Multimodal Biometrics

Version 1.4

Brian Tan

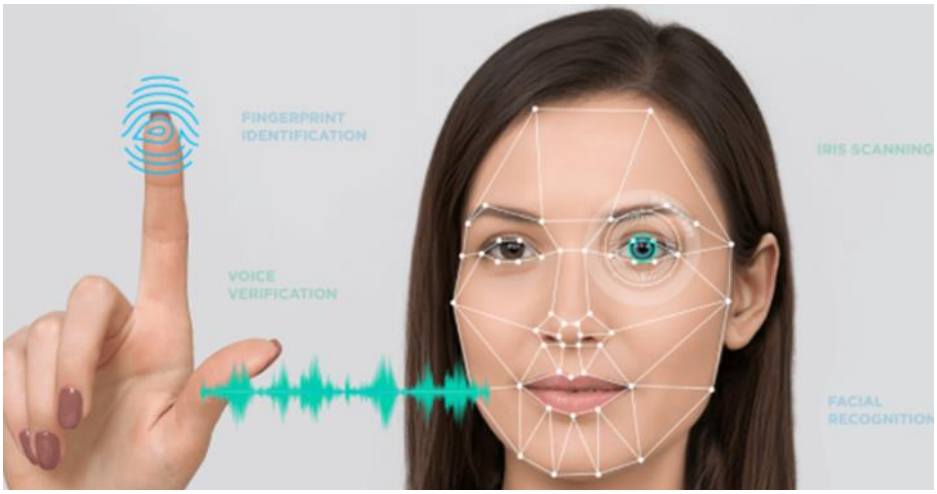
Davina Doran

Fulya Kocaman

Konnor Gutierrez

California State Fullerton

CPSC 362 SOFTWARE ENGINEERING



12/7/2020

Source: https://mobidev.biz/blog/multimodal-biometrics-verification-system-ai-machine-learning

Table of Contents

Revision History

Name	Date	Reason for Changes	Version
Brian Tan	12/5/20	Created	1.0
Fulya Kocaman	12/5/20	Added Conclusion and Lesson Learned	1.1
Brian Tan	12/6/20	Added Details and Observations	1.2
Fulya Kocaman	12/6/20	Reformatted	1.3
Fulya Kocaman	12/7/20	Added Cost Estimate	1.4

1. The Problem

Military security is always in need of improvement. As the number of cases of security breaches

rise, both physically and digitally, so too must the efforts to reinforce the security of infrastructure, computer systems, and access control.

Current access control measures require the use of a CAC. But like any ID card, they can be lost, stolen, or illegally duplicated for the purpose of identity theft. Military security must be on par or ahead of its civilian peers in order to maintain a competitive edge, and to ultimately better protect the nation's assets and secrets.

2. Potential Solution

This project proposes the use of multimodal biometrics as the next step in the evolution of military security. The military member already possesses the key identifiers; retina, fingerprint, voice, face, and palm. Multimodal biometric systems are very difficult to spoof as compared to unimodal systems. Even if one biometric modality could be spoofed for example fingers made of gelatin, contact lenses, etc., the individual can still be authenticated using the other biometric identifiers.

3. Goals

Our goal was to design and build a multimodal biometrics recognition system which used unique identifiers (**retina**, **fingerprint**, **voice**, **face**, **palm**) that can be customized based on the usage requirements to provide access to secure locations/rooms/systems for authorized personnel in military facilities.

Additionally, we wanted to develop a system that could be completely contactless for hygienic reasons in the wake of possible pandemics.

4. The Initial Plan

- Develop Requirements for the project
- Research existing technologies and upcoming innovations
- Design a modular system that can be customized to security needs
- Develop activity sequence for every possible scenario of access control
- Develop the necessary software and algorithms for each form of recognition
- The algorithms are efficient and accurate **Deep Learning** algorithms
- Biometric encryption techniques will be used. They use biometric characteristics as part of the encryption and decryption algorithm.
- **C/C#** will be the designated programming language, and the **BioAPI** (Biometric Application Programming Interface) will be used for development.
- A major part of the international biometric standards work has been taking place in **ISO/IEC** Joint Technical Committee 1 (JTC 1), particularly in its Subcommittee 37 (SC 37) on 'Biometrics' established in June 2002
- **Parallel and Distributed Processing** will be utilized to share the workload, just one processor would not be enough

- Develop testing software in tandem with the main code production
- Acquire components to build the hardware and combine it with the software
- Test the system in various environmental conditions
- Deploy system to initial sites of differing environmental conditions for pilot testing
- Conduct scheduled maintenance
- Maintain records of tests and maintenance

5. Schedule

The overall goal is to have systems securely up and running within 32 months. To do this the project has been compartmentalized into cohesive sections as follows: Requirements, Research, Design, Development, Testing (Phase I), Testing (Phase II), and Deployment. Each section has its specific project milestone that will be reached at competition of said phase. The modularity of our system allows for minimal interdependency between these processes until testing prototype multi modular systems.

6. Description

Controlling access to facilities, computer systems, and classified information depends on fast and accurate information. The Army also operates a vast set of human resources services involving health care, retiree and dependent benefits, troop support services and many others. These services create the need for accurate identification to prevent fraud and abuse. [1]

The U.S. Army currently uses a combination of a CAC card and personal identification numbers (PINs) for traditional means of access control. This project's perspective is to use the multimodal biometrics in conjunction with the CAC cards to

- improve accurate identification and security,
- reduce operational and administrative costs and
- increase user convenience.

This project describes the planning associated with the Multimodal Biometrics Software System. This plan outlines the organizational roles and contains the six steps of Software Development Plan including planning, analysis, design (Architectural Design and Software Lifecycle), development & implementation, testing & deployment and maintenance

7. Architectural Design

- Multimodal Biometrics Design shall be modular (compartmentalization of data and function) which makes it more flexible when adding and/or removing a user, hardware, database. This modular platform should collect the data, create a database, communicate with the hardware and then compare user data with the database using algorithms and the decision.
- Refactoring that simplifies the design without changing functionality should be used if possible.

Figure 7 represents sources of information for Biometric fusion that we shall use in this project:

- **Multisensors**: Multiple sensors shall be used to capture the data. For example, a facial recognition system might employ multiple cameras to capture different angles on a face.
- **Multiple algorithms:** The same capture data are processed using different algorithms.
- **Multiple instances:** Multiple instances of the same modality shall be used. For example, multiple fingerprints may be matched instead of just one, as may the retinal scan of both eyes. Depending on how the capture was done, such systems may or may not require additional hardware and sensor devices.
- **Multisamples:** Multiple samples of the same trait shall be acquired. For example, multiple angles of a face or multiple images of different portions of the same fingerprint are captured.
- **Multimodal:** Data from different modalities shall be combined, such as face, fingerprint and palm, retina and voice. Such systems require both hardware (sensors) and software (algorithms) to capture and process each modality being used [7].

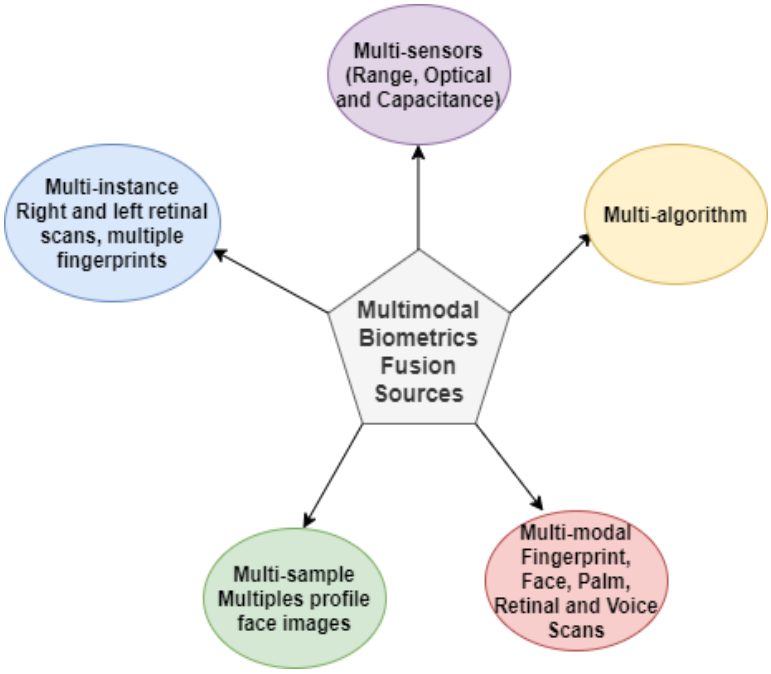


Figure 7: Sources of information for Biometric Fusion

7.1 System Architecture

There will be different types and kinds of Biometric information/data which will be shared with the different modalities in a Multimodal based Biometric system. Multimodal systems fusion architecture as mentioned in [6] combines several biometric systems and thus requires the acquisition and processing of several data (Figure 7.1).

- In sensor level fusion, we shall fuse the biometric traits coming from different sensors such as fingerprint scanner, retinal scanner, video camera etc. to form a merged biometric trait and process.
- In feature level fusion, signals coming from different biometric channels shall be first

processed after which the feature vectors are extracted separately from each biometric trait. The feature vectors are then combined to form a composite feature vector using a specific fusion algorithm and then used for further classification. In feature level fusion, some reduction techniques should need to be used in order to select only the useful features.

- In this matching score level fusion level, the feature vectors shall be processed separately rather than combining them. Then an individual matching score is found and based on the accuracy of each biometric channel, we then fuse the matching level to find a composite matching score which will be used for classification. We could use various techniques such as logistic regression, highest rank, Bayes rule, mean fusion etc. to combine match scores.
    - In addition to this, another important aspect of this fusion is the normalization of scores acquired from different modalities because each subsystem can have intervals of variation of the different scores, for example for a system the scores vary between 0 and 1 and for another the scores vary between 0 and 100. Hence, we shall need to normalize the scores before to combine them. We can use techniques such as Min-max, z-score, piecewise linear etc. to achieve normalization of the match scores. We could examine the effect of different score normalization techniques on the performance of a multimodal biometric system and compare normalization techniques on the basis of robustness and efficiency.
- In decision level fusion, each biometric trait is first pre-classified separately. The individual biometric trait is first captured and then features are extracted from the captured trait. The traits are classified as either accept or reject based on these extracted features. The final classification is obtained by combining the outputs of different modalities

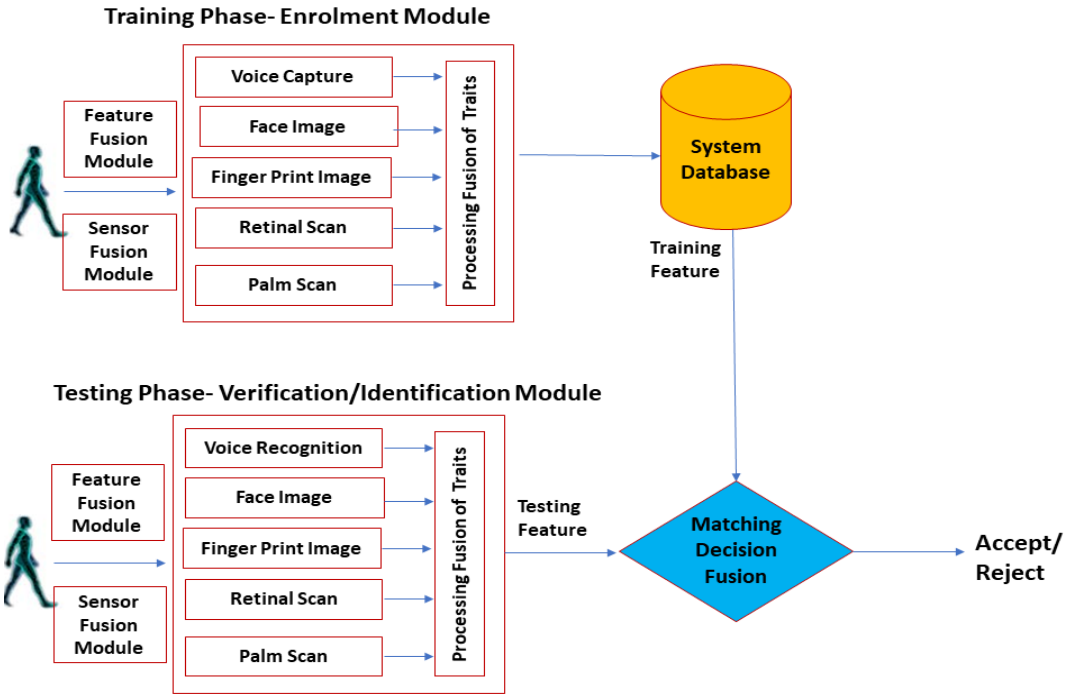


Figure 7.1: Enrollment and Authentication Phases of the system- Fusion Levels

8. Cost Estimate

8.1 COCOMO Model

Estimation was accomplished using the Basic COCOMO Model estimation technique for organic project types, and an estimated 250K lines of code. The calculations are as follows:

- Basic COCOMO Model Formula: Effort = a(KLOC)^b

  Development Time = c(Effort)^d

  Average Staff Size = Effort / Development Time

  Productivity = KLOC / Effort

Type	**a**	**b**	**c**	**d**
Organic	2.4	1.05	2.5	0.38

- Effort = $2.4(250)^{1.05}$ = 791 Person-Months
- Development Time = $2.5(791)^{0.38}$ = 32 Months
- Average Staff Size = 791 / 32 = 25 Persons
- Productivity = 250 / 791 = 0.32 KLOC/(Person-Month)

8.2 Time Allocation

There are 32 months reserved for competition and deployment of the modular biometric security system. Due to the low coupling between each biometric system phases can begin during the progression of a previous phase. 20% of the time is to be allocated to research and requirements. 60% of the time is to be allocated to design and development. Finally, 15% will be allocated to testing and 5% to deployment. These ratios can vary depending on the progression on each phase.

8.3 People Power Requirements

In order to complete this project on time it has been determined that the software development team will consist of an average staff size of 25 persons including: the senior management team, project specialist, steering committee, project manager, system administrator, system analyst, hardware engineers, requirement analyst, technical clerk, software engineers, algorithm engineers, database engineers, technical support QA manager.

- Already filled roles: senior management team, project specialist, steering committee.
- To be hired: project manager, system administrator, system analyst, hardware engineers (team of 4 people), requirement analyst, technical clerk, software engineers (2 teams of 3

people, 6 people total), algorithm engineers (team of 3), database engineers (team of 3-4 people), technical support (5-8 people), QA manager.

8.4 Cost

- **Cost to develop/run the system:**
  - All estimates are based on current national averages, 40-hour work weeks, and a project length of 30-32 months. Roles listed as indefinitely insinuates that the job necessity will persist longer than the length of development (30-32 months), and will have an additional yearly estimate.
    - Project manager: 30-32 months, $50-60 hourly
      - life of project est. $240,000-$307,200
    - System administrator: indefinitely, $25-$35 hourly
      - life of project est. $120,000-$179,200
      - yearly est. $48,000-$67,200
    - System analyst: indefinitely, $25-$35 hourly
      - life of project est. $120,000-$179,200
      - yearly est. $48,000-$67,200
    - QA manager: 30-32 months, $50-$60 hourly
      - life of project est. $240,000-$307,200
    - Technical clerk: indefinitely, $10-$20 hourly
      - life of project est. $48,000-$102,400
      - yearly est. $19,200-$38,400
    - Software engineers: 6 people, 30-32 months, $30-$40 hourly
      - life of project est. $144,000-$204,800 per person = $864,000-$1,228,800
    - Algorithm engineers: 3 people, 30-32 months, $55-$65 hourly
      - life of project est. $264,000-$332,800 per person = $1,584,000-$1,996,800
    - Database engineers: 3-4 people, indefinitely, $25-$35 hourly
      - life of project est. $120,000-$179,200 per person = $360,000-$716,800
      - yearly est. $48,000-$67,200 = $144,000-$268,800
    - Technical support: 5-10 people, indefinitely, $10-$20 hourly
      - life of project est. $48,000-$102,400 per person = $240,000-$819,200
      - yearly est. $19,200-$38,400 = $96,000-$307,200
  - Estimated Total for the Software Development (30-32 months): $3,696,000-$5,836,800 (Average $4,766,400 total)
  - Estimated total per year (maintenance and support): $355,200-$823,600 (Average $589,400 per year)

- **Hardware costs:**
  - All hardware costs vary per system implemented. ($10,000 – 2M+, 1M Average)
- Input Device Costs(per unit)

  - Voice: $500
  - Palm: $100
  - Fingerprint: $1,300
  - Facial: $25,800
  - Retinal: $50,000
- Environmentally hardened scanners run at x2's the rate
- Processing/Storage Devices:
  - CPU: $200 - $400 per system
  - RAM: $30 - $50 per system
  - Database: $5000 – $10,000

- Backup Power (UPS): $2,000-$5,000 per system

8.5 Management Reserve

Based on the estimate that the cost to develop the system would cost $6M. A 5-15% MR would account for a total of $6.3-6.9M USD.

9. Details of the Multimodal Biometric System in Operation

- Project from start to finish had to be done via online communication due to pandemic restrictions.
- Project had trouble getting started due to: a) Problems with acquiring workspace to build system, b) Problems with funding due to late budget signing, c) Limited capacity working conditions in any given work space due to social distancing rules.

- The details of the deployment of the system at the three locations went as follows:
  - Bldg 76, Main Entrance, Fort Bragg:
    - The outdoor system required only CAC and voice scanners.
    - Minor frequent interruptions during installation due to high volume of human traffic into building
    - Power source was an issue due to being outdoors as anticipated. Technicians engineered a lasting solution with POC in adherence to building code.
    - Time spent installing system: 2 hours

  - Bldg 360, Room A, Fort Bragg:
    - The indoor system required all scanners.
    - Issues making module connections due to tight work space. Rectified by using backup extensions.
    - Time spent installing system: 5hours

  - Bldg 81, Room J, Joint-Base Lewis-Mcchord:

- The indoor system required CAC, retinal, hand scanners.
- Issue with installation schedule. Planned time of install was 9am. POC was unaware of a last-minute change to the room's use. Room was available at 11am. Technicians adjusted accordingly.
- Time spent installing system: 3hours

- Testing
  - Initial tests showed average boot time of 3 min on first startup.
  - Subsequent boot times averaged 1min.
  - Error checking algorithm performed optimally
  - System temperature maintained a safe 70 degrees F when idle
  - System temperature increased to 90 degrees F when in continuous use by a line of 12 servicemembers. That is within the threshold of 95 degrees F.

10. Observations

- Documentation of tests written by technicians needed better clarity and details
- The system's error descriptions were vague and unclear
- Outdoor system screens had visibility issues during cold climate
- Hand scanner had issues recognizing wet or sweaty hands
- Weekends tended to be the best time to conduct system installs due to low volume of traffic.

11. Conclusion

This project is based on Multi-biometric fusion that tries to combine information from different biometric sources to enhance the verification and identification accuracy and usability. The fusion can be performed on different levels such as the data, feature, comparison score, or decision levels. While fusion in later stages, like score or decision levels, offers more implementation flexibility, feature and data level fusion might maintain more information and enable further joint processing.

Therefore, we believe using Deep Learning Algorithms is the key to this project. Deep Learning is becoming dominant in many applications that utilize machine learning. Biometrics is one of the applications where Deep Learning significantly advanced the state-of-the-art accuracies. Artificial Neural Network inspired by the structure of human brain cell in Deep Learning speeds up a system's face-scanning capabilities, as it learns more about the data it is processing. It can make the network learn good embeddings for each image and hence make it diversely trained, even the ones it has never seen before.

12. Lesson Learned

- Training Neural Network requires massive volume of data to train, so needs massive computational power and graphical processing units (GPUs)
- GPUs have thousands of cores as compared to the CPU and they are more expensive.
- Training time of the data could take months based on the amount of data and number of layers in the network.

- This project has taught us to work as a team and how to develop a Software by first making a detailed list of Software Requirements and then following the steps on the Software Development Life Cycle.
- Coordination among team mates, attention to detail, and preparation were keys to a successful rollout of the product.
- It has also made us a better Computer Scientist by preparing us for the real work life.

13. References

The references used in this document are:

[1] https://www.rand.org/pubs/monograph_reports/MR1237.html
[2] https://neurotechnology.com/megamatcher-large-scale-AFIS-and-biometric-identification-systems.html
[3] https://en.wikipedia.org/wiki/BioAPI
[4] https://www.dsp.dla.mil/Specs-Standards/List-of-DISR-documents/
[5] Software Engineering: A Practitioner's: 9th Roger Pressman, Bruce Maxim
[6] https://www.bayometric.com/unimodal-vs-multimodal/
[7] Biometric Recognition- Challenges and Opportunities (2010) National Research Council (US) Whither Biometrics Committee; Pato JN, Millett LI, editors.
[8] https://resources.infosecinstitute.com/a-project-management-guide-to-deploying-biometrics-part-3-the-modality-aspect/#article
[9] Fundamentals of Biometric System Design by S. N. Yanushkevich

Glossary

- CAC – Common Access Card
- SDP – Software Development Plan
- BioAPI – Biometric Application Programming Interface
- DOD – Department of Defense
- DISR – Department of Defense Information Technology Standards Registry
- POC – Point of contact
- NIST – National Institute of Standards and Technology
- GPU – Graphical Processing Unit