Initial Project Proposal

Year: 2019 **Semester:** Spring **Project Name:** Guard DAWGS
Creation Date: September 16th, 2018 **Last Modified:** September 16th, 2018

Team Members (#1 is Team Leader):
Member 1: Ian Sibley **Email:** isibley@purdue.edu
Member 2: Yash Nain **Email:** ynain@purdue.edu
Member 3: James Weber **Email:** weber99@purdue.edu
Member 4: Viktoryia Zhuleva **Email:** vzhuleva@purdue.edu

1.0 Description of Problem:

Privacy and security is something that's been a personal concern for most of the modern world, and new and innovative ideas are coming out every day for solutions to make your home, family, and life overall safer. This also means that the methods used to break into houses and personal property are, in turn, getting more complicated and creative. The ultimate goal for security is to make a system immune to tampering, but still lets the desired users through. Most systems in place today either have bugs or back-doors that allow others to bypass their security, or the user verification process is too troublesome to implement fully, which will cause the user to take shortcuts and compromise the overall security, or not use the system at all. Therefore, the goal is to make a security system that's simple for authorized users, without leaving back-doors open to others.

2.0 Proposed Solution:

As a result of the rising demand for better personal security and property insurance, computerization is commonly used to limit external interfacing, which also limits the ability for malicious entities to tamper with the product. The more interfaces there are for a user to interact with, the more security risks are exposed. For electronic home security solutions, electronic and computing resources are often made inaccessible from the outside, which is undesirable in the event of a component malfunction. The proposed solution will have a combination of automatic and manual input to unlock the house door for user convenience, and dynamic system functionality.
This solution will implement an image recognition system able to determine if a user can gain access to the house. A camera will capture an image of the user, and a facial recognition algorithm will determine whether or not the person walking up to the door is an authorized user. A numeric keypad can be used instead that will bypass the system's auto-locking capability as needed. The product will have a visual representation, such as LED's for system verification, should the lock motor fail but the algorithm and system functions remain correct. This would allow the user to replace any component of the system without having to disassemble its entire architecture in the future.

3.0 ECE477 Course Requirements Satisfaction

In order to meet the course requirements, our project will implement an embedded microcontroller, a custom-built PCB, and several peripheral connections that will send and receive signals to and from the microcontroller.

3.1 Expected Microcontroller Responsibilities

In order to facilitate the functionality described above, the microcontroller must interface with the camera, numeric keypad, and motorized lock. In order to perform the facial recognition, the microcontroller will send the image or video stream to a computer or server which will perform the verification algorithms. After this algorithm completes, the pass or fail result will then be transmitted to the microcontroller, and the door will be unlocked. It will also be able to implement the numeric override from the keypad to let the user in regardless of the facial recognition result.

3.2 Expected Printed Circuit Responsibilities

The PCB will hold the microcontroller, power-regulators, and microcontroller interfacing hardware such as USB interfaces, CSi for the embedded camera, and connector ports for the motorized lock. To display the “Locked/Unlocked” state, the PCB will orchestrate a simple visual representation to correspond to the current state of the lock. The power-regulators will regulate the voltage for the microcontroller and interfaces, to be enough to run the electronics on the board, not including the door lock. The motor attached to the door lock mechanism will have its own power electronics, and is activated by the microcontroller.

4.0 Market Analysis:

This product would be most useful for the home security industry and the average homeowner, since the design easily allows for scalability and implementation within already existing security solutions. With an estimated 3.7 million household burglaries per year [2], this product would provide an auto-lock feature that would help keep out unwanted visitors. This is especially useful for cases where the door was left unlocked. Thirty percent of all break-ins involve a burglar taking advantage of unlocked entrances to a building or home [3]. In addition, thirty-four percent of all burglars enter through the front door, locked or unlocked [5].

5.0 Competitive Analysis:

Several smart home security solutions already exist on the market today, such as those made by NEST, Schlage, Corum, Ultraloq, and Kwikset, which implement numeric locks or image recognition independently. The following are examples of other solutions in related fields.

5.1 Preliminary Patent Analysis:

5.1.1 US Patent Application US 07214949 A

Patent Title: "Home Security System"
Patent Holder: Robert J. Gaffigan
Patent Filing Date: May 23th, 1989

This patent is for a home security system, featuring sensors that, when armed, are set off upon unwanted person entering the domain. A remote station is connected to the radio transmitter, and sends the signal for the intruder alarm upon system activation. The main system flashes the exterior lights and home warning signals to notify the owner about breaking in. [1]

5.1.2 US Patent Application US 4360801 A

Patent Title: "Home Security and Garage Door Operator System"
Patent Holder: Stanley Works
Patent Filing Date: November 23th, 1982

This is a patent for a system that operates a garage door and features a gas sensor to monitor the level of toxic gas in the room. There is a two button transmitter that is used to sequentially close the garage door and set off an alarm system when needed. Once the security alarm has been set, the lock-out circuitry also disables the garage door control until the security alarm is deactivated. A heat sensor sends status information of monitored parameters to the remote modules located in the house. [4]

5.1.3 US Patent Application US 6400265 B1

Patent Title: "System and Method for Monitoring Security Systems by Using Video Images"
Patent Holder: MicroStrategy Inc
Patent Filing Date: April 24th, 2001

This patent presents a home security system that compares images and looks for differences that correspond to potential motion. The alarm can be configured so it is set off when the algorithm finds such movement, or it can instead pass the image on to a central security network for a separate process to evaluate the content in the image. This product either acts as a front-component of the full application, limiting the processing needed for other algorithms, or acts as a no-user-allowed, self-contained application for areas of high restriction. If the information is passed on to a central security network, the result of the network's evaluation is given control of triggering the alarm as appropriate. [6]

5.2 Commercial Product Analysis:

5.2.1 Commercial Product #1:

Product: Kwikset Kevo [10]
Description: Kevo makes use of an external electronic lock, passing the authorization for entry to something such as a phone or electronic key. This is done in order to give the user greater control over who is able to access a location, and to make access items difficult to replicate, as opposed to alternatives like the classic lock-key combination. This solution likely relies on a device with NFC capability, which can be convenient if the user has a smartphone or other NFC device, but can be terribly inconvenient if they don't, or if the device has run out of power. It also requires more external interfacing than is necessary.

5.2.2 Commercial Product #2:

Product: Corum Security CS-100 [11]
Description: This system relies on an image-recognition system, where the user holds their face in front of a camera and is recognized by the unit, which then unlocks the door and allows the person entry. The algorithm ensures that only an actual face will be processed, and not a picture of a face or an object. For a backup system, in case the algorithm doesn't recognize the user or the unit runs out of power, an external 9V battery can be plugged in, or a mechanical key can be used. This product relies on a similar methodology to the project proposal, but still relies on external interfacing that is being phased out over time.

5.2.3 Commercial Product #3:

Product: Nest x Lock System [12]
Description: This system implements a variable-length PIN for security, and can be connected to the internet for full control and implementation. After the door has been accessed, the auto-lock feature is activated, ensuring that the door is locked whenever the user desires. Given that most NEST devices can be interfaced with each other, this lock primarily relies on the same mechanism, and can be accessed by an app remotely. This is both a benefit and a drawback; while internet connectivity gives the device plenty of extra functionality, it will also hamper basic functionality for customers who may want the unit to run on its own. It also introduces an external security risk that doesn't need to be there.

5.3 Open Source Project Analysis:

5.3.1 Open Source Project #1: Pi-FaceRec-Box

A Raspberry Pi facial recognition system written in Python, hosted on GitHub and provided for free as part of an Adafruit project. The project uses facial recognition to control a servo that locks or unlocks a treasure box. [7]

Facial recognition was done using the Eigenfaces algorithm (Principal Component Analysis or PCA) and implemented using OpenCV library in Python. This facial recognition method requires positive training images of people authorized to unlock the box. The provide a program, capture-positives.py, can take pictures of users to feed to the algorithm and aid this training process. Different angles, facial expressions, and lighting may be needed to train this model properly. Training the model on a Raspberry Pi takes approximately 10 minutes to complete.

Pros:
This project provides a script to allow easy image capture of training data for the facial recognition. OpenCV provides a library for facial recognition.

Cons:
The eigenfaces algorithm requires a set of training data of pictures of faces of people are and are not allowed to open the lock. As mentioned above it takes 10 minutes to train on a Raspberry Pi. Depending on the microcontroller we choose, the processor may be of equal or lesser processing power than a Raspberry Pi, meaning that it would take an end user 10+ minutes to train their face for a lock.

5.3.2 Open Source Project #2: Face Recognition Door Lock

The next project is an ECE project implemented by students of Cornell University [8]. They have a similar setup where they use a Raspberry Pi with the OpenCV Python library. Additionally, they integrate a keypad into their product for back-up security.

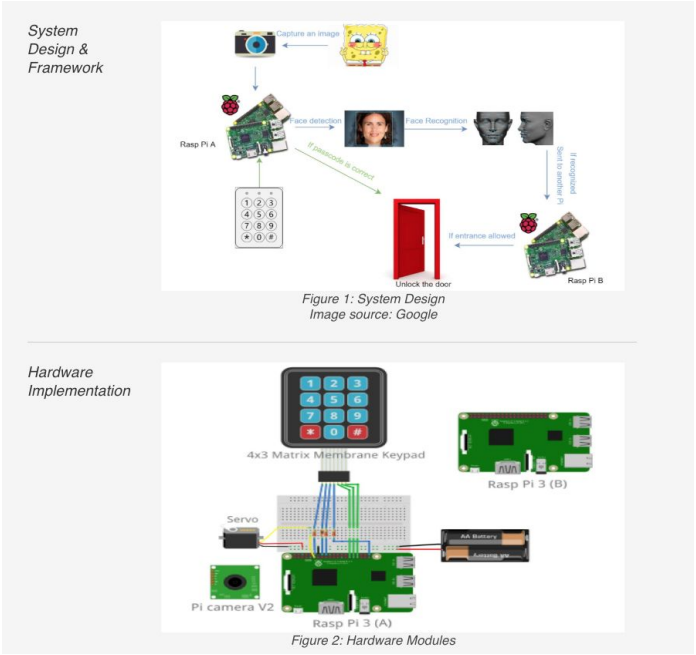

Figure 1: Student Project System and Hardware Diagrams [8]

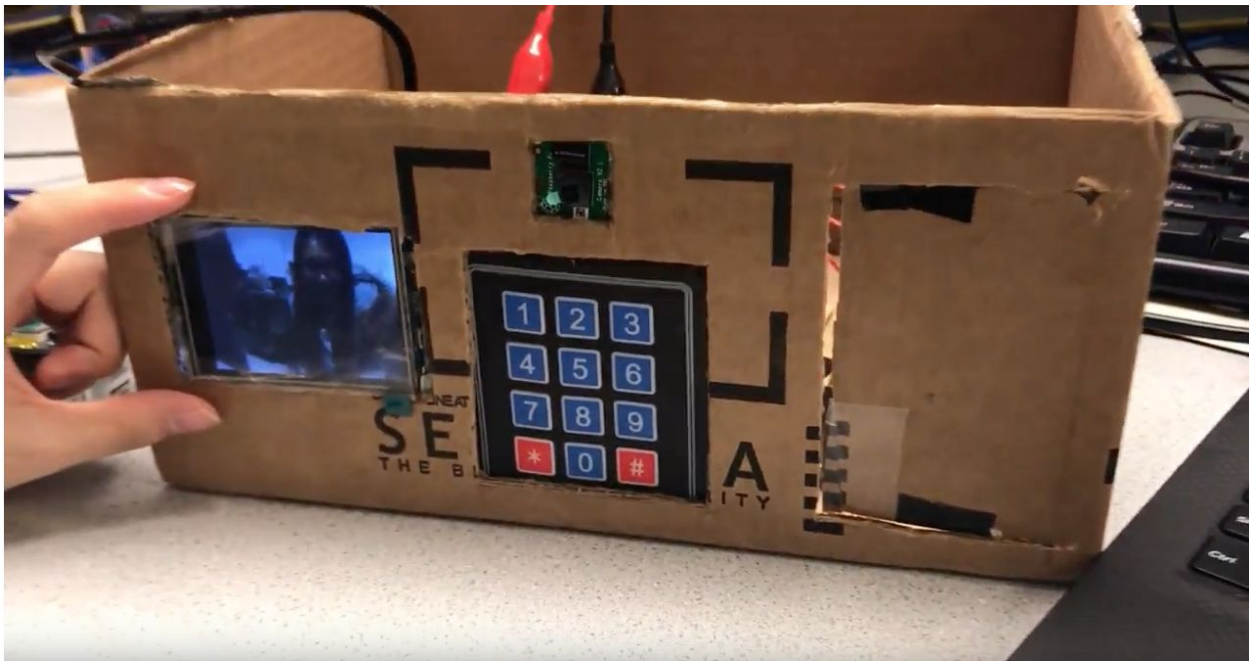

Figure 2: Project Deliverables for Face Recognition Door Lock

Interestingly, they chose to also include a touchscreen LCD that had lock/unlock buttons on it. Once the user clicked the unlock button, it would display the camera feed on the screen. It also allowed the user to enter and reset a passcode on the keypad.

This product also used TCP protocol to communicate between two Raspberry Pi microcontrollers (one for the display,the other - for the rest of the components).

Pros:
The LCD allowed users to set and reset the passcode on the keypad. That is definitely something that would be good to consider. Although an LCD may not be appropriate for an actual home door lock, something like a web or mobile application may be useful to reset the passcode.

Cons:
Used two Raspberry Pi microcontrollers for the security system. It may be necessary to send data wirelessly from the camera to the lock and vice versa, but we would not want to use two microcontrollers. To add, packaging looks substandard, at best. Obviously this group was focusing more on the technology rather than the whole product, but it would be wise to consider the presentation of the finished product to instill confidence into the customer.

5.3.3 Open Source Project #3: Facial Recognition Enabled Smart Door Using Microsoft Face API

This last project is an academic paper by students at the VIT University India [9]. These students used the Microsoft FACE API as well as Windows 10 IOT. The team also employed the use of a Raspberry Pi, however, unlike other groups, they used the Windows 10 IOT operating system to run their software. They had a doorbell that users would press which activated the HD capture. It used Microsoft APIs to recognize users' faces.

Other things to note are:
The Raspberry Pi is configured from a parent device with the Windows 10 IOT Dashboard.
The code base was written in C#.
The API is deployed over Microsoft Azure.

Pros:
Uses Microsoft API's, which are connected to high powered servers. It is also configurable from a parent device which could be useful to end users, however opens the system to more security risks.

Cons:
This project seemed to have many drawbacks written about extensively in its conclusions: Firstly, the "Process is slow, the result is not so accurate, and the methodology is complex". Secondly, the "Time after successful detection of face is indefinite," meaning the door remains

open for an indefinite amount of time. Thirdly, as touched upon in the first point, this project uses various Microsoft API's and is also written in C#, neither of which the team members are familiar with.

6.0 Sources Cited:

1. R. J. Gaffigan, "Home Security System," 23-May-1989. https://patents.google.com/patent/US4833449A/en?q=home&q=security&q=system&oq=home security system
2. Catalano, S. (2010). Victimization During Household Burglary. [ebook] NJC, p.1. Available at: https://www.bjs.gov/content/pub/pdf/vdhb.pdf [Accessed 16 Sep. 2018].
3. Safeguardtheworld.com. (2018). Home Security Statistics. [online] Available at: http://www.safeguardtheworld.com/statistics.html [Accessed 16 Sep. 2018].
4. D. C. Duhame, "Home Security and Garage Operator System," 23-Nov-1982. https://patents.google.com/patent/US4360801A/en?q=home&q=security&q=system&oq=home security system
5. Gromicko, N. and Shepard, K. (2018). Burglar-Resistant Homes - InterNACHI. [online] Nachi.org. Available at: https://www.nachi.org/burglar-resistant.htm [Accessed 16 Sep. 2018].
6. M. J. Saylor, A. Slavin, and J.-P. Hugues Martin, "System and Method for Monitoring Security Systems by Using Video Images," 04-Jun-2002. https://patents.google.com/patent/US6400265B1/en?q=home&q=security&q=system&oq=home security system
7. DiCola, T. (2014). Raspberry Pi Face Recognition Treasure Box. [online] Available at: https://learn.adafruit.com/raspberry-pi-face-recognition-treasure-box/overview.
8. Zeng, L. and Sun, R. (2017). Face Recognition Door Lock. [online] Available at: https://courses.ece.cornell.edu/ece5990/ECE5725_Fall2017_projects/lz455_rs2364_final/ECE_5725_Face_Recognition_Door_Lock.htm.
9. K. Maheshwari and N. N, "Facial Recognition Enabled Smart Door Using Microsoft Face API," International Journal of Engineering Trends and Applications (IJETA), vol. 4, no. 3, May 2017.
10. "Kevo Smart Lock - Control Your Lock With Your Phone.," *Kwikset*. [Online]. Available: https://www.kwikset.com/kevo/default. [Accessed: 20-Sep-2018].
11. "Shop," *Corum Security*. [Online]. Available: http://www.corumsecure.com/product/facial-recognition-lock/. [Accessed: 20-Sep-2018].
12. Nest, "Nest × Yale Lock | Installation and Tech Specs," *Nest*. [Online]. Available: https://nest.com/lock/nest-yale-lock-key-free-smart-lock/tech-specs/. [Accessed: 20-Sep-2018].

Appendix 1: Concept Sketch