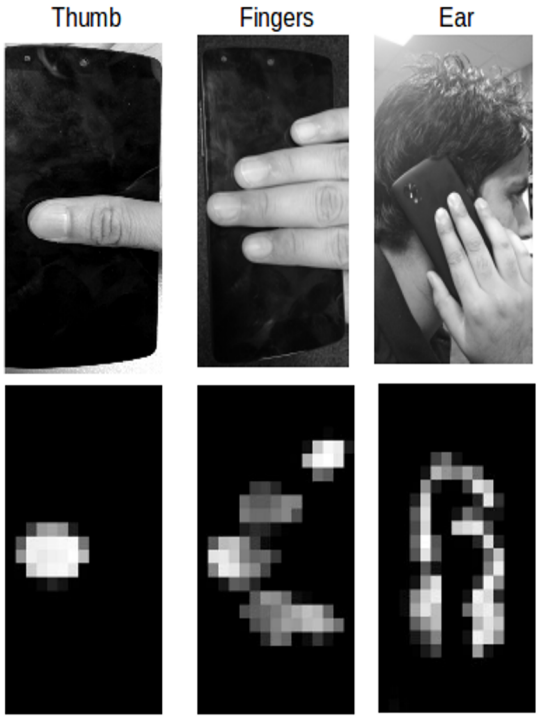
- While many technologies have integrated into daily human life, few have had more impact than the smartphone.
  - Number of smartphone users in the world is expected to exceed 3 billion by the end of 2021[1]
- However, while life becomes more convenient for smartphone users, it can come at the cost of security breaches.
  - Cyber-attacks which targeted smartphones rose 50% between 2018 and 2019[2].



[1] techcrunch.com, [2] https://www:zdnet:com/article/mobile-malware-attacks-are-booming-in-2019-these-are-the-most-common-threats

Mohamed's Research: Smartphone User Authentication

- **To strengthen the user authentication and identification in a smartphone,**
  - We develop a biometric authentication and identification system which uses the capacitive touchscreen that is featured in all current smartphones.
- Our methodology focuses on—
  - Using the touchscreen as a sensor to capture the image of a user's ear, thumb or four fingers.
- We extracted the capacitive raw data from the touched body part to obtain a capacitive image
- We extracted:
  - Geometric features (e.g., length and width of a finger)
  - principal components
- We experimented with:
  - Support Vector Machine (SVM)
  - Random Forest (RF)
- We achieved:
  - maximum authentication accuracy of 98.84% by four fingers with SVM
  - maximum identification accuracy of 97.61% by four fingers with RF
- Advantages:
  - Does not require additional hardware (unlike fingerprint sensor)
  - Does not require to take prints from various angles (unlike face detection)
  - Larger touchscreen surface



John Dogan

- Undergraduate student
- Started research with me in the 2nd semester while taking CSC152
- Publication:
- J. C. Dogan and M. S. Hossain, "**A Novel Two-Step Fall Detection Method Using Smartphone Sensors**," IEEE International Conference on Smart Computing (SMARTCOMP), Washington, DC, USA, 2019, pp. 434-438

John's Research:
Human Fall Detection using Smartphones

- Falls are a major cause of injuries and hospital admissions among elderly people.
  - Each year 2.8 million older people are treated in emergency departments for falls[1].
  - The consequences of a fall significantly depend on the time interval during which the person remains unaided after the fall.

- We develop a new fall detection method which precisely detects falls using smartphone sensors.
- We collected data from 10 users to evaluate our proposed fall detection method.
- Each user performed five normal activities–
  - walking, jogging, standing, sitting, lying, and also fell after performing each activity.
- We performed experiments with five common smartphone sensors:
  - accelerometer, gyroscope, magnetometer, gravity, and linear acceleration.
- We tested five machine learning classifiers–
  - Support Vector Machine, K-Nearest Neighbor, Decision Tree, Random Forest, and Naive Bayes.
- Our two-step fall detection method achieved:
  - maximum accuracy of 95.65% with the gyroscope sensor and Support Vector Machine classifier.

A smartphone-based fall detection system has two major advantages over a traditional fall detection system that comes as a separate device:

- The phone can automatically send messages to or call the emergency contact person when a fall is detected
- A user does not need to carry an extra device.

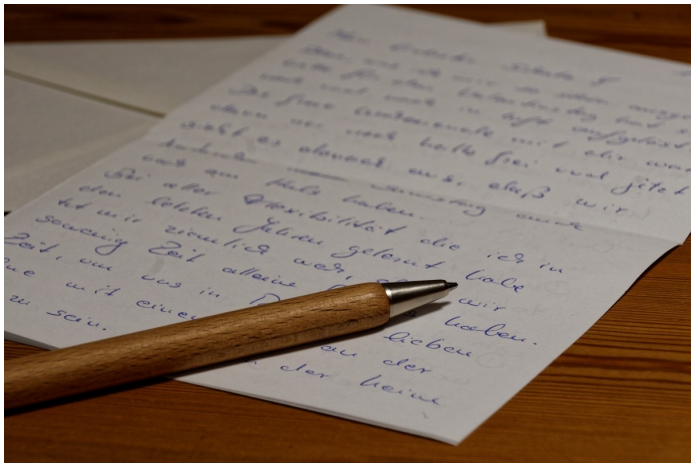
[1] Centers for Disease Control and Prevention

Tudor Boran

- Undergraduate student
- Started research with me in his senior year while taking CSC481
- Publication:
  - Tudor Boran, Muhamet Martinaj, Md Shafaeat Hossain, Authorship identification on limited samplings, Computers & Security, Volume 97, 2020, article number 101943.

Tudor's Research: Authorship Identification

- The internet has changed the way that many people access written works.
  - Books and articles, of various lengths, in several formats can be bought and accessed online, both legally and illegally.
  - Texts in even shorter form are originating through forums, SMS, blogs, emails, and social media.
- Automating the process of determining the authorship of posted texts would help combat online piracy of copyrighted text and plagiarism.
  - In addition, authorship identification could help detect fraudulent email messages from dangerous sources and combat cyberattacks by identifying authentic sources.
- We experimented with several machine learning algorithms on a limited set of public domain literature to identify the most efficient method of authorship identification.
- Different sized data sets were created from a total of 28 text books from a corpus of 7 authors.
- Traditional methods of authorship identification, such as Naive Bayes, Artificial Neural Network, and Support Vector Machine were implemented in addition to using a modern Deep Learning Neural Network for classification.
- Thirteen stylometric features were extracted ranging from character based, word based, and syntactic features.
- Our model consistently showed that Support Vector Machine out performed other classification methods.



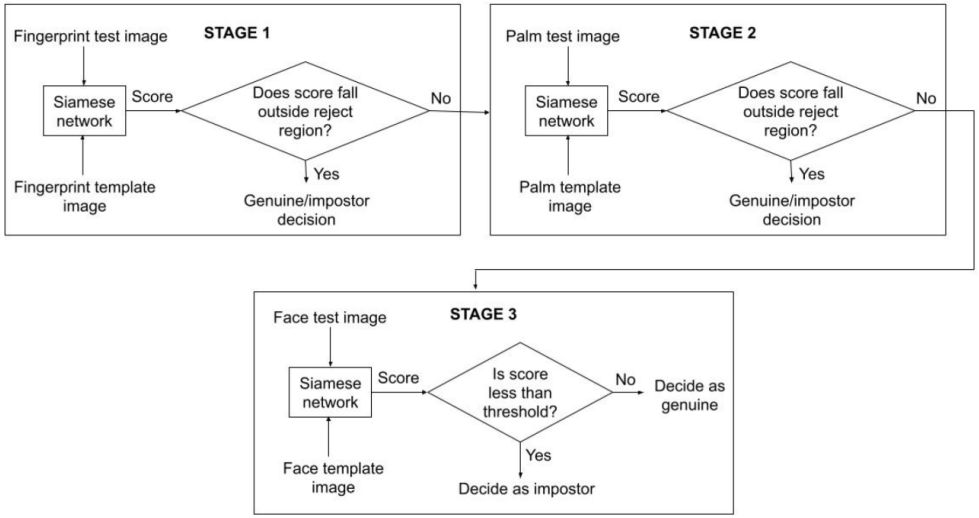
From short messages to full written works of literature, every writer leaves behind intrinsic evidence of a certain style of writing unique to them.

Tiffanie Edwards

- Undergraduate student
- Tiffanie started research with me in her senior year while doing honor's thesis CSC494
- Publication:
  - T. Edwards and M. S. Hossain, "**Effectiveness of Deep Learning on Serial Fusion Based Biometric Systems**," in IEEE Transactions on Artificial Intelligence, 2021, doi: 10.1109/TAI.2021.3064003.

Tiffanie's Research:
"Deep Learning + Serial Fusion" for Multi-biometric Systems

- We developed a multibiometric verification system by combining deep learning techniques and serial fusion methods.
- We worked on enhancing the 'user convenience' and reducing the 'verification error' in a multibiometric system.
  - With the advent of deep learning technologies, the accuracy of multibiometric systems have been improved significantly;
  - However, its applicability is still in question because of long verification times required by parallel fusion in a multibiometric system.
  - Our methodology—
    - alleviates the 'user inconvenience' issue by utilizing a serial fusion strategy in decision making
    - improves accuracy by leveraging deep learning technology in feature extraction and score generation.



- We developed a three stage multibiometric system using a user's fingerprint, palm, and face
- We tested three serial fusion methods with a Siamese neural network
- We achieved an AUC of 0.9996, where the genuine users require only 1.56 biometrics (instead of all 3) on
- an average.

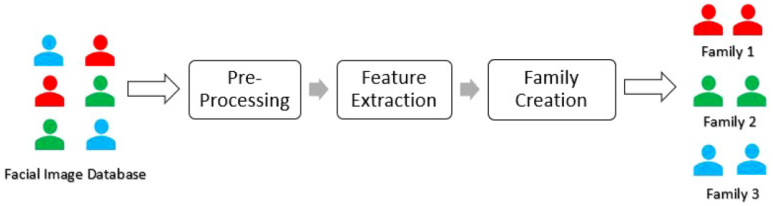
Matthew Kiley

- MS Thesis student
- Had a bachelor's degree in fine arts
- Publication:
  - Matthew R. Kiley and Md Shafaeat Hossain, "**Who are My Family Members? A Solution Based on Image Processing and Machine Learning**", in International Journal of Image and Graphics, Vol. 20, No. 04, 2050033, 2020

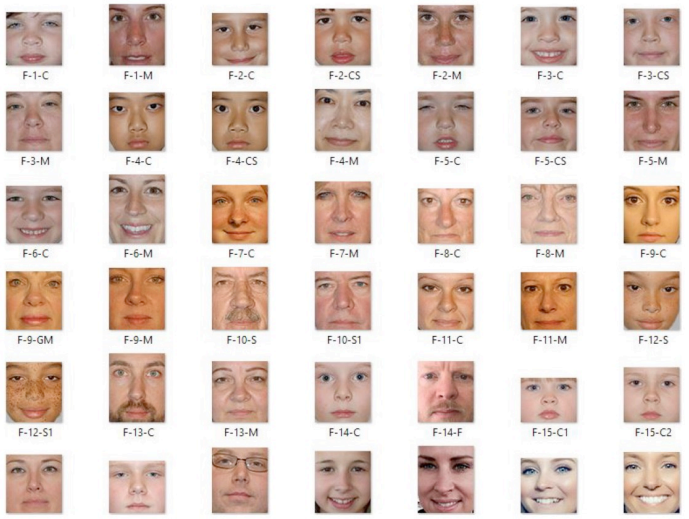
Matthew's Research
Family Detection in Facial Image Databases

- To discover family within a facial image dataset, we develop a framework, which allows a person to find his/her family within a set of facial images with no other knowledge of identification.
- Social impact and applications:
  - **Finding lost/missing children**: law enforcement could use our framework to identify the child's relatives through comparison to potential matches within their systems.
  - Identification of next of kin: law enforcement or humanitarian agencies applying our approach, would have the ability to **identify family members in the event of a crime, natural disaster or other tragedy using the face databases**.
  - Social media, Facebook, for instance: by connecting the individual datasets across the social network, a new massive image dataset is created. Our approach could have a significant impact on **finding one's biological family in the case of an adoption, family they never knew existed, or medical necessity such as organ donation**.
- We tested two feature extraction techniques:
  - Principal Component Analysis (PCA) and Histogram of Oriented Gradients (HOG)
- We tested three machine learning algorithms for creating families:
  - K-Means clustering, agglomerative hierarchical clustering, and K-nearest neighbors
- We evaluated our framework on two facial image datasets:
  - Y-Face, which we created and KinFaceW, which is a publicly available dataset.
- We achieved a maximum detection rate of 94.59% using K-Means

Family Detection Framework



Samples in Y-Face Dataset



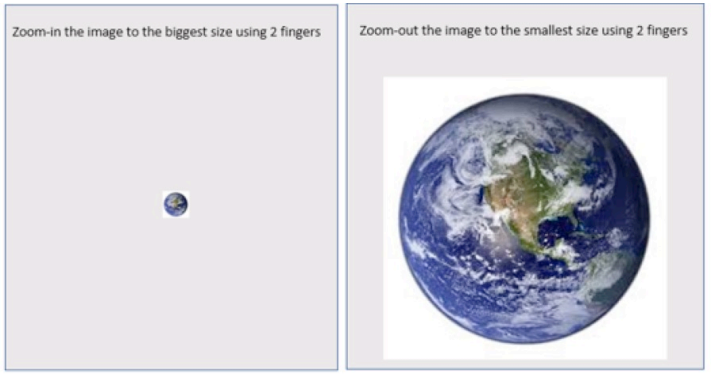
Leran Wang

- MS Thesis student
- Had a bachelor's degree in linguistics
- Publication:
  - Leran Wang, Md Shafaeat Hossain, Joshua Pulfrey, Lisa Lancor, "**The Effectiveness of Zoom Touchscreen Gestures for Authentication and Identification and Its Changes Over Time**", in computers & security, 2021 (revised and resubmitted—minor revision).

Leran's Research
Smartphone User Authentication using Zoom Gesture

- In this study, we focus on how zoom touchscreen gestures can be used to continuously authenticate and identify smartphone users.
  - The zoom gesture is critically under-researched as a behavioral biometric despite richness of data found in this gesture.
  - Furthermore, we analyze how the zoom gesture performs over time, which is a novel line of inquiry.
- We developed an Android app to collect zoom gesture samples.
  - Zoom samples were collected from 34 users and three different data collection sessions
  - In these sessions, each participant zoomed in and out on three images
- Eighty-five features were extracted from each gesture, which were grouped into seven categories: pressure, size, coordinate, distance, velocity, time, difference, and other features.
- The classification models used were:
  - Support Vector Machine (SVM), Random Forest (RF), and K-nearest Neighbor (KNN).
- Results:
  - The best authentication performance of EER 10.6% was achieved using the SVM
  - In terms of stability over time, SVM proved to be the most stable classifier
- This analysis proves that zoom gestures demonstrate promise for use in continuous smartphone authentication and identification applications.

Screenshots of our Android App



Carl Haberfeld

- MS Thesis student
- Had a bachelor's degree in biochemistry
- Publications:
  - Carl Haberfeld, Md Shafaeat Hossain, Lisa Lancor, "**Open code biometric tap pad for smartphones**", in Journal of Information Security and Applications, Volume 57, Article number 102688, 2021.
  - Md Shafaeat Hossain and Carl Haberfeld, "**Touch Behavior Based Age Estimation Toward Enhancing Child Safety**," IEEE International Joint Conference on Biometrics (IJCB), Houston, TX, USA, 2020, pp. 1-8.

Carl's Research
Open Code Biometric Tap Pad

(a) Pattern A

(b) Pattern B

(c) Pattern C

- A key reason behind data breach in smartphones is the poor security practice by smartphone users
  - such as the use of simple, easily guessed, or repetitive passcodes for logins
  - This poor security practice is a result of the effort required to memorize stronger ones.
- We devise a concept of ''open code'' biometric tap pad to authenticate smartphone users,
  - which eliminates the need of memorizing secret codes.
- A biometric tap pad consists of a grid of buttons each labeled with a unique digit.
  - The user attempting to log into the phone will tap these buttons in a given sequence.
  - He/she will not memorize this tap sequence; the sequence will be displayed on the screen.
  - The focus here is how the user types the sequence. This typing behavior is used for authentication.
- We designed three tap pads and incorporated them into an Android app.
- We tested several sequence styles:
  - simple vs. complex, ordered vs. unordered, etc.
- We experimented with five different fingers:
  - two thumbs, two index fingers, and the ''usual'' finger.
- We collected data from 33 participants over two weeks.
- We tested 3 machine learning algorithms:
  - Support Vector Machine, Artificial Neural Network, and Random Forest.

An open code biometric tap pad has several advantages, such as:

- users do not need to memorize passcodes
- manufacturers do not need to include extra sensors
- onlookers have no chance to practice shoulder-surfing.

Experimental results show significant promise of open code biometric tap pads as a solution to the problem of weak smartphone security practices used by a large segment of the population.

Thank you

Email: HossainM3@SouthernCT.edu