SOAR

STATE-OF-THE-ART REPORT (SOAR)
AUGUST 2024

HDIAC-BCO-2024-579

BIOMETRIC STANDOFF DETECTION: EXAMINING THE TECHNOLOGIES, IMPLEMENTATIONS, AND DEVELOPMENTS OF BIOMETRIC SYSTEMS

By Megan N. Lietha, Trey Kibodeaux, and Doyle T. Motes III
Contract Number: FA8075-21-D-0001
Published By: HDIAC

This Page Intentionally Left Blank

SOAR

STATE-OF-THE-ART REPORT (SOAR)
AUGUST 2024

BIOMETRIC STANDOFF DETECTION: EXAMINING THE TECHNOLOGIES, IMPLEMENTATIONS, AND DEVELOPMENTS OF BIOMETRIC SYSTEMS

MEGAN N. LIETHA, TREY KIBODEAUX, AND DOYLE T. MOTES III

ABOUT HDIAC

The Homeland Defense & Security Information Analysis Center (HDIAC) is a U.S. Department of Defense (DoD) IAC sponsored by the Defense Technical Information Center (DTIC). HDIAC is operated by SURVICE Engineering Company under contract FA8075-21-D-0001 and is one of the three next-generation IACs transforming the DoD IAC program: HDIAC, Defense Systems Information Analysis Center (DSIAC), and Cybersecurity and Information Systems Information Analysis Center (CSIAC).

HDIAC serves as the U.S. national clearinghouse for worldwide scientific and technical information in eight technical focus areas: alternative energy; biometrics; chemical, biological, radiological, nuclear, and explosives (CBRNE) defense; critical infrastructure protection; cultural studies; homeland defense and security; medical; and weapons of mass destruction. As such, HDIAC collects, analyzes, synthesizes, and disseminates related technical information and data for each of these focus areas. These efforts facilitate a collaboration between scientists and engineers in the homeland defense and security information community while promoting improved productivity by fully leveraging this same community's respective knowledge base. HDIAC also uses information obtained to generate scientific and technical products, including databases, technology assessments, training materials, and various technical reports.

State-of-the-art reports (SOARs)—one of HDIAC's information products—provide in-depth analysis of current technologies, evaluate and synthesize the latest technical information available, and provide a comprehensive assessment of technologies related to HDIAC's technical focus areas. Specific topic areas are established from collaboration with the greater homeland defense and security information community and vetted with DTIC to ensure the value-added contributions to Warfighter needs.

HDIAC's mailing address:

HDIAC
4695 Millennium Drive
Belcamp, MD 21017-1505
Telephone: 443-360-4600

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE	**2. REPORT TYPE**	**3. DATES COVERED**
August 2024	State-of-the-Art Report	

4. TITLE AND SUBTITLE Biometric Standoff Detection: Examining the Technologies, Implementations, and Developments of Biometric Systems	**5a. CONTRACT NUMBER** FA8075-21-D-0001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Megan N. Lietha, Trey Kibodeaux, and Doyle T. Motes III	**5d. PROJECT NUMBER**
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Homeland Defense & Security Information Analysis Center (HDIAC) SURVICE Engineering Company 4695 Millennium Drive Belcamp, MD 21017-1505	**8. PERFORMING ORGANIZATION REPORT NUMBER** HDIAC-BCO-2024-579
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Defense Technical Information Center (DTIC) 8725 John J. Kingman Road Fort Belvoir, VA 22060	**10. SPONSOR/MONITOR'S ACRONYM(S)** DTIC
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Distribution Statement A. Approved for public release: distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Biometric systems are used independently or in tandem with other systems to establish a person's identity, such as for surveillance and monitoring (law enforcement trying to track persons of interest) or to ensure identification for security (a person's face unlocking a phone). Performing these observations at a significant physical standoff is important for organizations clandestinely monitoring individuals to ensure they do not pose a security risk and to provide security to the everyday lives of those interacting with online services. Characteristics capable of being monitored include facial features (facial recognition), distinguishing features (tattoos, vein patterns), acoustic patterns (voice), and repetitive characteristics (arm motions, gait). Active research includes increasing the standoff distance biometric capability of systems and extracting a person of interest, visually from crowds and acoustically from a cacophony of voices. This report details available state-of-the-art hardware and software that provide biometric identification at increasing standoffs and degrees of noise. Standoff biometric-sensing options and pros and cons of these systems (with a focus on homeland defense and security) are discussed. Ways in which hyperspectral data fusion can be used to bring further certainty to identification and allow more conclusions to be remotely drawn about a person's emotional state or motivation are also examined.

15. SUBJECT TERMS
biometrics, standoff detection, multimodality, artificial intelligence, machine learning, facial recognition, gait recognition

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
U			UU	60	Vincent "Ted" Welsh
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED			443-360-4600

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

ON THE COVER:
(Source: Shutterstock)

THE AUTHORS

MEGAN N. LIETHA

Megan N. Lietha is a writer and editor from Austin, TX, and is the publications manager at Texas Research Institute, Austin, Inc. She has written and edited for software companies, technology firms, independent authors, and small businesses. She has additional training in technical writing and editing and is a member of the Association for Proposal Management Professionals. Ms. Lietha holds a degree in professional writing from the University of Oklahoma's Gaylord College of Journalism and Mass Communication.

TREY KIBODEAUX

Trey Kibodeaux is a writer and editor from Lake Jackson, TX, and is a publications editor at Texas Research Institute Austin, Inc. He is a technical writer with experience in a wide range of different subjects. He holds a degree in English literature from the University of Houston at Clear Lake in Clear Lake, TX.

DOYLE T. MOTES III

Doyle T. Motes III, P.E., is a licensed professional engineer in the state of Texas and is the director of the Nondestructive Evaluation Division of Texas Research Institute, Austin, Inc. He has extensive experience and has published in the fields of pulsed power, materials engineering and processing, sensing and sensor development, and nondestructive testing. His research interests include additive manufacturing, materials engineering, processing, nondestructive testing (in particular, ultrasound and eddy current testing), sustainment of aging aircraft, automation of inspection/validation technologies, materials state sensing, and high-temperature material properties. Mr. Motes holds bachelor's and master's degrees in mechanical engineering from the University of Texas at Austin.

ABSTRACT

Biometric systems are used independently or in tandem with other systems to establish a person's identity, such as for surveillance and monitoring (law enforcement trying to track persons of interest) or to ensure identification for security (a person's face unlocking a phone). Performing these observations at a significant physical standoff is important for organizations clandestinely monitoring individuals to ensure they do not pose a security risk and to provide security to the everyday lives of those interacting with online services. Characteristics capable of being monitored include facial features (facial recognition), distinguishing features (tattoos, vein patterns), acoustic patterns (voice), and repetitive characteristics (arm motions, gait). Active research includes increasing the standoff distance biometric capability of systems and extracting a person of interest, visually from crowds and acoustically from a cacophony of voices. This report details available state-of-the-art hardware and software that provide biometric identification at increasing standoffs and degrees of noise. Standoff biometric-sensing options and pros and cons of these systems (with a focus on homeland defense and security) are discussed. Ways in which hyperspectral data fusion can be used to bring further certainty to identification and allow more conclusions to be remotely drawn about a person's emotional state or motivation are also examined.

ACKNOWLEDGMENTS

The authors would like to thank Mr. John Clements of the Homeland Defense & Security Information Analysis Center for his guidance in this effort.

CONTENTS

CONTENTS, *continued*

FIGURES

TABLES

SECTION 01 INTRODUCTION

The biometric technology industry has seen rapid development, particularly in biometric detection software, in the past decade due to the introduction of new and more advanced artificial intelligence (AI) and machine learning (ML) tools. Advancements in AI tools such as deep convolutional neural networks [1] (also called deep learning), computer vision, computer processing for large AI datasets [2], better and larger training datasets, and many other software-driven improvements are allowing dramatically improved capabilities in biometric detection technologies. For facial recognition technology (FRT), not only have general accuracy and speed dramatically improved, particularly in adverse conditions (such as low light and low resolution, partial face covering, etc.) [3], but liveness detection, spoofing detection [1], and newer biometric methods (such as human-emotion detection) have all improved with the implementation of new AI/ML techniques. These improvements are proliferated across the entire sphere of biometric detection modalities and are seeing varying degrees of real-world application by both industry and government.

As biometric technologies are improving and becoming both faster and more reliable, they are being employed across a broad spectrum of operations. The biometrics industry was valued at over $34B globally in 2022, with North America making up more than 30% of that market [4]. According to one study, as of 2022, approximately 79% of U.S. businesses (872 respondents surveyed) are now using biometrics in two-factor authentication for users, up from 27% in 2019 [5]. The financial sector has launched a plethora of voice-recognition biometric tools, including many customer-facing tools, allowing users to make payments and conduct banking transactions through smart speakers. Based on a survey by Forrester in 2021, an estimated 30% of U.S. adults had used voice-activated devices and smart speakers to check account balances and perform banking functions [6, 7]. Financial institutions are also utilizing voice recognition for authentication and in customer-service applications [8]. At least 9 of the top 12 U.S. banking institutions employ voice recognition as an authentication method in their banking services. An address by U.S. Senator Sherrod Brown in 2023 identifies 6 institutions [9], and research into the top U.S. banks identified on Wikipedia [10] shows at least 3 others providing voice-recognition services [11–13]. In the retail industry, more companies and major retailers are turning to FRTs to prevent and deter theft, including stores such as Home Depot, Lowe's, Macy's, and Walmart [14]—who was also reportedly developing the technology to analyze shoppers' emotions in store in 2017 [15, 16].

In addition to the growing commercial use of biometrics, according to the U.S. Government Accountability Office (GAO), "three quarters of U.S. federal agencies surveyed…are already using facial recognition, and more than 40% [had planned] to use more of the technology by 2023" [17, 18]. The agencies who reported using FRT also "reported using FRT for one or more purposes, with digital access and domestic law enforcement as

the most common" [18]. While the most commonly reported use for FRT in the GAO's report was for digital access and cybersecurity (i.e., employees unlocking devices using biometrics), the next most common uses were for law enforcement (identifying persons of interest), physical security (access to and surveillance of secure facilities), and border/transportation security (identifying people crossing borders), as well as national security (monitoring potential threats both domestically and abroad). Facial recognition and fingerprint identification (ID) are the most common biometric modalities used by federal agencies, and facial recognition is quickly growing in its use and implementation. U.S. federal agencies owned at least 27 facial recognition programs in 2020 [18], and the Transportation Security Administration (TSA) has implemented the Credential Authentication Technology (CAT-2) FRT system in 84 U.S. airports, with plans to expand it to as many as 400 airports in coming years [19].

While the United States is increasing implementation of biometric systems in public sectors, other countries have already been utilizing widespread or cutting-edge biometric systems. China runs not only one but multiple infamous statewide surveillance operations. Its surveillance state began in the 2000s with the Golden Shield project, which established a nationwide closed-circuit television (CCTV) network and connected its policing forces with access to video feeds [20, 21]. This early surveillance system coincided with the beginning of establishing a social credit system, which fully launched in 2014, designed to act as a credit system with greater reach than similar systems in other countries by incorporating a social credit aspect to increase national "trustworthiness" [22]. More recent programs include the Sharp Eyes program started in 2016, which "could allow community workers to proactively go to individuals' doors to investigate a crime that has not even been committed yet" [23], as well as the Strike Hard Against Violent Terrorism program launched in 2014 to monitor and control Muslim minorities. Russia, in addition to China, is producing cutting-edge FRT technology and is recognized for developing some of the top-performing matching algorithms. According to accuracy tests carried out by the National Institute of Standards and Technology (NIST), "at present, 9 of the top 10 performing 1:1 algorithms were developed by Chinese or Russian companies" [24]. Russia had reportedly used facial recognition to monitor residents during the coronavirus lockdown in 2020 [25] and to identify and detain protestors of Russia's war in Ukraine in 2022 [26]. Additionally, Russia and China are not the only countries to use biometrics programs to track, monitor, and detain people. Israel was revealed earlier this year to have implemented an extensive facial recognition program cataloging Palestinians crossing borders and living in Gaza, which was then used as a means to target individuals in crowds in the unrest resulting from the October 2023 Hamas attacks [27]. The program was developed by a domestic Israeli corporation and has allegedly also used Google Photos recognition technology to help make IDs, particularly when an image only captures partial visibility of the face.

Where the United States lags behind other countries is not in the pervasive monitoring of its citizenry but in the funding, implementation, and management of new systems at all levels, from federal agencies down to local law enforcement. Developing advanced systems for capturing, analyzing, and potentially storing information, as well as ensuring data accuracy and fidelity and addressing privacy concerns and needs for sensitive data storage, particularly while following relevant policies and regulations, are all hurdles to updating and implementing new state-of-the-art biometrics systems. One GAO report requested by Congress identified one such major shortcoming in the lack of follow-through on the development of a countrywide "exit system" [28, 29]. With only one half of a completed entry-exit system, the United States lacks robust abilities to track visa overstays, improve immigration enforcement, and monitor potential criminal or terrorist activities [30]. According to GAO, the U.S. Department of

Homeland Security (DHS) has made steps toward identifying the need for an exit system for air-based travel, but this still leaves gaps for land and port points of entry/exit [29]. Other programs, like TSA's new CAT-2 FRT system, while improving current technology, will take many years to roll out nationwide and, in that time, superior technology will likely be developed. Addressing the gaps created by cyclical replacements of existing technology for more state-of-the-art systems capable of addressing ever-evolving, ever-present security threats is an important consideration for policy and program decision-makers.

1.1 EXPLAINING BIOMETRICS

From unlocking smart phones to positively identifying combatants on the battlefield, biometrics is becoming increasingly utilized across modern-day broader society in identifying and authenticating people, allowing access to doors, devices, data, transportation, and other areas (including across borders and into military bases). Governments and corporations across the world have acknowledged the inherent value in peoples' biometric data, as they move to replace older, less reliable methods of identifying individuals and allowing access. For instance, even common consumers and iPhone users would rather use their phone's fingerprint or Face ID technology to verify their identity, therefore granting access to the device, than continue to rely on passwords and keys that can easily be lost, forgotten, or even stolen. Biometrics, on the other hand, is not entirely subject to these shortcomings, as it relies on the values and measurements of an individual's bodily makeup to come up with unique identifiers. The score or value given through biometric measurements does not change and cannot easily be faked or manipulated, making biometrics the perfect passcode for authorized individuals.

The most common biometrics used today primarily constitute fingerprint, face, and voice recognition, though several other biometric modalities exist, including iris, gait, vein patterns, and handprints, and some more experimental modalities are being explored, such as ear shape, heartbeat, or even odor detection. These modalities have evolved from a long history of earlier biometric ID techniques and have been spurned forward by several technological advancements along the way.

1.2 HISTORY

Biometrics, the ID of individuals based on their unique human characteristics, has been employed since the early ages of humankind. From the use of handprints as "signatures" by early cave dwellers, to the first use of fingerprinting for transactional purposes in ancient China, people have been using unique biological markers to identify each other for centuries [31]. However, it was not until the 1800s that systems for cataloging and indexing fingerprints (as well as other types of biometric information such as eye color, height, and hair color) became common practice—these were primarily developed by and for policing and justice systems as cities grew and became more populated. Manual fingerprinting and ID prevailed until the late 1960s, when advancements in computing allowed digital systems to be developed. Alongside the rise of digital fingerprint recordkeeping, the early methodologies for facial, iris, voice, and automated signature/handwriting recognition were born. While fingerprinting is still the most commonly used modality for biometric detection [32], after 9/11, facial recognition has risen in response to anti-terror initiatives [33] and voice recognition is being used more and more in the financial and commercial sectors [34, 35]. Many events over the last several decades have either contributed to the advancement of biometric technologies or are significant markers of the growing importance of biometrics in modern society. Though recent advancements in this field are great, and seem to occur rather quickly, it is important to understand and acknowledge its long history and development in the decades prior to the year 2000.

1.2.1 1960–2000: Automation and Digitization of Biometrics

An article by S. Mayhew [31] provides a biometrics history timeline. The implementation of automated biometric ID started in the 1960s when the "first semi-automatic face recognition system was developed by Woodrow W. Bledsoe under contract to the U.S. government." For this system to work, the user would outline the subject's facial features and the distance between feature points was measured and applied for a match with reference data. Also during this time, the first model able to show how people can engage in acoustic speech, physiologically, was created and published by a Swedish Professor, Gunnar Fant. Later, the Federal Bureau of Investigation (FBI) found itself becoming overwhelmed with the standard process involved with recording and recognizing fingerprints by hand and, in 1975, it began funding what can be thought of as early biometric scanners that were able to collect fingerprints and store other useful images and information. In 1985, ophthalmologists Dr. Leonard Flom and Dr. Aran Safir made the scientific claim that "no two irides [irises] are alike" and the two "were awarded a patent for their concept that the iris could be used for identification." They took this discovery to Dr. John Daugman with the task of developing an algorithm to automate iris recognition, for which a patent was later awarded in 1994. The late 1980s also saw the first deployment of the semi-automated facial recognition system, and, "in 1988, the Lakewood Division of the Los Angeles County Sheriff's Department began using composite drawings (or video images) of a suspect to conduct a database search of digitized mugshots." Five years later, in 1993, the face recognition technology evaluation was sponsored by the Defense Advanced Research Products Agency to assess various facial recognition systems for quality and standards and help them become commercially viable. That year also saw the FBI hold a competition for private industry to develop an Integrated Automated Fingerprint Identification System (IAFIS), and, jumping forward to 1998, the bureau launched its DNA forensic database, the Combined DNA Index System, known as CODIS. In the next year, IAFIS was deployed and mostly operational, allowing for the checking of fingerprints across multiple different matching systems and databases.

1.2.2 2000s–Present: 9/11, the Boston Marathon Bombing, and the COVID Pandemic

Along with the rise of computer technologies that came with the start of the 2000s, which did a great deal to increase biometric capabilities in authentication and ID, there were several particularly outstanding events that played a great role in the United States in either forwarding the study of biometric recognition technology or that biometrics greatly impacted due to the success or failure of the implementation of the technology at the time.

The most impactful event of the early 2000s was, of course, the terrorist attack on 11 September 2001. This incident led to a heightened security apparatus, with the United States and other Western world governments taking action and passing legislation to deter any future terrorist attacks. The United States passed the Homeland Security Act of 2002 and the Patriot Act, which established the DHS and allowed the government the ability to monitor all communication of its citizens and foreign terror suspects. Then, "a few years later, in 2004, the 9/11 Commission's final report called for the installation of biometric scanning devices to be used on those entering and leaving U.S. borders" [33]. The United States then used biometric screening, in the form of facial recognition, on immigrants, those crossing its borders, and even on combatants overseas in Iraq and Afghanistan to identify enemies [33].

Identifying terrorists proved to be quite a difficult task, as so much ID and communication data had to be combed through for so many different individuals, that it has been commonly equated to

"looking for a needle in a haystack," as former army intelligence officer William Buhrow said [33]. Still, the newly adopted security effort continued, and places like Iraq and Afghanistan became the testing grounds for biometric recognition technology for much of the 2000s and 2010s. Since these countries were outside of the United States and lacked any real protections or rights to privacy for their citizens, less pushback and risk were involved with trying and employing new security measures and tactics. To successfully find matches using biometric technology, a robust matching database of individuals' biometric information had to be developed. The United States allowed the private sector to meet these needs by "supplying fingerprint readers, iris scanners, and database solutions" [33]. Throughout this time in the Middle East, biometric data were collected from "nearly every person [the U.S. military] came into contact with: suspected insurgents, enemy combatants (both dead and alive), detainees, military contractors, and applicants seeking to work on U.S. military bases or join the Afghan or Iraqi police, as well as ordinary citizens" [33]. These years of experience with biometric recognition, while ethically murky today, spurred the development of new technologies and techniques, forming modern, complex, and competent systems by putting the technology into practice in real environments with real people as subjects.

In 2013, the limits and capabilities of FRT were tested after the infamous Boston Marathon Bombing, as the local police force and FBI tried to use this technology to identify and catch those responsible for the attack. The attack was an attempt by the Chechen Tsarnaev brothers to place and detonate two homemade bombs along the sidelines of the annual Boston Marathon. The attack resulted in over 250 injured and 3 deaths. Although the two brothers and suspects were captured through multiple CCTV videos and other media, FRT, at the time, was unable to decipher their identities due to the low quality of the video and picture, as well as the technology itself not being ready for such a daunting and practical task [36]. D. McCormick notes that [37]:

> According to the Post, "facial recognition software did not identify the men in the ball caps [the two suspects]. The technology came up empty, even though both Tsarnaevs' images exist in official databases. Dzhokhar had a Massachusetts driver's license, the brothers had legally immigrated, and Tamerlan had been the subject of some FBI investigation." Image analysis software [had] not caught up with the grimy reality of street photography: low-resolution, long-range images—often poorly focused, rapidly moving, and caught from odd angles.

Once video was captured of the suspects, and since the combined effort of the law enforcement agencies present at the time were unable to identify the suspects themselves, the decision was made by law enforcement to release the information (video footage and images of the suspects) to the public for help with identifying them [37]. "For the first time at scale, the FBI took the unprecedented steps of opening their tip line for the public to submit photos and videos to aid the investigation. The response was overwhelming, and the FBI was quickly inundated by terabytes of multimedia from private citizens who wanted to help" [36]. Despite the flood of information, including family members positively identifying the suspects, the manhunt eventually led to a shootout after the brothers attempted to flee [37]. After this incident, a major issue study was conducted by the FBI, and the assessment found that, "at the time, face recognition technology wasn't built for unconstrained environments with unusual angles or lighting, and it certainly wasn't built to handle terabytes of data in seconds" [36]. While FRT was able to make positive IDs of mugshots, still-frame photographs, and compliant subjects, identifying moving targets with varying

degrees of image quality and visibility was still out of reach. "Since 2013, the field of biometric and computer vision technology has made incredible progress. Face recognition technology is now faster, more accurate, and more reliable than ever before, enabling even small local law enforcement agencies to identify potential suspects more efficiently" [36]. One of the most significant advancements in the technology was the development of a new processing technique—rectified linear unit, called ReLU, which is a formula that improved and accelerated the ability for neural networks to analyze data for faster IDs. Additionally, in the commercial sector, the ancillary biometric scanners and camera quality improved dramatically.

While hardware and software advancements improved the capabilities to take clearer, higher-quality pixels, analyze data more quickly, and more positively and accurately identify subjects, the Covid-19 pandemic presented significant, new roadblocks to FRT and other biometrics. Since person-to-person direct contact was discouraged by the Centers for Disease Control (as well as other government bodies worldwide), the need for contactless biometric systems grew. An article by S. Carlaw [38] details biometric impacts of the Covid-19 pandemic. Mainly, iris and facial recognition were prioritized over applications like fingerprint and vein recognition for authentication and ID purposes during this time. This caused a change in the protocols, procedures, and even funding and research involved with previous methods of biometric recognition that relied heavily on fingerprint ID systems like law enforcement, border control, and travel security agencies. These modalities were combined or "merged with AI and machine vision—to develop systems capable of adapting to users' various different objectives and screening protocols." Along with these changes came great advances in the capabilities to collect greater amounts of data and process them at faster speeds, largely made possible by the ancillary improvements to biometric scanners and cameras, as well as graphics processing unit and central processing unit capabilities. Another major obstacle to existing FRT software was the need to identify people with masks obscuring portions of their faces. New algorithms needed to be developed to use different and fewer parts of the face for positively matching people to database records. Also, with the widespread use of protective face coverings came the need to further develop and use iris-scanning technology as an alternative biometric modality. Carlaw states, "The most immediate impact of Covid-19 is that contactless technologies like face and iris recognition [were then] being forced to adapt to the emergent threat. Biometric AI and ML algorithms are being pushed to new heights to extend governments' protective, monitoring, and screening reach."

1.3 BIOMETRICS BASICS AND MODALITIES

Biometric ID can be performed through an array of methods, using a variety of different biometric markers, and in many different environments. This report aims to explore the state of the art for standoff biometric detection, or the detection of biometric identifiers at a distance of one to several hundred meters from the target subject [39]. To elaborate, contact biometrics involves a biometric reading being taken either in contact with a subject or within mere millimeters. These methods include, for example, fingerprint, palmprint, or iris scans taken by contact or extremely close proximity. Medium-distance standoff detection ranges from a few inches to several feet, such as face recognition scans performed from a few feet away or a palmprint scan being taken from a few inches away. Long-distance standoff detection (also called remote biometrics) is the detection of biometric identifiers for individuals at least 1–2 m or greater from the sensing system, such as identifying a single individual in a crowd or from across a room or street.

The methods for obtaining biometric readings at different distances can vary, and, generally, the larger the distance, the less fine or detailed the identifying marker will be, but the key objective for any biometric system primarily falls into one of two categories: (1) ID or (2) verification. ID is the process of taking in information for an unidentified subject and identifying that person from a database of records, also commonly called 1-to-many or 1-to-N matching [40]. Verification (also referred to as authentication) is the process whereby a subject is presented as a known entity with biometric identifiers matched against a known record of the subject, also called 1-to-1 matching. Biometric ID has been used primarily on borders, in battlefields, and in law enforcement to identify targets and wanted suspects of crimes. Biometric verification is commonly used to restrict or control access to data or spaces by authenticating the person's identity to gain access. These authentication methods can usually be found in transportation hubs, border checkpoints, military bases, and private industry.

Every biometric modality, or key category of identifier (i.e., face, finger, voice), uses different techniques to capture and analyze biometric data, but all share some common, overarching concepts. First, most systems involve an enrollment process, whether this is done cooperatively or noncooperatively with a subject [41]. Enrollment is the first step of scanning one or more biometric features. This is typically done cooperatively with the subject, who willingly provides biometric data to be scanned. However, it can also be done noncooperatively, where biometric data are recorded either unknowingly or with a noncooperative subject, such as covering the face or not remaining still for the capture process. The individual record that is stored, such as a fingerprint, is called a sample; multiple samples are often taken in a single scan or recording event. These samples are combined and labeled based on the taxonomy of the recognition system into what is known as a template, which can be stored and used for later verification or ID purposes (Figure 1-1).

Combining different modalities, known as multimodal biometrics, greatly increases the rate of positive IDs by utilizing multiple different possible data points or identifiers. In terms of standoff detection, multimodal biometrics is key to increasing the probability for making IDs, particularly at greater distances, and is identified as a key area for continuing research.

Ensuring positive ID and verification is paramount to successfully employing any biometric system, and there are a few key metrics used across different systems to determine the accuracy of a program. False acceptance rate (FAR) and false rejection rate (FRR) are two of the most common measurements used to measure a verification system's success, whereas false positive identification rate (FPIR) and false negative identification rate (FNIR) are commonly used in measuring an ID system's success [42]. FAR is "the probability of cases for which a biometric system fallaciously authorizes an unauthorized person" [41]. FAR measures false acceptance in the percentage of instances that an unauthorized individual is falsely authorized by the system, so a rate of 0.01% equates to 1 false acceptance in 10,000 cases. FRR, conversely, is the measure of the number of instances that an authorized individual is not correctly matched by a system, or returns a "no match" response. FPIRs, much like Covid-19 and pregnancy tests, are the measurement of the rate of a positive ID being made with no matching identifying record [43]. An example is when a system incorrectly identifies a person as matching the record for a wanted felon. FNIRs measure the opposite, or the rate of instances where a system fails to correctly identify an individual for whom a record does exist, such as a wanted felon not being matched to an existing record by a security system or law enforcement database. Beyond these basic steps, each modality employs different techniques and approaches to capture, catalog, and analyze biometric data.

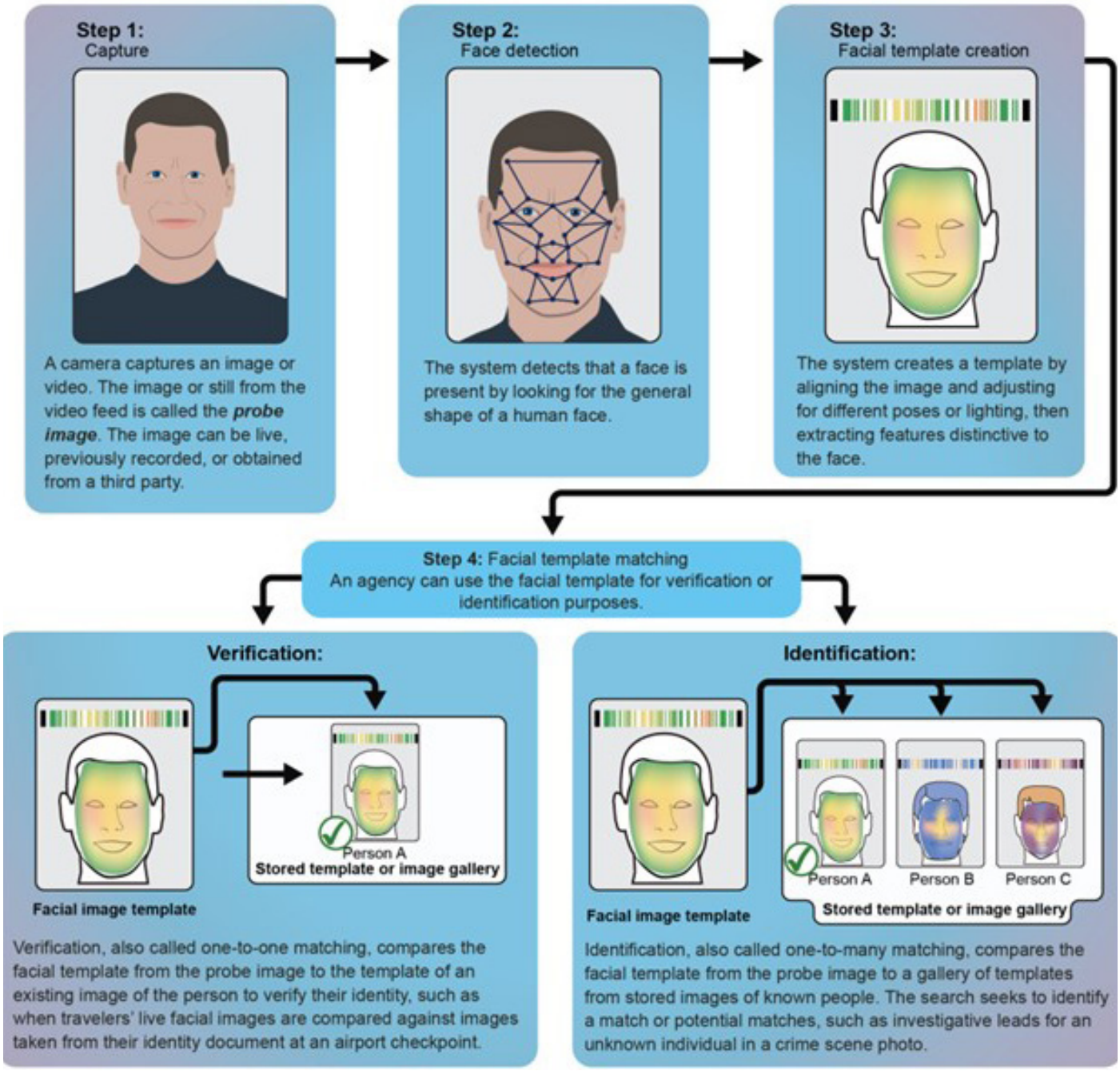

Figure 1-1. Biometric Recognitions Process Showing Capture and Template Creation *(Source: GAO [44])*.

1.3.1 Fingerprints, Palmprints, and Vein Patterns

Fingerprint biometrics is one of the most well-known and historically often-used biometric modalities in the world. Fingerprints and palmprints are completely unique to each individual and are composed of the patterns of ridges, arches, loops, whorls, wrinkles, and textures of each individual finger and hand [45, 46]. Today, most finger and palmprint scans are done with optical sensors that light up the hand or finger through a prism and read the reflection of the light off of the ridges and valleys to create an image [47].

A capacitive scanner (typically very small, not used for whole-hand scans, and commonly found in consumer electronics) uses an array of capacitors to detect electrical currents from the finger, which it turns into a map of the fingerprint's ridges (contacting the surface of the sensor and conduct current) and valleys (leaving a small airgap and therefore nonconductive) [47].

The latest technology in fingerprint scanning includes ultrasonic transmitters and receivers. Ultrasonic scanners emit an ultrasonic pulse and measure the reflected signal to create a three-dimensional (3-D) image of the fingerprint [48]. Ultrasonic scanners can provide extremely detailed scans, even for hands that are dirty or wet, but are slower and more costly than optical and capacitive scanners.

Vein patterns are yet another unique aspect of the hand, and the past decade has seen a rise in the development of this modality, which has been particularly useful as a noncontact authentication method. Vein (or vascular) patterns are imaged using near-infrared (IR) light to illuminate the vascular pattern of either one or more fingers or the palm [49]. Using light-emitting diodes (LEDs) to shine IR light through the hand, the differences in reflected light, which vary through different tissues and the blood vessels, are observed.

Fingerprints, palmprints, and vascular patterns are all generally considered contact or near-contact biometric modalities and, while constituting a large sector of the biometric authentication market, are not particularly adaptable to remote or long-distance biometrics. However, that does not mean finger and palmprint recognition at a distance is strictly impossible. Researchers in Japan in 2017 used photographs of people using the "peace" hand sign to copy individuals' fingerprints with success [50]. Currently, replicating this success requires extremely high-resolution cameras, perfect lighting, and angles for capture [51], but image-quality improvements in cameras may push this capability forward in the future.

1.3.2 Iris

"Iris recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of one or both of the irises of an individual's eyes, whose complex patterns are unique [and] stable and can be seen from some distance" [52]. Iris recognition is used for its high accuracy in identifying people based on the unique patterns within the ring-shaped region surrounding the eye's pupil. Iris recognition can be performed from at a greater range than similar eye-related recognition systems such as retinal scanning.

The iris ID system (drawn on from Daugman's work in 1994, though he was originally tasked with creating the method in 1989), involving a two-dimensional (2-D) Gabor filter and measuring the Hamming distance between the shapes of an iris captured in images [53], is considered one of the most accurate forms of biometric ID due to the amount of detail and texture in the iris. No two eyes contain the same iris formats, meaning someone's left- and right-eye irises are different as well. They also do not change shape over time, making them a very reliable source of biometric ID. Iris ID, recognition, and matching systems were improved upon throughout the late 90s and 2000s to eventually reduce any outside "noise" (like eyelashes) and to substantially increase the amount of test subjects used, reaching an accuracy rate of 99% by 2008. The first iris-recognition systems succeeded by utilizing the Hough Transform and measured the Euclidean distance between the shapes of the iris. However, researchers in this field went on to improve their accuracy in iris ID technology by increasing the number of methods employed, such as utilizing support vector machines and several filters and wavelets. The relatively modern iris ID and matching process also utilizes imaging technology and involves segmenting the iris into easily measurable portions.

1.3.3 Facial Recognition

FRT is perhaps the fastest-growing biometric recognition system in both use and interest, as it is currently being employed by militaries and security personnel all over the world, in addition to government border, immigration, and transportation organizations. Facial recognition involves identifying "facial vectors and features [and] matching them with pre-enrolled individuals" [54]. Facial recognition begins with detection, which involves algorithms identifying areas in images that match the "learned" features for a face and label the identified area (typically using bounding boxes). As the technologies have improved in recent years, identifying faces has reached the point that even oblique camera angles or partial face coverings are often not a hinderance to many detection algorithms. Once a face has been detected, its individual features can be measured. Measurements from distance between the eyes or between the nose and the lips to the depth of eye sockets and prominence of someone's cheekbones can all contribute to the individual template of data for a face scan. After feature extraction has been performed, ID or verification can be performed. FRT is one of the leading modalities in standoff biometrics, and more detailed information can be found in Section 2 of this report.

1.3.4 Voice and Acoustic

The Biometrics Institute discusses voice as [55]:

> A person's voice—i.e., the way they sound when they speak—is the result of a combination of distinctive physical attributes (such as the length of vocal cords and the shape of the throat) and distinctive behavioural attributes (such as the accent with which a person speaks).
>
> The human voice consists of/creates wavelengths that can be measured. The voice is collected and analysed by software that employs artificial intelligence and machine learning techniques to produce a vast array of data derived from factors such as modulation of speech, tones, accent, frequency, etc. These elements enable the system to create a reference template of the voice (known as a "voice print" or "voice model") that can be used to authenticate the speaker in subsequent transactions. Similar technology is applied to allow devices to understand, translate, and interact with a voice command/question, for example, when talking to smart speakers, mobile devices, domestic appliances, [or a] virtual assistant.
>
> There is a difference between speaker recognition (recognising who is speaking) in biometric applications and speech recognition (recognising what is being said), e.g., applications such as machine dictation, voice command systems, integrated telephony automation, etc. These two terms are frequently confused, as is voice recognition. In simple terms voice is a synonym for speaker and not speech.

This type of biometric mechanism is accurate but, like everything, is not infallible. Statistical models are used to determine the likelihood that a voice matches to the person on a saved voiceprint. Accuracy is affected by the means in which the original voiceprint was captured, which is affected by microphone quality, background noise, compression quality of stored voiceprint, etc.

However, several items are immediately evident when attempting to transition voice and acoustics to a standoff biometric ID system. First is microphone quality, which is determined by both hardware and software associated with the

voice-capture system. A sensitive microphone is required to capture acoustic voice data at a standoff, but such a system is also going to capture a great deal of other nearby noise even more so than a traditional microphone would, owing to the increased sensitivity (in this case, not exactly background noise since the signal-to-noise ratio is so low). For many hypothetical cases, microphone arrays are explored, but these come with issues as well when trying to sync these up to appropriately analyze the data [56]. There are numerous software tools now available that allow the removal of background noise from acoustic recordings, but the problem for standoff biometrics is that any voice of interest is now part of the background noise. As a result, although this methodology is a possibility for biometric detection, implementation at standoff distances has not taken place widescale and research into this area continues.

This Page Intentionally Left Blank

SECTION 02 TECHNOLOGY

A previous HDIAC report from 2021, titled "Artificial Intelligence (AI) and Machine Learning (ML) in Biometric Data Fusion" [57], discusses the advancements that AI has made in biometric ID processes and identifies the standoff range of biometrics as a target area for the application of data and computing advancements in the field. Deep neural networks are allowing researchers to make significant strides forward in improving biometric recognition across the industry. Additionally, the advancements made for FRT and other modalities in ML are being leveraged to help advance newer and less developed modalities such as gait and body shape, or whole-body recognition, which will be instrumental to furthering standoff detection at greater distances. The FarSight multimodal standoff detection system developed by researchers under the Intelligence Advanced Research Projects Activity (IARPA) Biometric Recognition and Identification at Altitude and Range (BRIAR) program tackles many of the core issues encountered at long ranges in biometric detection [58]. Developing these standoff recognition capabilities benefits security forces, homeland defense, border agents, and overseas military efforts.

2.1 CURRENT TECHNOLOGY

Many of the limitations and needs to improve the state of the art for standoff distance biometrics are dependent upon improvements in various aspects of imaging, and it is therefore important to understand how sensing in biometrics works by looking at the standards for microwave and millimeter-wave imaging.

2.1.1 Microwave/Millimeter-Wave Imaging

All biometric data come from exposing a person to a different type of electromagnetic (EM) radiation and observing changes in the returned signal. The most common frequency bands used for biometric capture are associated with nonionizing radiation, including visible light, IR light, terahertz radiation, and millimeter-wave radiation. Other nonionizing radiation, such as frequencies below millimeter waves (such as radio waves), produces wavelengths that are too long to interact with any features of interest on a human. Ionizing radiation types include gamma rays (not used), X-rays (commonly used for a number of everyday activities but cannot offer the means to clandestinely observe a person), and ultraviolet (UV) radiation. Millimeter waves have a variety of uses but are especially important in radio broadcasting and cell phone transmissions. Because the wavelengths of this type of EM radiation are large relative to natural and synthetic fibers, they tend to pass through most materials, such as clothing, making them an ideal candidate for scanning technologies. They cannot penetrate electrically conductive materials and will interact with materials containing water (such as the human body).

A millimeter-wave scanner is most commonly a whole-body-imaging device that is primarily used for detecting objects concealed underneath a

person's clothing using EM radiation. Typical uses for this technology include detection of items for commercial loss prevention, smuggling, and screening for weapons at government buildings and airport security checkpoints.

Millimeter wave is one of the technologies used for body imaging and is most commonly associated with use in TSA airport security screening processes. Although the exact definition varies, millimeter wave tends to encompass the use of EM radiation at frequencies between 300 MHz and 300 GHz. Lower frequencies are capable of penetrating through more materials (such as looking for firearms underneath many layers of clothing) but struggle to provide to high-resolution imagery. Higher frequencies cannot penetrate materials as well (and may struggle when being used farther from the target of interest) but have the capability to provide comparatively high-resolution imagery. All millimeter-wave radiation reflects from and does not penetrate metallic surfaces.

The wavelengths for this type of standoff inspection technique are fairly long, meaning that imagery generated tends to be less highly resolved than techniques that utilize shorter-wavelength EM radiation, such as visible light photography. However, this type of radiation is sensitive to other features on the human body that would be unique from person to person (or unique when used in conjunction with another inspection technique). Examples of this would include different EM signal responses reflected by and received at the receiver antenna from items such as birthmarks, differing blood flows, thermal differences, etc. It is also sensitive to the presence of potentially hidden items on a human under clothing (such as weapons). This type of screening is the most common use of millimeter-wave imaging.

2.1.1.1 Components for Microwave Imaging Systems

Components for imaging systems such as these will include numerous subcomponents, but, most importantly, will include antenna elements and sources that set the frequencies at which the system can operate. Each of these different systems is usually designed to a specific frequency band (or combination of frequency bands). There are a number of different means to delineate frequency bands, such as those shown in Table 2-1.

As mentioned, higher frequencies can provide higher resolutions in images but suffer from higher degrees of attenuation (meaning that they do not penetrate through materials as well). Lower frequencies provide lower resolution when producing imaging but can penetrate more deeply in materials. Generally, operating frequency ranges with a wide frequency band are often used to provide a balanced approach, although it is more important to design an imaging system that is properly targeted to the type of item being inspected.

Chips to enable microwave sources are the other most necessary component. These are most often semiconductor chips. Zhao et al. [59] discuss some of the most recent work in miniaturizing these chips.

2.1.1.2 Use of Millimeter-Wave Imagers for Biometrics

The first millimeter-wave full body scanner was developed at the Pacific Northwest National Laboratory (PNNL) in Richland, WA. In the 1990s, PNNL patented its 3-D holographic-imagery technology, with research and development support provided by the TSA and the Federal Aviation Administration [60]. In 2002, Silicon Valley startup SafeView, Inc., obtained an exclusive license to PNNL's intellectual property to commercialize the technology and developed a production-ready millimeter body scanner system and software [61]. This included scanner control and algorithms for threat detection and object recognition, as well as techniques to conceal raw images to resolve privacy concerns. By 2006, SafeView's body-scanning portals had been installed and trialed at various locations around the globe. These have been installed at border crossings, international

Table 2-1. Frequency Bands for Microwave/Millimeter-Wave Imaging

Rectangular Waveguide Band Letter Designation	Operating Frequency Range (GHz)	Rectangular Antenna Dimensions (cm × cm)
L	1.12–1.70	16.51 × 8.25
R	1.70–2.60	10.92 × 5.46
S	2.60–3.95	7.21 × 3.40
H or G	3.95–5.85	4.75 × 2.21
C or J	5.85–8.20	3.48 × 1.58
X	8.20–12.4	2.28 × 1.01
Ku	12.4–18.0	1.58 × 0.79
K	18.0–26.5	1.07 × 0.43
Ka	26.5–40.0	0.71 × 0.35
Q	33.0–50.5	0.57 × 0.28
U	40.0–60.0	0.48 × 0.24
V	50.0–75.0	0.38 × 0.19
W	75.0–110.0	0.25 × 0.12
D	110.0–170.0	0.17 × 0.08
G	140.0–220.0	0.13 × 0.06

airports, ferry landings, railway stations, government buildings, and commercial buildings and were employed to secure soldiers and workers in Iraq's Green Zone.

In 2006, SafeView was acquired by L-3 Communications (later L3Harris) [62]. In 2020, Leidos acquired L3Harris, which included its body scanner business unit [63].

Examples of millimeter-wave biometrics appear to split and include work to integrate data processing and analytics into the images produced. Advances to the hardware/software used to produce the images include augmenting other biometric systems with millimeter-wave technology as a means of confirming a face is actually being seen. Work like this is being performed by PNNL [64]. This work is seeking commercial partners to develop a prototype.

Examples of imaging systems that have been developed include work by Li et al. [65] (University of Science and Technology of China to produce a high frequency 76–81-GHz band unit), Dvorsky et al. [66] (Texas Research Institute and Iowa State University to produce a 26.5–40-GHz band unit), and Horst et al. [67] (Iowa State University) (see Figure 2-1). In either case and any other use case, the technology needs to drive toward being able to address longer standoff distances and data acquisition faster so the technology can move toward real-time video.

Realistically, millimeter-wave imagery is coupled with other biometric types to provide a check for the presence of hidden items that may present a threat. Such solutions are being fused with AI and ML tools [68]. Other groups have been able to demonstrate work on using millimeter-wave technology for determination of facial expressions [69].

Figure 2-1. Example of Millimeter-Wave Imagers Operating at Different Frequencies and Designed for Inspections Through Different Materials *(Source: D. Motes)*.

2.1.2 Practical Limitations on Microwave/ Millimeter-Wave Imaging

The most common type of a microwave/millimeter-wave imaging system is that seen in airports to inspect for suspicious items on a person. Imaging systems that would be used for biometrics are subject to the same type of constraints. The most common of these would be a consistent standoff distance (and potentially a specific distance range in which the inspection target is being imaged) with a stationary inspection target. These may limit the deployment of this type of technology to individuals who participate in a biometric screening willingly. Millimeter-wave imagers also have problems reading through sweat, in addition to yielding false positives from buttons and folds in clothing.

2.2 TECHNOLOGICAL LIMITATIONS AND SOLUTIONS

There are several limiting factors affecting the development of reliable and highly accurate standoff-range biometrics, and many of these factors are inter-related, particularly as they pertain to hardware. While there are cameras capable of taking extremely long-range and high-quality still photos and videos, these cameras tend to be large and prohibitively expensive, making them unlikely choices for either large-scale or covert detection operations. Even assuming state-of-the-art cameras, issues arise immediately with elevated viewing angles, platform vibration, air turbulence (at particularly great distances of 300+ m), inferior or incomplete capture data due to moving targets and unconstrained environments, and even time of day. Several research groups have been working to tackle many of these issues, including developing new models for imaging through turbulence, improving the state of the art for gait and body shape modalities, and developing better multimodal systems.

There is a technology gap between high-quality cameras and research involving state-of-the-art systems with actual in-the-field applications, where camera systems are typically not the highest available quality. In-the-field camera systems can be broken down into a few categories: (1) indoor and close-range cameras, (2) midrange cameras, and (3) specialized cameras. Indoor and close-range cameras, like those found in a typical security setting, and standard digital single-lens reflex (DSLR) cameras are used to acquire close-range still images. "These systems are used at either the indoor, controlled collection...or at close distances. Midrange cameras have larger zoom range, are capable of narrower fields of view, and are often high-end commercial-off-the-shelf (COTS) systems. These camera systems are leveraged for facial imaging up to 300 m and [whole body] WB imaging up to 600 m" [70]. Specialized cameras can be defined as custom integrated imaging systems using high-end optics and sensors that can be adjusted to achieve higher resolutions, variable frame rates, or other imaging optimizations. These cameras include long-range and military-grade cameras "designed specifically for surveillance from significant distances. These systems are either specialty COTS systems or imaging systems actively used in strategic operations" [70].

In terms of image quality and value to biometric recognition, "recognition accuracy performance rapidly declines once face regions with an area of 32×32 pixels or below are present" [71]. In order to combat low-quality images, image restoration can

be performed. However, there is a risk of changing identity in the process [58]. Therefore, it is essential that any image restoration work performed improves downstream performance. Additionally, using multiframe fusion is shown to alleviate some of these issues. Extreme pitches or angles between the capture system and target, typical of long-range biometric recognition, also present issues to image quality and processing capabilities. At particularly extreme angles, facial recognition can be rendered entirely ineffective due to the loss of visible features needed for modeling and ID. Overall image quality at great distances can also be affected by air turbulence or weather phenomena. "The presence of turbulence over horizontal imaging paths severely reduces the resolution available to imaging systems and introduces anisoplanatic distortions in the image frame" [72]. Recent approaches have been developed to combat air turbulence perturbations in image processing by modeling the turbulent volume and the resulting perturbations of light passing through it. Additionally, "simulating these effects most often comes in the form of mirroring nature: a wave is numerically propagated through a simulated atmosphere" [58]. Finally, the movement of a target through the frame can also alter image quality and processing. Adapting new modalities to recognize biometrics for larger human movement patterns, such as gait and whole-body recognition, and integrating these modalities into multimodal systems are the focus for current research in adapting new technological advances to standoff detection.

2.2.1 Developments in Gait and Whole-Body Detection Modalities

Gait recognition algorithms are used to identify individuals based on their walking patterns. These algorithms consider both dynamic and static features of the human body, such as body shape [73]. Human gait has person-specific characteristics, and studies show that humans can deduce gender and recognize known individuals based on gait. Gait biometrics can be acquired passively, eliminating the need for explicit subject interaction. However, the matching performance of these algorithms is influenced by factors like clothing, footwear, walking surface, speed, and direction. Additionally, the gait pattern can change over time, making it difficult to mitigate. Therefore, evaluation of gait recognition algorithms is primarily conducted in controlled environments, and more research is needed to promote its incorporation into commercial biometric systems.

Analyzing human gait and 3-D body shape provides a higher pixel area target for recognition operations, thereby increasing the functional data that can be processed for ID purposes. Both gait recognition and whole-body recognition are still being developed by researchers, and these systems have yet to be widely deployed for field operations. "When a person walks, it is possible to observe around 24 individual parameters and movements that form the uniqueness of their gait" [74]. "Every human has a specific way of walking and running. Factors such as the subject's overall physique; stride length and width; speed of movement; [and] the various angles formed by the joints at the hip, knee, and ankle, as well as the angles of the torso, thighs, and feet, can be captured on cameras for analysis" [75]. IARPA has established the BRIAR program to tackle many of these challenges head on. One aspect of the program is developing gait and whole-body recognition techniques and fusing them with existing technologies into a multimodal recognition package.

Gait recognition begins with identifying the human shape and its constituent parts. Three-dimensional modeling of the human shape relies upon locating joints on human subjects in single frames, but this is difficult to accomplish. Researchers have instead developed a method to model the 3-D orientations and rotations for each joint, called Human Mesh Recovery. This new approach overcomes hurdles such as the lack of large-scale, ground-truth, 3-D annotation for in-the-wild images, the inherent

ambiguities in single-view 2-D-to-3-D mapping, and scale ambiguity between the size of the person and the camera distance. According to researchers on the Human Mesh Recovery framework [76]:

> ...a key insight is that there are large-scale 2-D keypoint annotations of in-the-wild images and a separate large-scale dataset of 3-D meshes of people with various poses and shapes. [Their] key contribution is to take advantage of these unpaired 2-D keypoint annotations and 3-D scans in a conditional generative adversarial manner. The idea is that, given an image, the network has to infer the 3-D mesh parameters and the camera such that the 3-D keypoints match the annotated 2-D keypoints after projection. To deal with ambiguities, these parameters are sent to a discriminator network, whose task is to determine if the 3-D parameters correspond to bodies of real humans or not. Hence, the network is encouraged to output parameters on the human manifold and the discriminator acts as weak supervision. The network implicitly learns the angle limits for each joint and is discouraged from making people with unusual body shapes.

The work performed on the Human Mesh Recovery framework supported further development by researchers in the BRIAR program. The Human Body Model-Based Biometric Identification (HMID) system is a continuation on whole-body modeling research that utilizes the training datasets developed for gait recognition by another group of BRIAR research participants. According to the research team, HMID [77]:

> ...exploits (but is not limited to) features tied to the anthropometric properties of the subjects for discrimination. [Additionally,] HMID is a robust approach to the challenges of long-range data, low image quality, elevated viewpoints, and view invariance. [Research augmented] the training of HMID by using degraded images and forcing its shape output to reproduce nondegraded shape data in the form of silhouettes extracted from the original, high-resolution versions of the images.

These developments have produced a system that does not rely on human silhouettes in the process of identifying body shapes.

The FarSight system has been developed by a group of researchers from multiple American universities under the BRIAR program. It pushes the envelope for long-range standoff biometric detection by addressing the hurdles in distance recognition, as previously discussed, as well as developing a model for turbulence, a new detection and tracking module, an image restoration method, and implementing multimodal biometric fusion [58]. The workflow begins with an input video sequence, which undergoes detecting and tracking, identifying regions of interest and forwarding them to gait and body modules for processing, as well as the face module for restoration.

The face module consolidates features across sequences. In addressing turbulence, FarSight utilizes propagation-free models that incorporate turbulence effects through random sampling at the aperture. With additional steps in processing, this approach allows for 1,000× faster propagation than split-step methods while maintaining accuracy, making it a suitable choice for the system [58].

The detection module uses a region-based convolutional neural network detector with a modified backbone to associate face and body bounding boxes. It uses associative embeddings to match faces and bodies, learned through pulling and pushing loss functions. Pulling loss

brings embeddings of the same subject closer, while pushing loss pushes away bounding boxes assigned to different subjects, accounting for intersubject variations. The losses are combined by a weighted sum, and the final associative embedding loss is a weighted sum of these losses [58].

The biometric image restoration methods utilize lightweight, real-time techniques to preserve identity. They are divided into single-frame and multiframe restorations, with single-frame restorations requiring lower throughput (with stronger priors) and multiframe restorations requiring larger throughput (with weaker priors) [58].

The multimodal fusion module of FarSight incorporates face, gait, and body shape. The study calculates per modality scores for each probe-gallery pair, creating a singular subject-level feature for face, gait, and body. Probe features are compared to gallery features, and an equal weighted sum score fusion is employed to generate a single score from cosine similarity scores. If feature extraction fails, missing scores are imputed to the middle of the score range, "which is zero for the cosine similarity metric" [58].

2.2.2 Nonoptical Sensor Applications for Biometrics

Current biometric technologies almost completely rely upon optical sensing for biometric detection and ID, but there is potential for using alternative EM ranges for detection, such as UV and terahertz sensing. UV imaging is not traditionally used for biometrics but does offer another option. UV imaging is a photographic process of recording images by using radiation from the UV portion of the EM spectrum. Images taken with UV radiation can reveal features that are not apparent under visible light (an example is shown in Figure 2-2, where applied patches of sunscreen are shown to block UV radiation from interreacting with the skin below the application site). Diagnostic medical images may be used to detect certain skin disorders or as evidence of injury.

UV illumination's potential for biometrics is the ability to identify specific skin disorders in humans, evidence of injury, and the application of particular substances. UV radiation is generally defined as extending from ~10 nm to 400 nm and is often divided into three bands [78]:

1. Near UV: Includes 200–380-nm wavelengths (abbreviated as NUV)
2. Far UV: Includes 10–200-nm wavelengths (sometimes referred to as vacuum UV; abbreviated as FUV or VUV)
3. Extreme UV: Includes 1–31-nm wavelengths (abbreviated as EUV or XUV)

"Only near UV is of interest for UV imaging" (and, hence, standoff biometrics capabilities). This is because Earth's atmosphere is opaque to wavelengths below ~200 nm and most transparent lens glass is opaque below ~180 nm. In addition, lower-wavelength UV is not used as a flash source due to the health hazard that this type of radiation poses. Near UV can be further subdivided into the following categories [78]:

- Long-Wave UV: Ranges from 320 to 400 nm (also called UV-A)
- Medium-Wave UV: Ranges from 280 to 320 nm (also called UV-B)
- Short-Wave UV: Ranges from 200 to 280 nm (also called UV-C)

Two options are available to use UV radiation for imagery: (1) reflected UV and (2) UV-induced fluorescence photography [78].

2.2.2.1 Reflected UV Photography

As the name suggests, reflected UV light is captured after bouncing off the subject, and any visible light

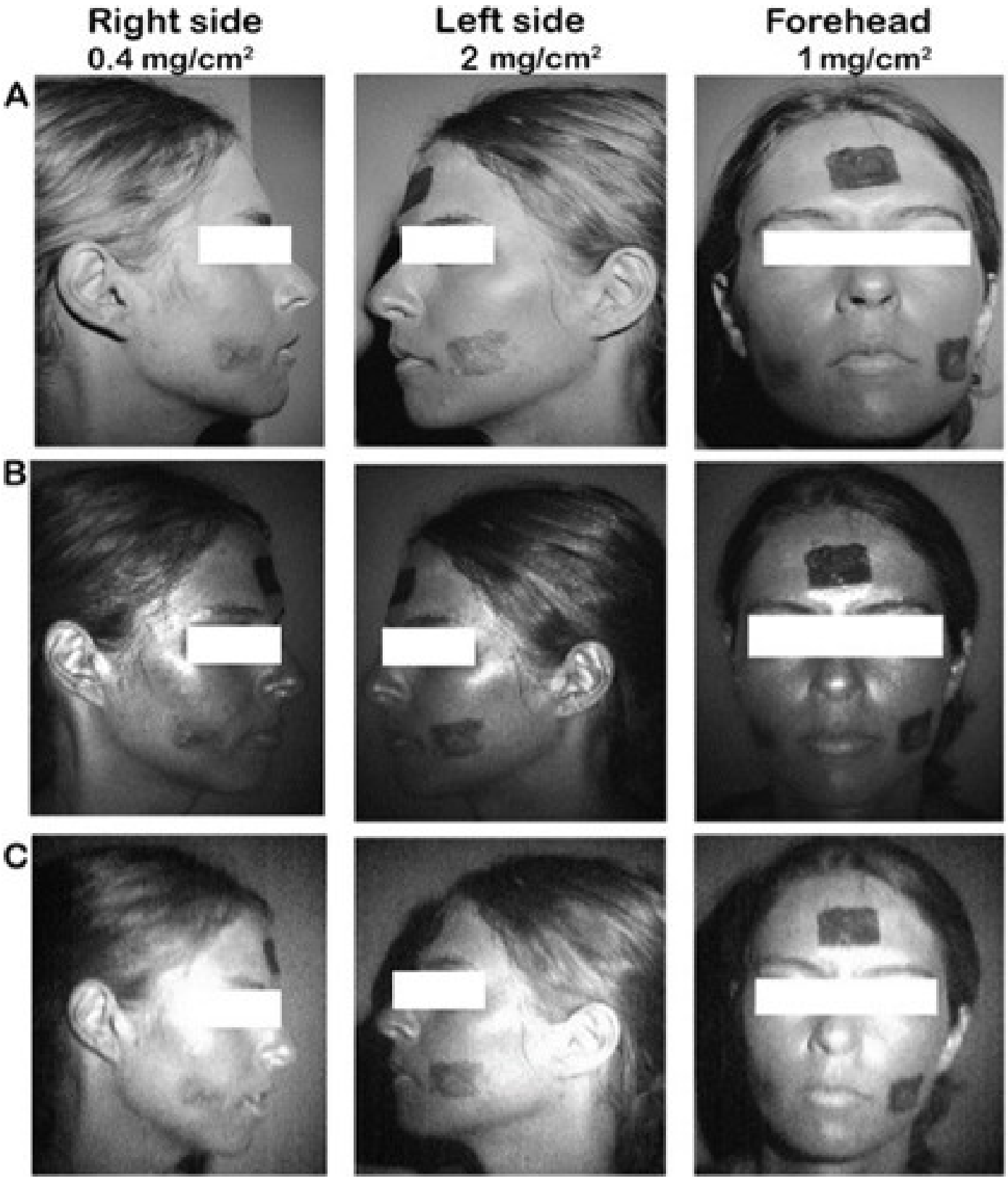

Figure 2-2. Comparison of UV Photography Device Images of Sun Protection Factor (SPF) 50+ Lotion Applied to a 4 × 2.5-cm² Area of the Cheeks and Forehead: (A) DSLR UV Camera, (B) Nurugo SPF Camera, and (C) Sunscreen Camera *(Source: Horsham et al. [79])*.

is deliberately blocked from entering the camera. Modifications may be needed to allow UV light to pass through modern lenses and be captured. In reflected UV photography, the subject is illuminated directly by UV-emitting sources or by strong sunlight. A UV-transmitting filter is placed on the lens, which allows UV radiation to pass into the camera and absorb or block all visible and IR radiation.

2.2.2.2 UV-Induced Fluorescence Photography

For UV-induced fluorescence photography, UV radiation is absorbed into the subject and visible light is re-emitted for capture by a traditional visible light camera with no modifications. This method of operation requires a dark environment and a UV-only radiation source. The most important aspect of UV fluorescence photography is the source of the UV light and controlling the visible spectrum (more on that later). This can include a pure UV source or a specific type of filter, which, again, blocks or absorbs all visible light radiation and only lets UV radiation pass through. These special bandpass filters look completly black when viewed by human eyes.

2.2.2.3 UV Radiation Sources

Sunlight is the "most available free UV radiation source" and is suitable for reflected UV photography (similarly to visible light photography). As with visible light photography, "the quality and quantity of the radiation depends on atmospheric conditions" (the presence of clouds and rain in the atmosphere block UV light) [78].

Much like visible flash photography, UV flash photography is accomplished with an electronic flash in conjunction with an aluminum reflector. "Most modern UV sources are based on a mercury arc sealed in a glass tube." This glass tube can be internally coated with suitable luminescent materials to become an effective long-wave UV source. Recently [78]:

> UV-LEDs have become commercially available [at affordable prices and in large quantities]. Grouping several UV-LEDs can produce a strong enough source for reflected UV photography, although the emission waveband is typically somewhat narrower than sunlight or electronic flash. Special UV lamps known as "black light" fluorescence tubes or bulbs also can be used for long-wave UV photography.

2.2.2.4 UV Filters

UV filters [78]:

> …are made from special colored glass [that contains materials internally that can block certain wavelength] and may be coated or sandwiched with other filters to aid in blocking unwanted wavelengths. Examples of UV transmission filters include the Baader-U filter or the StraightEdgeU UV bandpass filter, both of which exclude most visible and IR radiation. Older filters include the Kodak Wratten 18A, B+W 403, Hoya U-340, and Kenko U-360, most of which need to be used in conjunction with an additional IR blocking filter. Typically, such IR-blocking UV transmissive filters are made from Schott BG-38, BG-39, and BG-40 glass. Filters for use with digital camera sensors must not have any IR leak ([unwanted] transmission in the IR spectrum). [If any IR leakage occurs,] the sensor [within the digital camera] will pick up reflected IR radiation, as well as UV radiation, which [will] attenuate the contrast [within the produced image] and can even completely obscure the details that would be resolved solely by the UV radiation alone.

Most glasses will allow long-wave UV to pass through but will absorb all other UV wavelengths, usually ≤350 nm. Specially developed lenses

made from fused quartz or quartz and fluorite are necessary for UV photography to avoid focus shifts. Examples of the quartz and fluorite lenses include "the Nikon UV-Nikkor 105-mm f/4.5, the Coastal Optics 60-mm f/4.0, the Hasselblad (Zeiss) UV-Sonnar 105 mm, and the Asahi Pentax Ultra Achromatic Takumar 85-mm f/4.5" (Kodak) [78].

Acceptable digital cameras (that do not require customized modifications) for reflected UV photography include the Nikon D70 or D40 DSLRs. Many other digital cameras can be made to be suitable for UV photography "after having their internal UV- and IR-blocking filters removed. The Fujifilm FinePix IS Pro digital single-lens reflex camera is purpose-designed for UV (and IR) photography," with wavelength responses rated from 380 to 1,000 nm. The primary material (silicon) used to make DSLR sensors responds to wavelengths from 190 to 1,000 nm. This range covers a large portion of the UV spectra, the entire visible light spectra, and a significant portion of the near-IR spectra [78].

2.2.2.5 UV Sources

UV sources include LEDs, mercury lamps, and sunlight.

2.2.2.6 UV LEDs

UV LEDs operate on the same principal as visible-light LEDs but have slightly different mixes of the gallium, indium, and aluminum in the diode. They require more energy than visible-light LEDs. LEDs for UV production are available in various packages: dual in-line package (known as DIP), surface-mounted device (known as SMD), and chip on board (known as COB).

2.2.2.7 Traditional UV Lamps

Traditional UV lamps take the form of electric-discharge lamps, which are lighting devices consisting of a transparent container within which a gas is energized by an applied voltage and thereby made to glow. Mercury is often used also in fluorescent lamps and some UV lamps. Helium in amber glass glows gold, blue light in yellow glass shows green, and combinations of gases give white light [79, 80].

2.2.2.8 UV in Biometrics

UV imagery is not as prevalent as other methods, but it is still an option for standoff biometric detection systems. The two areas that are garnering the most research are: (1) standoff analysis of residual biometric markers (fingerprints) and (2) imaging to leverage melanin face pigmentation (MFP).

2.2.2.9 ID of Residual Biometrics

Long-wave UV reflection imaging has been reported as a simple, safe, and noninvasive technique that significantly aids in the visualization of cyanoacrylate-developed latent fingermarks. Information is available in King et al. [81] and Stodddart et al. [82].

2.2.2.10 Facial Recognition Using UV Imager

UV imagery has been suggested as a means to perform MFP ID to extend classical face biometrics. Melanin pigmentation results from sun-damaged cells that occur as a revealed and/or unrevealed pattern on human skin. Most MFP can be found on the faces of some people when illuminated with UV radiation. Samartzidis et al. [83] proved the relevance of leveraging this body response feature for biometrics via 91 multiethnic subjects in both the visible and the UV spectrum and extracted MFP features from the UV images. They observed a significant amplification of performance where traditional face recognition in the visible spectrum is extended with MFP from UV images. In addition, a patent has been issued on a system and method for biometric ID of a target individual based on a query containing UV image data of the target individual [84].

2.2.2.11 Commercial Systems

There are no systems available that are marketed exclusively as UV biometric standoff analysis systems, but Sirchie (based out of Youngsville, NC) sells a number of UV camera and analysis systems that are marketed for forensic use.

2.2.3 Terahertz

Terahertz radiation refers to EM waves within a frequency range that, depending on the application, can range from approximately 0.1 to 10 THz (corresponding to wavelengths from 30 µm to 3 mm). This spectral region allows inspections of targets with photons that have lower energies than X-rays and UV light, minimizing the risk of damaging delicate samples. Moreover, many materials that are opaque to visible light are transparent to terahertz waves, enabling the visualization of objects or layers beneath surfaces.

Generating and detecting terahertz waves has historically been challenging due to the so-called "terahertz gap." This gap is a frequency range where traditional electronic and optical devices are less effective. However, advancements such as photoconductive antennas, quantum cascade lasers, and nonlinear optical crystals have enabled terahertz-wave generation and detection. In photoconductive antennas, for instance, ultrafast laser pulses excite carriers in a semiconductor, which, in turn, emit terahertz radiation when in the presence of an applied electric field (E-field).

Detection methods range from direct detection, such as using bolometers (a device used for measuring radiant heat via a material having a known temperature-dependent electrical resistance) or pyroelectric detectors. Pyroelectric detectors leverage changing the temperature of crystalline lithium tantalate to change its polarization. When the crystal is heated and cooled, a surface charge with opposite polarity is created. These charges equalize through the visible sparks between the top and bottom surfaces. Indirect detection includes coherent detection where the phase and amplitude of the terahertz waves are measured, allowing for a more complex analysis of the wavefront.

Terahertz-imaging systems can be broadly categorized into time- and frequency-domain systems. Time-domain systems measure the time it takes for a terahertz pulse to travel through a sample, yielding both amplitude and phase information, which can be used to construct a 3-D image. Frequency-domain systems use continuous-wave terahertz radiation at different frequencies to obtain spectral information about the sample.

One of the significant benefits of terahertz imaging is its ability to perform spectroscopic analysis. Many compounds have characteristic absorption features in the terahertz range, making it possible to visualize internal structures and identify the materials based on their spectral fingerprints. Examples of this include compounds on/in human skin and can include unique items on the actual person that can be used for biometric ID.

For biological imaging, terahertz radiation has demonstrated potential for detecting skin cancer (cancerous tissues have different terahertz signatures than healthy tissue). Terahertz radiation has also shown promise in imaging tooth decay and skin burns without the need for harmful ionizing radiation.

Security screenings have the potential for significant enhancement by employing terahertz imaging. Terahertz imaging can detect concealed weapons and explosives under clothing without the health risks and specialized equipment associated with X-rays. Furthermore, terahertz systems can differentiate between substances based on their spectral signatures, enabling the detection of illegal drugs and hazardous chemicals.

2.2.3.1 Challenges

Deployment of terahertz imaging also faces several challenges. The technology typically requires sophisticated and expensive equipment that is not widely accessible. Additionally, the atmosphere absorbs terahertz waves quite strongly (especially in high-humidity environments [the presence of atmospheric water]), which can limit the range of applications in open environments (many laboratory terahertz experiments and measurements are done in a dry nitrogen purge to eliminate this effect).

For terahertz imaging to become more mainstream, further developments in compact, cost-effective terahertz sources and detectors are necessary. This also needs to include the development of miniaturized arrays of the sources and detectors so that large areas of interest can be illuminated and inspected. There is also ongoing research into the development of novel materials with tailored terahertz properties, such as metamaterials and photonic crystals, which could vastly improve the control and manipulation of terahertz waves.

2.2.3.2 Terahertz Uses for Biometrics

Cong et al. [85] point out that, over the past 6 years, the application of terahertz imaging in tumor tissue has made encouraging progress. This type of imaging leverages changes in the chemicals within the initial layers of the skin. However, due to the strong absorption of terahertz by water, along with the large size, high cost, and differing degrees of sensitivity of terahertz devices, it is still difficult for it to be widely used in clinical practice and its use for standoff biometrics is likely still some time away.

Qi et al. [86] also examined this technology via a terahertz-imaging technology based on a narrow-band quantum cascade laser at 2.8 THz for human skin pathology detection with diffraction limited spatial resolution. They used terahertz imaging on three different groups of unstained human skin samples (benign naevus, dysplastic naevus, and melanoma) compared to the corresponding traditional histopathologic stained images. The primary constraint of this effort was that the inspection target was a dehydrated piece of human skin and was 50 μm (approximately one-half wavelength of the terahertz frequency used), meaning there are still a number of practical challenges that need to be overcome before it can be deployed as an in-field medical or, in the interest of this report, a biometric scanner (Figure 2-3). The setup does the job but, again, is not practical for in-field imaging. The results did show that the terahertz images from the different skin samples were well correlated with the histological findings and suggest that terahertz imaging could provide a feasible imaging modality for skin cancer detection that is beyond visible light (and, by extension, a means to identify hidden, trackable features for biometric inspections).

More recent work by Qi et al. 2024 [87] compared the ability to differentiate between different skin pathologies using high-resolution terahertz imaging. Both phase and amplitude components of the signal were used to discriminate between several different lesion types successfully. The scan field used was comparatively small compared to what would be needed to field a successful terahertz biometric scanner (on the order of 50×40 mm). It is possible that this system could be used to address inspections around known biological landmarks (such as an eye) and inspect small sections around them, but this limits the technology and simultaneously renders it easier to spoof or overcome.

Terahertz imaging has also been proposed as a way to extract biometric information from other parts of the body, such as fingerprints. High-spatial-resolution terahertz imaging has been used for fingerprint biometrics. Terahertz radiation can penetrate the outer, drier layers of the skin, allowing subsurface imaging for advanced security biometrics or for diagnosis of diabetic diseases [88]. Due to the short wavelengths and significant penetration depth, terahertz imaging

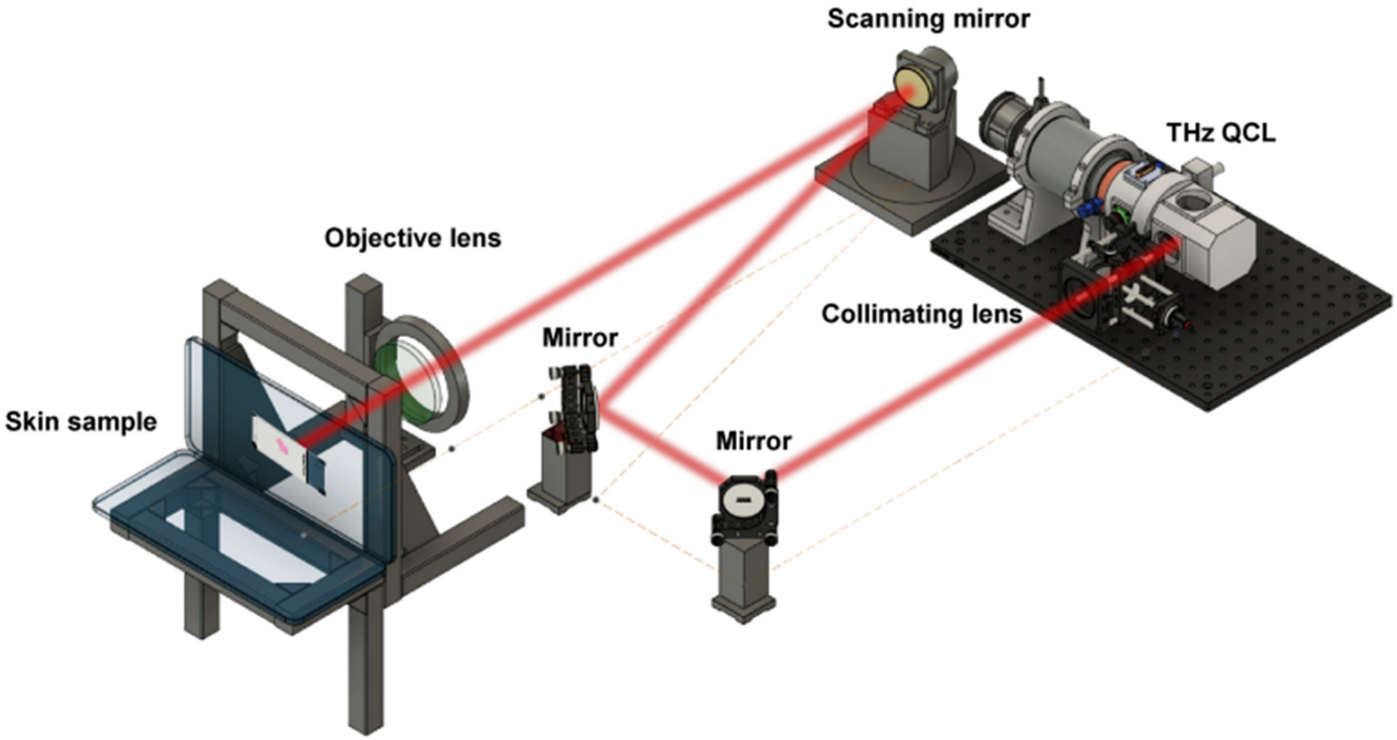

Figure 2-3. Imaging Setup Used to Inspect for Cancers in Human Skin *(Source: Qi et al. 2024 [87])*.

allows noninvasive probing of the finger skin and can provide images of the underlying tissue traits with high spatial resolution. Additionally, imaging is possible when through thin, nonconductive materials associated with protective gear (e.g., nitrile gloves), potentially extending biometric options in challenging environments.

More esoteric uses have been demonstrated. For example, Freer et al. [89] show how it is possible to use terahertz imaging to facilitate human biometrics, although practical standoff biometric systems based on this technology are not immediately feasible.

2.2.3.3 Materials

Two areas of technology that are being pursued are: (1) terahertz sources and (2) detectors.

2.2.3.4 Sources

Seddon et al. [90] provide an overview of terahertz-source technologies. Due to a range of technological challenges in the generation and detection of terahertz radiation, fewer technologically mature solutions are available than for other portions of the EM spectrum. There have been several proposed technological solutions for generation of terahertz radiation. These include:

- Schottky Diode Multiplier Chains
- Complementary Metal-Oxide Semiconductor (CMOS)-Based Transistors
- Gunn Diodes
- Impact Ionization Avalanche Transmit-Time (known as IMPATT) Diodes
- Quantum Cascade Lasers
- Photoconductive Switches
- High-Speed Photodiodes

Key terahertz applications such as spectroscopy, imaging, metrology, and communications impose differing sets of requirements on the terahertz source and detector. For example, terahertz

spectroscopy and metrology require a wide-bandwidth tunable source with a spectral linewidth narrow enough to resolve spectral features of interest and with a power level high enough to pass through a sample under test and be detected.

For communications and imaging applications, there are less stringent requirements on frequency tuneability of the source but stronger emphasis on the output power level. Of the terahertz sources discussed previously, coherent photonics-based sources can fulfill many of the requirements of tuneability and frequency stability, along with high spectral resolution. One of the areas where photomixing sources underperform is output power level, when compared to electronic room-temperature sources, such as Schottky diodes and CMOS sources that generate milliwatt-level power at 300 GHz.

The most widely developed photonics-based source, particularly for time-domain spectroscopy (TDS), is based on low-temperature-grown gallium arsenide (LT-GaAs), which makes use of femtosecond pulses from a mode-locked laser to generate ultrafast terahertz pulses. TDS, however, does have limitations arising from the costs of the ultrafast pulsed-laser drive systems, which operate at ~800 nm. The spectral resolution achievable is also limited primarily by the physical length of the optical delay line. TDS systems-based on 1,550-nm pulsed fiber lasers have also been developed as a commercial solution making use of low temperature indium-gallium-arsenic (LT-InGaAs) and indium-aluminum-arsenic (InAlAs)/indium-gallium-arsenic (InGaAs) heterostructures.

Continuous-wave generation of terahertz radiation can also be achieved by difference frequency photomixing in LT-GaAs and LT-InGaAs or in high-speed InGaAs photodiodes. In the case of LT-InGaAs and photodiodes, the operating wavelength is within the 1,550-nm telecommunications wavelength band. Operation in the telecommunications band has the advantage of the availability of a very wide selection of low-cost, off-the-shelf photonic components and low-loss transmission through standard optical fibers.

2.2.3.5 Detectors

An editorial article in *Frontiers in Physics* [91] provides the most recent overview of terahertz detector technology. Terahertz quantum-well photodetectors have high sensitivity and fast response. Quantum-well photodetectors have been integrated with LEDs to upconvert terahertz radiation into near-IR emission for broadband up-conversion terahertz detection and pixel-less imaging. Theoretical studies have been performed on the neon glow discharge characteristics and the interaction between the discharge plasma with terahertz waves to develop low-cost, real-time operation and user-friendly detectors. Photoactive materials are vital for real-time terahertz bolometers. Thin films such as niobium nitride thin film coupled with a radio-frequency choke-enhanced dipole antenna have been examined. Photoconductive antennas are widely used detectors in TDS systems. Layered molybdenum disulfide crystals are promising materials for novel optoelectronic devices.

Other work has examined field-effect transistors coupled to integrated antennas (terahertz field-effect transistors) as photodetectors for terahertz radiation [92]. Antimony-telluride thin-film metal–semiconductor-metal structure with a subwavelength gap has also been examined to create an EM-induced potential well within the semiconductor by utilizing the antisymmetric E-field of terahertz radiation capable of large-area terahertz detection [93].

SECTION 03 APPLICATIONS

Federal agencies in the United States and around the world (including law enforcement and security operations) use biometric technologies for many different purposes, such as identity verification and investigative leads, as well as facial recognition for immigration, travel, traveler inspection, and border security. Biometrics is also used for employee access to buildings or networks. In the United States, agencies such as the DHS and NIST conduct research and testing to support the development of biometrics, evaluate technology capabilities, identify gaps for further research, and inform standards development. Other countries are also using biometric systems in the field for purposes of suppression, detainment, and determent of criminal activities.

3.1 BIOMETRIC APPLICATIONS IN DOMESTIC/ HOMELAND ENVIRONMENTS

The U.S. government has implemented numerous biometrics programs across many agencies and is continuing to increase development and implementation of different programs to address new and growing needs (Table 3-1). By and large, the majority of U.S. biometrics programs are implemented for homeland security purposes, with travel and border services and criminal and terrorist investigations being the most prevalent use cases. Fingerprint (and palmprint) and facial recognition are the most common modalities used for biometric systems operated by the government, but there are also established systems for vascular pattern, iris, and voice recognition.

In addition to the many biometric systems operated at the government level, there are several programs that have been developed and implemented at the state and local level. For example, the state of Michigan has implemented the Statewide Network of Agency Photos (known as SNAP) Unit program, which "allows for the completion of digital lineups that meet the best practice standards for eyewitness ID and facial recognition (FR)" [94]. Additionally, the Los Angeles County Regional Identification System (known as LACRIS) is a mobile application that allows authorized agencies and personnel working for Los Angeles County to make positive IDs of subjects in the field [95]. The system is connected to the county's Multimodal Biometric Identification System (known as MBIS) and can perform searches of the California Department of Justice's fingerprint repository and the FBI's Repository of Individuals with Special Circumstances (known as RISC) database.

There have also been several commercial biometrics systems developed and either implemented or integrated into local law enforcement and federal security activities. One of the companies offering services to local and federal law enforcement is Clearview AI. Clearview AI has been marketing FRT services to local law enforcement agencies [96] and has also been reportedly used by several different federal agencies [18]. Clearview AI's database reportedly holds over 50 billion images that have all been sourced from publicly available materials [97]. Another company, CLEAR, is currently providing biometrics services to U.S. domestic travelers at

Table 3-1. A List of Some of the Biometric Systems Used by U.S. Government Agencies

System	Agency Responsible	Purpose	Modalities
Automated Biometric Identification System (IDENT)	DHS	Provides biometric data to cooperating agencies for national security, law enforcement, immigration, intelligence, and other related functions [98].	Fingerprint, Iris, and Facial Recognition
Homeland Advanced Recognition Technology (HART)	DHS	Is intended to replace the legacy IDENT system as DHS's premiere system for storage and processing of biometric and associated biographic information. The system's development is still in planning phase [99].	To Be Determined
Automated Biometric Identification System (ABIS)	U.S. Department of Defense (DoD)	Supports the DoD with storing, matching, and sharing of collected biometric data primarily obtained during Operation Iraqi Freedom and Operation Enduring Freedom [100].	Fingerprint, Palmprint, Iris, and Facial Recognition
Next-Generation Identification (NGI)	FBI	Serves as the FBI's new electronic repository for criminal information. It is composed of and compatible with multiple individual systems and databases [101].	Fingerprint, Palmprint, Facial Recognition, and Iris
Facial Analysis, Comparison, and Evaluation Services (FACE)	FBI	Serves as the FBI's facial recognition search tool and repository for all tenprint transactions [102].	Facial Recognition
Second-Generation CAT-2	TSA	Is used by transportation security officers to verify the authenticity of a traveler's ID credentials, flight status, and vetting status [103].	Facial Recognition
Traveler Verification System (TVS)	Customs and Border Protection (CBP) (DHS)	Serves as a biometric entry/exit system to record arrivals and departures to and from the United States, operated by CBP. The exit system has faced development and implementation delays [104].	Facial Recognition
Real-Time Automated Personnel Identification System (RAPIDS)	DoD	Serves as the DoD's credentialing system for individuals. It is paired with the Defense Enrollment Eligibility Reporting System (known as DEERS) [105].	Facial Recognition and Fingerprint
Integrated Biometric System (IBS)	U.S. Department of State	Serves as a computerized face recognition system used by the U.S. Department of State for issuing visas and passports [106].	Facial Recognition

airports as part of airport security [107]. CLEAR Plus is a member-based service that provides travelers with an option to register their biometric information with the company's service to expedite their time in TSA security lines. The service is available in 58 airports, as well as many other venues, such as arenas and stadiums where event security may be used.

Implementing biometrics systems across the United States is a difficult undertaking, and federal agencies face several hurdles to successfully implementing robust systems while ensuring the accuracy, fairness, and security of those systems. As an example, the GAO (in 2016) identified a gap in the implementation of a congressionally mandated entry-exit system for travelers in the United States [28]. In the report, the GAO stated that the DHS faced significant challenges in developing a biometric exit system and reporting reliable overstay data for which it had not fulfilled statutory requirements. Reportedly (in January 2016), the DHS was planning efforts to address requirements but had not yet met them. The GAO recommended that the DHS establish time frames and milestones for a biometric air-exit evaluation framework to guide its assessment efforts. The DHS had also implemented several projects to test and evaluate biometric air-exit technologies, such as "testing a handheld mobile device to collect biographic and biometric exit data from randomly selected, foreign national travelers at 10 selected airports" [28]. The GAO stated that, despite taking action to strengthen its overstay data, there were still challenges to reporting reliable overstay data and weaknesses in departure data. One of the issues reported to hinder the execution of exit systems was infrastructure limitations. "CBP noted that U.S. airports generally do not have outbound, designated, secure areas for exiting travelers where biometric information could be captured by U.S. immigration officers" [29].

Considerations for privacy, data security, user training, and robust research are also important to implementing new biometric systems in the United States. In one GAO report on FRT, 14 of 42 agencies surveyed reported using nonfederal systems to support activities [108]. Thirteen of these agencies were found to not be conducting audits of employee use on these systems, nor tracking potential data and privacy risks. Privacy risks around biometric data include data breaches, mishandling of information, abuse of access, and more. Protecting individuals' biometric data is not only important for security reasons, as ensuring data security and privacy can improve public opinion on the government's use and handling of biometric data.

The accuracy of biometric data and the processes that are conducted to handle and act upon biometric data are also of great concern. Research on biometric ID technologies, particularly facial recognition, has shown improvements in accuracy [44]. However, there are still gaps in understanding real-world performance due to factors like lack of demographic diversity in training datasets. While laboratory testing has studied differences, real-world performance has been less extensively studied due to challenges in acquiring meaningful samples across demographic groups. Additionally, not all agencies who depend upon biometric systems for criminal investigations and related activities are providing necessary training [109]. Training topics of importance include "how facial recognition technology works, what photos are appropriate to use, and how to interpret results" [109]. The GAO found in one research effort, that "agencies with available data reported conducting about 60,000 searches—nearly all of the roughly 63,000 total searches—without requiring that staff take training" [109]. Agencies acknowledge that this training is necessary, but it has yet to be implemented in some cases. These gaps represent risks to biometric systems and to the privacy of people's data.

The pipeline for implementing new biometric systems is long, from fundamental research of emerging technology needs; to the development of field-ready systems; to the adherence to standards and regulations for biometric systems; and, finally, to the training and rollout of systems in the field. Upholding the privacy and security of individuals' data, while also addressing ever-evolving national security needs, puts strain on the timelines for agencies to bring the latest in research and development into the field. Agencies conducting

research into the needs for new and improved systems, including the DoD and DHS, are leading the effort to overcome these hurdles. Meanwhile, commercial entities, that have historically filled the gaps for hardware needs, are beginning to fill the gaps for software and security needs.

3.2 FOREIGN GOVERNMENTS IMPLEMENTING BIOMETRICS

On the global scale, governments are implementing biometric systems at a rapidly growing rate. Biometric systems are being used around the world for everything from border control and visa applications; to health tracking and medical records; to providing government services such as voter registration, banking services, licensing, and more [110]. Identifying how other countries use biometrics can reveal where systems are being implemented that outpace U.S. systems.

3.2.1 China

China's history with biometric ID dates back to ancient times, when the first fingerprints were used by government officials to authenticate documents. However, China is more widely known for the biometric systems it began implementing in the 1990s. China first implemented a state security program in 1998, with the Golden Shield Project. Since then, several more surveillance programs have been developed, including the Sharp Eyes Project and the Strike Hard Against Violent Terrorism program. "After 2016, [China] became the world's largest surveillance market, with government purchases accounting for 60% of the nearly trillion-dollar Chinese market. According to analysts, of the nearly one billion cameras in the world today, more than half are Chinese" [23]. Many of China's security needs are being met by its tech firms, which are some of the largest in the world [20]. These firms are now branching out beyond the domestic market and exporting technologies previously developed for state security initiatives around the globe.

China's goals for biometric system development are twofold. First, China aims to design a system to maximize information about individuals' identity, activities, and social connections to maintain party rule [111]. Second, China aims to extend its technology and security leadership globally [20]. It is working to accomplish the first of these aims by investing heavily in both research and development of new and increasingly comprehensive systems. Not only does China have some of the best facial recognition systems in the world, but it is also working to add capabilities such as identifying race, gender, and types of clothing being worn by passersby [111]. Additionally, China is developing capabilities to match recorded data across systems and build personal profiles of civilians and collecting biometric samples from all residents, indiscriminately. The success of these efforts is reportedly hindered by the lack of analytical capabilities and data centralization. China is even reaching out to foreign universities to fund additional research for state surveillance, including universities in the United States [112].

China's push to extend its power in the security market has had a wide reach, particularly in the global south. Chinese companies have reportedly supplied surveillance technologies to 63 countries and utilized multinational cooperative organizations to promote its technologies in areas such as Africa, Brazil, and India [20]. Due to these efforts, "the use of Chinese surveillance technologies in South Africa has risen largely in tandem with police-to-police training and cooperation" [20]. China's drive to spread the use of state surveillance technology is due in part to its desire to legitimize its own state surveillance programs, which have faced criticism from Western countries. The U.S. government has taken steps previously to abate the spread of Chinese surveillance, including issuing bans on the sale or use of technologies from Chinese companies [113] and banning the sale of private data to China and Russia [114], as well as warning the public about Chinese spying and threats to privacy [115].

3.2.2 Israel

When the Israel-Palestine armed conflict began in October 2023, the Israeli Defense Forces (IDF) started using a facial recognition program to identify Israelis taken hostage by Hamas. Soon after, when the IDF ordered residents to begin evacuating the Gaza strip, Palestinians were picked out of crowds by IDF officials for questioning [27]. The IDF was using its new program indiscriminately on all fleeing Palestinians to identify any individuals accused of having ties to or involvement with Hamas.

However, this was not Israel's first use of widespread biometrics on unwitting citizens. In 2021, the *Washington Post* reported on Israel's Red Wolf program, which allowed IDF officers to perform facial recognition scans on occupants of the West Bank using high-quality scanners, CCTV, and phone cameras [116]. The scans were reportedly stored as part of an extensive database containing West Bank residents' information (from pictures, to family history, to education), with each resident assigned a security score. The accompanying Blue Wolf phone application displayed a green, yellow, or red indicator when officers scanned an individual (whether up close or from a distance), allowing them to target those individuals who had been flagged by the database. The program and its subsequent counterparts have been developed for counterterrorism but have been used for a wider range of purposes. Reportedly, Israeli officers were incentivized by rankings in the app to score more points by capturing more data on Palestinian residents [117].

The program used in Gaza was developed by Corsight, a Tel Aviv-based company that specializes in facial recognition [27, 118]. According to reports, the technology requires at least 50% of the face to be uncovered and performs poorly with low-quality images (despite claims from the company's chief executive officer). The Israeli officers who spoke with the *New York Times* claimed that officials were depending on help from Google Photos algorithm(s) to help make positive IDs, stating the program was superior at matching faces. The camera hardware used for the CCTV system has historically been provided by foreign companies as well, including one Chinese and one Dutch company [119].

Israel's widespread use of biometrics within its borders has allowed it to develop, implement, and adapt new systems quickly in recent years. By depending on established third-party hardware and software and, in part, due to a lack of privacy requirements and rigorous standards, the IDF has been able to construct new systems much more quickly within its borders. Additionally, the success of these programs is spurring the company creators into global expansion. Corsight has established offices in the United Kingdom, United States, Portugal, India, Brazil, Australia, and more [120]. Oosto, formerly called AnyVision, has also expanded its operations around the globe and now even has a partnership with the CyLab Biometric Research Center at Carnegie Melon University [121].

3.2.3 Others

Russia is considered, alongside China, to have developed some of the highest-performing facial recognition algorithms in the world. Several of the top-ten tested algorithms listed by NIST have been produced by Russian companies [42]. One of the reasons for this is that Russia has elected not to rely upon Western developers for its proprietary data (though it does use Western hardware) [122]. Russia's largest biometric surveillance system, one of the largest in the world, is powered by the software developments of Russian-based NtechLab—who even won a contest hosted by IARPA in 2017. The strength of Russia's biometric software has helped to spurn the administration of even more biometric surveillance efforts, with the Russian government now requiring banks and state institutions to register clients' biometrics [123], expanding its collection of biometrics to

all foreign visitors [124] and encouraging private businesses to require biometric ID as part of the payment process for goods and services [125]. All of these developments are part of Russia's desire to expand its surveillance state within the country. "In November last year, the Russian Ministry of Digital Development said that, by 2030, the number of CCTV cameras in the country will grow to 5 million and all of them will be connected to AI systems capable of processing the video stream" [126].

The United Kingdom uses biometrics systems for many of the same purposes as the United States and other countries—security, identify verification, and immigration. It has been working to expand its biometric services, establishing the Electronic Travel Authorization program in 2023, which collects biometric data for visa and immigration purposes [127]. The United Kingdom has also started using live FRT to help identify members of the public suspected of criminal activity [128]. The implementation of these technologies has been uncertain, and, in several instances, people have been wrongfully arrested for offenses such as shoplifting, leading to several lawsuits [129]. In addition to these struggles, recent measures taken by the parliament may jeopardize the establishment of new standards and requirements for biometrics use by the government and law enforcement [130].

SECTION 04 KEY CONTRIBUTIONS AND IMPACT PLAYERS

The advancement of the state of the art in biometrics is a joint effort across government, academia, and commercial and public entities. Some of these organizations making a significant impact on the industry are discussed in this section.

4.1 DHS

The DHS is one of the U.S. government's leading agencies in researching, developing, implementing, and maintaining government biometric systems. The DHS operates the Biometric and Identity Technology Center, a test facility in Maryland, where it hosts testing events such as the Biometric Technology Rally [131]. Since 2020, the Rally has focused testing events on improving facial recognition for transportation biometric services, including addressing acquisition and matching systems with face masks [132]. In 2022, the focus of the Rally was on high-throughput systems of groups ranging from 2 to 12 people and standoff detection at distances of several feet. The results of the testing showed that the tested systems had "fast transaction times," maintained privacy for nonusers, were unaffected by group size, expressed some errors in acquiring quality images, and faltered with some demographic differentials. The DHS's biometric technology rallies provide a means to bridge the gap between research-level systems that demonstrate state-of-the-art technology and actual in-the-field technologies in real-world environments. In 2024, the DHS announced, in partnership with the TSA, NIST, and Homeland Security Investigations Forensic Laboratory, an event called the Remote Identity Validation Technology Demonstration to "challenge industry to deliver secure, accurate, and easy-to-use remote identity validation technologies" [133]. The primary aim for this testing is to improve anticounterfeit and antispoofing technologies in biometrics, including a focus on liveness detection in identity verification.

4.2 NIST

NIST plays an important role in transitioning biometric technologies from the research arena into real-world application by studying and defining the requirements for new technologies. It has issued standards for fingerprint, face, and iris biometrics, setting the requirements for the quality of data captured, the accuracy of matching and ID technology, and the interoperability of biometric systems [134]. In support of interagency biometric data sharing, NIST tests and grades systems through multiple interoperability challenge programs (listed in Table 4-1). It is also involved in addressing future challenges for biometrics and is currently researching methods and standards for liveness detection in antispoofing efforts.

4.3 IARPA

IARPA is currently leading the foremost effort in addressing better biometric ID at standoff distances through its BRIAR program [135]. The program, which began in 2021, is establishing systems for multimodal biometric detection at long distances and high angles through the

Table 4-1. NIST Performance and Interoperability Testing for Different Modalities *(Source: NIST [134])*

Modality	Testing Program
Fingerprint	Fingerprint Minutiae Exchange Testing Program (known as MINEX)
Iris	Iris Exchange (IREX) Testing Program: IREX I and IREX III
FRT	Face Recognition Vendor Testing Program (known as FRVT)
Voice and Language	Speaker and Language Recognition Evaluation Testing Program (known as SLRE)

advancement of biometric modalities such as gait and body recognition, the development of better and more robust training data sets for AI/ML development, and the generation of new techniques to compensate for image blur and turbulence, as well as several other advancements. The program has included contributions from companies, universities, and research partners across the United States and the globe. Several of these developments are in Section 2 of this report, particularly the FarSight system, but many of the developments were made possible by the establishment of new training data.

Oak Ridge National Laboratory assisted the BRIAR program with the development of the BRIAR dataset, a "one-of-a-kind dataset comprising still images and videos of subjects from multiple ranges and elevations across two sets of clothing" [68]. The BRIAR dataset is unique in that it collects images and videos in both constrained and unconstrained environments, thereby providing a better framework for improving algorithms for whole-body detection, as well as person reidentification (when subjects are reidentified across camera views and even across biometric detection systems).

4.4 MICHIGAN STATE UNIVERSITY (MSU)

MSU's Biometrics Research Group, led by Dr. Anil Jain, has been producing some of the foremost research in the field of biometric detection and has been heavily involved in projects across all biometric modalities [136]. MSU partnered with researches at several other universities in developing the FarSight system previously discussed in Section 2 and have also developed new technologies in fingerprint, palmprint, iris, face, latent fingerprint, and whole-body biometrics [137]. MSU is also heavily involved in research on adversarial threats to biometric technologies and is leading research in detecting spoofing in biometric recognition.

4.5 WEST VIRGINIA UNIVERSITY (WVU)

WVU's Biometrics and Identification Innovation Center was named a national leader and university partner for the FBI's Biometric Center of Excellence in 2015 [138], which was first established in 2010. The partnership continues today, and WVU has shifted its biometric research into the university's Vision and Learning Group. WVU's biometrics research areas include facial recognition, person reidentification, activity recognition, object detection, video tracking, and 3-D object modeling [139].

4.6 DHS CENTERS OF EXCELLENCE

The DHS's Centers of Excellence are a collection of universities, academic institutions, research institutions, and industry partners performing leading research for the DHS's Science and Technology Office of University Programs [140]. Many of the university partners operating centers are contributing to the agency's biometrics research, including the University of Arizona, University of Rutgers, Purdue University, the University of Nebraska, and many others. Some of the research being conducted by Centers of

Excellence partners includes improving facial recognition capabilities with mobile phones [141], improved operational environment facial recognition [142], and observing human behavioral patterns to identify threats [143].

4.7 NATIONAL SCIENCE FOUNDATION'S CENTER FOR IDENTIFICATION TECHNOLOGY RESEARCH

The National Science Foundation's Center for Identification Technology Research is a university partnership program working to address challenges in biometric recognition and identity security [144]. Its university partners include Clarkson University, WVU, MSU, and the University at Buffalo.

4.8 ACCENTURE FEDERAL SERVICES

Accenture Federal Services, a subsidiary of Accenture LLP, developed a dataset of both static images and video feed called Accenture Multimodality 1 (known as ACC-MM1) for training for large-scale, multimodal biometric recognition [145]. The dataset fills a gap in AI/ML for standoff detection, providing researchers with a robust set of training images to develop better recognition algorithms for camera views from multiple distances and angles. The dataset includes over 300 hours of footage of 227 participating individuals, with biometric data collected for several modalities.

4.9 SOME INDUSTRY BIOMETRIC TECHNOLOGY PROVIDERS

A large number of the biometric detection systems on the market today are provided by major internation technology companies, who have been serving government and other industry customers for decades. The DoD, TSA, CBP, and other U.S. agencies depend on the COTS systems provided by these major suppliers for their in-the-field operations [146, 147].

Fujitsu Ltd. is a Japan-based multinational information and communications technology equipment and services corporation. Fujitsu provides biometric hardware such as palmprint and fingerprint scanners, as well as multifactor authentication services [148].

NEC Corporation "is the global leader in the field of biometric authentication, bringing the best of their class in the world, providing the most suitable solutions to customers' needs in six areas—face recognition, iris recognition, fingerprint/palmprint recognition, voice recognition, and ear acoustic authentication" [149].

3M Cogent, a subsidiary of 3M Corporation, provides facial ID management solutions, mobile ID solutions, and biometric enrollment solutions [150].

Parsons Corporation provides several identity solution systems to government agencies in the national security field and offers comprehensive identity management services [151].

HID Global provides biometric services and systems for commercial and government partners [152]. HID's biometric services cover facial recognition, finger and palmprint recognition, mobile biometrics, and backend software for enrollment, matching, and identity management.

Leidos has been a leader in biometrics-based ID and credentialing missions providing large-scale systems integration, design and development of biometric solutions, and technical evaluations to government and industry [153].

This Page Intentionally Left Blank

SECTION 05 FUTURE DEVELOPMENTS AND PROJECTIONS

When predicting the future of biometric recognition technology, it can be quite difficult to tell which modalities are going to grab the spotlight or what developments may occur in the field in the next few years. However, one prediction can be made—biometric technology appears to be a quickly growing market, meaning there is no shortage of money to be made in the buying, selling, and further research and development of the biometric scanning technology and algorithms/software used to run the systems [147]. Reputable predictions, such as: "IMARC Group expects the market to reach U.S. $144.0B by 2032, exhibiting a [compound annual] growth rate (CAGR) of 15.2% during 2024–2032" [147]; this is up from the $39B of total value in 2023 and the projected $51.15B in 2024 [147, 154].

Looking more specifically into some of the top modalities such as fingerprint and facial recognition, it appears that fingerprint technology may be on the downslope as face recognition and other modalities take larger market shares [155]. In 2023, companies such as Next Biometrics, who makes fingerprint biometric sensors, and Precise Biometrics, who makes fingerprint verification software, both reported declining earnings and sales [156]. Though outside of fingerprint-related biometrics, it appears that the global facial recognition market that was valued at $5.15B in 2022 is showing a similar trend to the biometric market as a whole and "is expected to grow at a compound annual growth rate (CAGR) of 14.9% from 2023 to 2030"[157].

While FRT may be the biggest star among the modalities individually, biometrics as a whole has been moving toward multimodal options that utilize AI and ML and "this has prompted manufacturers to transition from single-sample verification matchers, such as face, fingerprint, iris, and voice, to a wide range of multimodal, fully automated recognition systems" [147]. This includes biometric modes that can be better utilized from long range, such as gait and vein recognition. When the massive amounts of biometric information are gathered, they can be accurately sifted through using the automated computing power of ML and applied to whatever mode or modes available that allow for ID of the subject or target. This would be the ideal application of what some call multimodal fusion, and it essentially involves being able to identify subjects by their biometrics based on the information that can be obtained while observing them with the biometric scanners (usually in the form of video or pictures). Additionally, continuing advances in AI and ML "will further enhance the capabilities of biometric authentication, making it even more robust and secure" [158].

The future of biometric recognition technology really "lies in multimodal biometrics, which combines multiple biometric identifiers for enhanced accuracy and reliability. This approach combines different biometric modalities, such as facial recognition, fingerprint scanning, and voice recognition, to create a more comprehensive and robust authentication system" [158].

Additionally, according to M. Tayib [159]:

> The future of biometric identification is multimodal biometrics, which combines numerous biometric identifiers for increased accuracy and dependability. This method integrates several biometric techniques to produce a complete and robust identification system. The reliance on biometric authentication will only grow in the future. It's no longer simply about security; it's about providing a seamless personalized customer experience. And, as market statistics show, biometric authentication is becoming more prevalent than before.

There are other reasons, though outside of defense or security-related industries, as to why the biometrics market is growing, and that is mainly due to consumers using biometrics for authentication purposes. For instance, facial recognition has become a popular means of unlocking one's smartphone, along with voice recognition and fingerprint scanning. Biometric information can also be used by companies to easily or quickly confirm a customer's identity, and it has spanned across multiple industries including (but not limited to) healthcare, banking, hospitality, and payment processing. In healthcare, patients' identities can be authenticated using FRT, iris recognition, fingerprint scanning, and voice recognition. Healthcare workers can even use specialized biometric tools to monitor patients and administer medicine remotely. In the field of banking, biometrics is also used to authenticate the identities of customers. These biometric authentication practices are also used in payment processing and transactions [160].

It seems that any market or product that requires identifying the customer or user can benefit from biometric recognition. Since the previous method of authentication involved keeping a taxing number of passwords to be remembered and relayed to others or carrying around ID cards, biometrics appears to have become a good solution to that problem. Not only is biometrics applicable as a good solution for all things authentication and ID, it also includes other "numerous benefits for both individuals and businesses" such as increased security, enhanced user experience, cost-effectiveness, better fraud prevention potential, and increased efficiency [161]. Although there are some major challenges to address within the field of biometrics, like combatting spoofing, deepfakes, and the ethical issues involved with using and holding people's biometric information, it is safe to say that, for now, "the future of biometrics looks promising" [161].

Developing other fringe and underdeveloped biometric modalities (like gait and body shape) and long-range, highly applicable multimodal biometric ID systems may be the key to continuing to push biometrics to its full potential. There is also potential growth in the areas of AI and ML, as their integration continues to drive the future of biometrics (and other technologies) to new heights. Now, every biometric modality has its own advantages and disadvantages that will decide its applicability and effectiveness in the field. Older relied-upon modes like fingerprint ID, have issues with both getting and keeping a good fingerprint sample to use. It has to be applied to someone's fingerprint data that is already collected in order to compare against it for a possible match. Therefore, facial and iris recognition have become some of the modern solutions to fill the gaps left by fingerprints. Unfortunately, they both come with their own limitations as well. For instance, the face must be at least partially visible for facial recognition. For iris recognition, the demands around lighting and visibility of the eye leave even less room for error. In addition, since both modalities are usually captured by camera or video, they can only work from so far away to capture a useful sample for FRT or iris recognition.

Some biometric modalities can, however, work from farther away, without having to get a good-quality, close-up picture of the face or eye. However, these biometric modalities, such as gait and vein recognition, are still relatively new and lack the appropriate development and research to make them entirely viable to use in the field today. Still, all modes are bound to be better or worse in various situations than others, and this is where multimodal fusion biometrics comes into play. Depending on the modes used, they are able to adapt to whatever biometric data can be gathered at the time, and the best mode for the situation at hand is the one that could ideally be able to identify a target. "This is why the multimodal biometric ID system was developed to reliably verify individuals based on several biometric traits. If one method of authentication fails, another can be utilized to identify and verify any person" [162].

The vast amount of biometric data collected can be quickly sorted through and matched thanks to the advances made by way of AI and ML. Creating and developing other modes that work to identify targets better and from farther away, combining these effective modes to use as needed in the field, and continuing to utilize the advancements of current biometric scanning technology and AI and ML will make the most of biometric identification technology. "With each passing year, biometrics pushes the envelope, bringing new applications and improved performance" [163]. If these trends continue to grow as they have, then the future of biometrics does indeed look bright.

This Page Intentionally Left Blank

REFERENCES

1. Shaheed, K., P. Szczuko, M. Kumar, I. Qureshi, Q. Abbas, and I. Ullah. "Deep Learning Techniques for Biometric Security: A Systematic Review of Presentation Attack Detection Systems." *Engineering Applications of Artificial Intelligence*, vol. 129, pp. 107569, https://www.sciencedirect.com/science/article/abs/pii/S0952197623017530, March 2024.
2. Burt, C. "ARM Produces Two New AI Chips for Improved Facial Recognition and Object Detection." *Biometric Update*, https://www.biometricupdate.com/201802/arm-produces-two-new-ai-chips-for-improved-facial-recognition-and-object-detection, 14 February 2018.
3. Burt, C. "Sightcorp Deep Learning Method Improves Biometric Face Detection at Challenging Angles." *Biometric Update*, https://www.biometricupdate.com/201908/sightcorp-deep-learning-method-improves-biometric-face-detection-at-challenging-angles, 9 August 2019.
4. Grand View Research, Inc. "Biometric Technology Market Size, Share & Trends Analysis Report by Component, by Offering, by Authentication Type, by Application, by End-Use, by Region, and Segment Forecasts, 2023–2030." Grand View Research, https://www.grandviewresearch.com/industry-analysis/biometrics-industry, January 2023.
5. Capers, Z. "GetApp's 5th Annual Data Security Report: U.S. Businesses Gaining Ground Amid Ongoing Threats." GetApp, https://www.getapp.com/resources/annual-data-security-report/, 26 September 2023.
6. Schmidt, H. "Hey, Siri, What's Behind the Remarkable Rise of Voice Banking?" International Banker, https://internationalbanker.com/banking/hey-siri-whats-behind-the-remarkable-rise-of-voice-banking/, 4 October 2022.
7. Yurcan, B. "Is Voice-Based Digital Banking Finally Catching on?" The Financial Brand, https://thefinancialbrand.com/news/banking-technology/is-voice-based-digital-banking-finally-catching-on-133644/, 29 March 2022.
8. Fitsak, S. "Goodbye to Passwords: Is Voice Authentication the Future of Fintech Security?" Finextra, https://www.finextra.com/blogposting/24926/goodbye-to-passwords-is-voice-authentication-the-future-of-fintech-security, 20 September 2023.
9. U.S. Senate Committee on Banking, Housing, and Urban Affairs. "Brown Presses Banks on Voice Authentication Services." Washington, DC, https://www.banking.senate.gov/newsroom/majority/brown-presses-banks-voice-authentication-services, 4 May 2023.
10. Wikimedia Foundation, Inc. "List of Largest Banks in the United States." Wikipedia, https://en.wikipedia.org/wiki/List_of_largest_banks_in_the_United_States, 4 July 2024.
11. CB Information Services, Inc. "Capital One Patent Looks to Bring Voice Recognition Technology to Mobile Payments." CBInsights, https://www.cbinsights.com/research/capital-one-patent-voice-recognition-tech-mobile-payments/, 13 October 2020.
12. The PNC Financial Services Group. "PNC Voice Banking." PNC, https://www.pnc.com/en/personal-banking/banking/services/telephone-banking-services.html, accessed on 29 October 2024.
13. Lee, J. "Citigroup's Voice Authentication Option Reaches One Million Customers in Asia." *Biometric Update*, https://www.biometricupdate.com/201703/citigroups-voice-authentication-option-reaches-one-million-customers-in-asia, 20 March 2017.
14. Fight for the Future. "Ban Facial Recognition in Stores." Ban Facial Recognition, https://www.banfacialrecognition.com/stores/#scorecard, accessed on 29 October 2024.
15. CB Information Services, Inc. "Facial Recognition Is Already Here: These Are the 30+ U.S. Companies Testing the Technology." CBInsights, https://www.cbinsights.com/research/facial-recognition-technology-us-corporations/, 5 June 2019.
16. Peterson, H. "Walmart Is Developing a Robot That Identifies Unhappy Shoppers." *Business Insider*, https://www.businessinsider.com/walmart-is-developing-a-robot-that-identifies-unhappy-shoppers-2017-7?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+typepad%2Falleyinsider%2Fsilicon_alley_insider+%28Silicon+Alley+Insider%29, 19 June 2017.
17. Hersey, F. "U.S. Federal Agencies Plan to Increase Facial Recognition Use, GAO Report Says." *Biometric Update*, https://www.biometricupdate.com/202108/us-federal-agencies-plan-to-increase-facial-recognition-use-gao-report-says, 26 August 2021.
18. U.S. Government Accountability Office. "Facial Recognition Technology: Current and Planned Uses by Federal Agencies." GAO, GAO-21-526, https://www.gao.gov/assets/gao-21-526.pdf, August 2021.

REFERENCES, *continued*

19. Transportation Security Administration. "Facial Recognition Technology." TSA, https://www.tsa.gov/news/press/factsheets/facial-recognition-technology, accessed on 29 October 2024.
20. Jili, B. "China's Surveillance Ecosystem and the Global Spread of Its Tools." Atlantic Council, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/chinese-surveillance-ecosystem-and-the-global-spread-of-its-tools/, 17 October 2022.
21. Gates, M. "The Rise of the Surveillance State." *Security Technology*, https://www.asisonline.org/security-management-magazine/monthly-issues/security-technology/archive/2021/june/The-Rise-of-The-Surveillance-State/, 1 June 2021.
22. Wikimedia Foundation Inc. "Social Credit System." Wikipedia, https://en.wikipedia.org/wiki/Social_Credit_System, 19 August 2024.
23. Ka, Y. "A Billion Cameras, Two Billion Eyes: How China's Mass Surveillance Fuses Tech and Citizen Buy-in." Microsoft Start, https://www.msn.com/en-us/news/world/a-billion-cameras-two-billion-eyes-how-chinas-mass-surveillance-fuses-tech-and-citizen-buy-in/ar-BB1ltvbM, 11 April 2024.
24. Swann, B. S., and J. Loudermilk. "Facial Recognition: A Strategic Imperative for National Security." *Biometric Update*, https://www.biometricupdate.com/201906/facial-recognition-a-strategic-imperative-for-national-security, 3 June 2019.
25. Reevell, P. "How Russia Is Using Facial Recognition to Police Its Coronavirus Lockdown." *ABC News*, https://abcnews.go.com/International/russia-facial-recognition-police-coronavirus-lockdown/story?id=70299736, 30 April 2020.
26. Masri, L. "Facial Recognition Is Helping Putin Curb Dissent With the Aid of U.S. Tech." *Reuters*, https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions/, 28 March 2023.
27. Frenkel, S. "Israel Deploys Expansive Facial Recognition Program in Gaza." *The New York Times*, https://www.nytimes.com/2024/03/27/technology/israel-facial-recognition-gaza.html, 27 April 2024.
28. U.S. Government Accountability Office. "Border Security: Actions Needed by DHS to Address Long-Standing Challenges in Planning for a Biometric Exit System." GAO, GAO-16-358T, https://www.gao.gov/assets/gao-16-358t.pdf, 20 January 2016.
29. U.S. Government Accountability Office. "Border Security: DHS Has Made Progress in Planning for a Biometric Air Exit System and Reporting Overstays, but Challenges Remain." GAO, GAO-17-170, https://www.gao.gov/products/gao-17-170#:~:text=Since%20GAO%27s%202013%20report%20on%20the%20Department%20of,development%20and%20implementation%20of%20a%20biometric%20exit%20system, 27 February 2017.
30. Immigration Task Force. "Entry-Exit System: Progress, Challenges, and Outlook." Bipartisan Policy Center, https://bipartisanpolicy.org/download/?file=/wp-content/uploads/2019/03/BPC-Immigration-Entry-Exit-System-Progress-Challenges-and-Outlook.pdf, May 2014.
31. Mayhew, S "History of Biometrics." *Biometric Update*, https://www.biometricupdate.com/201802/history-of-biometrics-2, 1 February 2018.
32. IDology. "What Is Biometric Authentication?" GBG IDology, accessed on 29 October 2024.
33. Fast Company & Inc. "How 9/11 Sparked the Rise of America's Biometric Security Empire." Fast Company, https://www.fastcompany.com/90674661/how-9-11-sparked-the-rise-of-americas-biometrics-security-empire, 10 September 2021.
34. Mariana, M. "Voice Payment in Banking: The New Revolution in Fintech." Data Science Central, https://www.datasciencecentral.com/voice-payment-in-banking-the-new-revolution-in-fintech/, 10 January 2020.
35. Lis, J. "How Big Is the Voice Assistant Market." EMARKETER, https://www.emarketer.com/content/how-big-voice-assistant-market, 15 September 2022.
36. Rank One Computing. "Looking Back at Boston Marathon Bombing: A Decade of Face Recognition Advancement." ROC, https://roc.ai/2023/04/17/looking-back-at-boston-marathon-bombing-a-decade-of-face-recognition-advancement/, 17 April 2023.
37. McCormick, D. "Face Recognition Failed to Find Boston Bombers: Facial Recognition Software Didn't Spot the Boston Marathon Bombers; Armchair 'Investigators' Found Too Much." *IEEE Spectrum*, https://spectrum.ieee.org/face-recognition-failed-to-find-boston-bombers, 23 April 2013.
38. Carlaw S. "Impact on Biometrics of Covid-19." *Biometric Technology Today*, vol. 2020, issue 4, pp. 8–9, https://doi.org/10.1016/S0969-4765(20)30050-3, 2020.
39. Bourlai, T., and S. E. Armistead. "Standoff Biometric Identification: Face Recognition." DSIAC, https://dsiac.org/technical-inquiries/notable/standoff-biometric-identification-face-recognition/, 30 September 2018.

REFERENCES, *continued*

40. Choi, T. "Explainer: Verification vs. Identification Systems." *Biometric Update*, https://www.biometricupdate.com/201206/explainer-verification-vs-identification-systems, 19 January 2022.
41. Clark, M. "Biometric Glossary: Technical Terms and Definitions." Bayometric, https://www.bayometric.com/biometric-glossary-terms-definitions/, accessed on 29 October 2024.
42. Grother, P., M. Ngan, and K. Hanaoka. "Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification." NIST, NISTIR 8238, https://doi.org/10.6028/NIST.IR.8238, 2018.
43. Wikimedia Foundation, Inc. "False Positives and False Negatives." Wikipedia, https://en.wikipedia.org/w/index.php?title=False_positives_and_false_negatives&action=history, 15 July 2024.
44. U.S. Government Accountability Office. "Biometric Identification Technologies: Consideration to Address Information Gaps and Other Stakeholder Concerns." GAO, GAO-24-106293, https://www.gao.gov/assets/gao-24-106293.pdf, April 2024.
45. MacDonald, R. "Behind Fingerprint Biometrics: How It Works and Why It Matters." 1Kosmos, https://www.1kosmos.com/biometric-authentication/behind-fingerprint-biometrics-how-it-works-and-why-it-matters/, 5 April 2024.
46. Wikimedia Foundation, Inc. "Palm Print." Wikipedia, https://en.wikipedia.org/wiki/Palm_print, 14 February 2024.
47. Triggs, R. "How Fingerprint Scanners Work: Optical, Capacitive, and Ultrasonic Explained." *Android Authority*, https://www.androidauthority.com/how-fingerprint-scanners-work-670934/, 11 March 2024.
48. Davies, M. "Fingerprint Scanners 101: Capacitive vs. Optical vs. Ultrasonic." Konsyse, https://www.konsyse.com/articles/fingerprint-scanners-101-capacitive-vs-optical-vs-ultrasonic/, 19 August 2024.
49. Mayhew, S. "Explainer: Vascular Pattern Recognition." *Biometric Update*, https://www.biometricupdate.com/201208/explainer-vascular-pattern-recognition, 22 August 2012.
50. Phys.org. "Japan Researchers Warn of Fingerprint Theft From 'Peace' Sign." *PhysOrg*, https://phys.org/news/2017-01-japan-fingerprint-theft-peace.html, 11 January 2017.
51. Butler, S. "Can a Smartphone Photograph Reveal Your Fingerprints?" *How to Geek*, https://www.howtogeek.com/895809/can-a-smartphone-photograph-reveal-your-fingerprints/, 20 June 2023.
52. Rawate, K. R., and P. A. Tijare. "Human Identification Using IRIS Recognition." Academia, https://www.academia.edu/33109825/Human_Identification_Using_IRIS_Recognition, 19 April 2017.
53. Mohammed, R. T., H. Kaur, B. Alankar, and R. Chauhan. "Recognition of Human Iris for Biometric Identification Using Daugman's Method." *IET Biometrics*, vol. 11, no. 4, pp. 304–13, 14 May 2022.
54. FaceMe. "What Is Facial Recognition: The 2024 Ultimate Guide for Facial Recognition Technology." https://www.cyberlink.com/faceme/insights/articles/204/Facial-Recognition-at-the-Edge-The-Ultimate-Guide#:~:text=The%20technology%20leverages%20proprietary%20AI%20trained%20to%20learn,generated%20template%20with%20existing%20templates%20in%20a%20database., 1 February 2024.
55. Biometrics Institute. "Types of Biometrics—Voice." https://www.biometricsinstitute.org/types-of-biometrics-voice/, accessed on 29 October 2024.
56. Fowler, M., M. McCurry, J. Bramsen, K. Dunsin, and J. Remus. "Standoff Speaker Recognition: Effects of Recording Distance Mismatch on Speaker Recognition System Performance." *Proceedings of Interspeech 2013*, pp. 3713–3716, August 2013.
57. Rahman, A., S. R. Knudsen, D. C. Milonas, D. Fleming, and J. Clements. "Artificial Intelligence (AI) and Machine Learning (ML) in Biometric Data Fusion." HDIAC-BCO-2021-192, Homeland Defense and Security Information Analysis Center, Belcamp, MD, December 2021.
58. Liu, F., R. Ashbaugh, N. Chimitt, N. Hassan, A. Hassani, A. Jaiswal, M. Kim, Z. Mao, C. Perry, Z. Ren, Y. Su, P. Varghaei, K. Wang, X. Zhang, S. Chan, A. Ross, H. Shi, Z. Wang, A. Jain, and X. Liu. "FarSight: A Physics-Driven Whole-Body Biometric System at Large Distance and Altitude." arXiv:2306.17206v2, https://arxiv.org/pdf/2306.17206, 6 September 2023.
59. Y. Zhao, J. K. Jang, G. J. Beals, K. J. McNulty, X. Ji, Y. Okawachi, M. Lipson, and A. L. Gaeta. "All-Optical Frequency Division on-Chip Using a Single Laser." *Nature*, vol. 627, pp 546–552, 11 March 2024.
60. Collins, H. D., D. L. McMakin, T. E. Hall, and R. P. Gribble. "Real-Time Holographic Surveillance System." U.S. Patent 5,455,590 A, 1994.
61. Stanford Technology Ventures Program. "Is the App-Pocalypse Nigh?" STVP, https://stvp.stanford.edu/app-pocalypse-nigh/, 14 April 2016.

REFERENCES, *continued*

62. American City Business Journals. "L3 Communications Buys SafeView." *Silicon Valley Business Journal*, https://www.bizjournals.com/sanjose/stories/2006/03/20/daily20.html, 21 March 2006.

63. Duenas, M. "Leidos Completes Acquisition of L3Harris Technologies' Security Detection and Automation Businesses Creating a Comprehensive, Global Security and Detection Portfolio." Leidos, https://www.leidos.com/insights/leidos-completes-acquisition-l3harris-technologies-security-detection-and-automation, 4 May 2020.

64. Solinski, J. C., N. C. Anheier, Jr., and D. L. McMakin. "Facial Feature Evaluation Based on Eye Location." U.S. Patent 7,809,171, 5 October 2010.

65. Li, Y., D. Zhang, R. Geng, Z. Lu, Z. Wu, Y. Hu, Q. Sun, and Y. Chen. "A High-Resolution Handheld Millimeter-Wave Imaging System With Phase Error Estimation and Compensation." *Communications Engineering*, vol. 3, no. 4, 5 January 2024.

66. Dvorsky, M., S. Y. Sim, D. Motes, A. Shah, T. Watt, M. T. Al Qaseer, and R. Zoughi. "Multistatic Ka-Band (26.5-40 GHz) Millimeter-Wave 3-D Imaging System." *IEEE Transactions on Instrumentation and Measurement*, vol. 72, pp. 1–14, August 2023.

67. Horst, M. J., M. T. Ghasr, and R. Zoughi. "A Compact Microwave Camera Based on Chaotic Excitation Synthetic Aperture Radar (CESAR)." *IEEE Transactions on Antennas and Propagation*, vol. 67, no 6., pp. 4148–4161, June 2019.

68. Baur, C. "Leveraging AI for People Screening: Millimeter Wave Tech and Deep Learning Can Produce Effective, Automated Virtual Searches." SIA, https://www.securityindustry.org/2022/04/07/leveraging-ai-for-people-screening-millimeter-wave-tech-and-deep-learning-can-produce-effective-automated-virtual-searches/, 7 April 2022.

69. Zhang, X., Y. Zhang, Z. Shi, and T. Gu. "mmFER: Millimetre-Wave Radar Based Facial Expression Recognition for Multimedia IoT Applications." *ACM MobiCom '23: Proceedings of the 29th Annual International Conference on Mobile Computing and Networking*, no. 23, pp. 1–15, October 2023.

70. Cornett III, D., J. Brogan, N. Barber, D. Aykac, S. Baird, N. Burchfield, C. Dukes, A. Duncan, R. Ferrell, J. Gooddard, G. Jager, M. Larson, B. Murphy, C. Johnson, I. Shelley, N. Srinivas, B. Stockwell, L. Thompson, M. Yohe, R. Zhang, S. Dolvin, H. J. Santos-Villalobos, and D. S. Bolme. "Expanding Accurate Person Recognition to New Altitude and Ranges: The BRIAR Dataset." arXiv:221.0197v1, https://arxiv.org/pdf/2211.01917, 3 November 2022.

71. Garcia, L. S. L., L. Chang, H. M. Vazquez, Y. Martinez-Diaz, and M. Gonzalez-Mendoza. "A Study on the Performance of Unconstrained Very Low Resolution Face Recognition: Analyzing Current Trends and New Research Directions." *IEEE Access*, vol. 9, https://www.researchgate.net/publication/351650994_A_Study_on_the_Performance_of_Unconstrained_Very_Low_Resolution_Face_Recognition_Analyzing_Current_Trends_and_New_Research_Directions, 17 May 2021.

72. Bos, J. P., and M. C. Roggemann. "Technique for Simulating Anisoplanatic Image Formation Over Long Horizontal Paths." *Optical Engineering*, vol. 51, no. 10, pp. 101704-1–101704-8, https://www.researchgate.net/publication/232174938_Technique_for_simulating_anisoplanatic_image_formation_over_long_horizontal_paths, October 2012.

73. Jain, A. K., K. Nandakumar, and A. Ross. "50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities." *Pattern Recognition Letters*, vol. 79, pp. 80–105, https://biometrics.cse.msu.edu/Publications/GeneralBiometrics/JainNandakumarRoss_50Years_PRL2016.pdf, 12 January 2016.

74. RecFaces. "Gait Recognition System: Deep Dive Into This Future Tech." https://recfaces.com/articles/what-is-gait-recognition#1, accessed on 29 October 2024.

75. Biometrics Institute. "Types of Biometrics—Gait." https://www.biometricsinstitute.org/types-of-biometrics-gait/, accessed on 29 October 2024.

76. Kanazawa, A., M. J. Black, D. W. Jacobs, and J. Malik. "End-to-End Recovery of Human Shape and Pose." arXiv:1712.06584v2, https://arxiv.org/pdf/1712.06584, 23 June 2018.

77. Sundaresan, A., B. Burns, I. Sur, Y. Yao, X. Lin, and S. Kim. "Human Body Model Based ID Using Shape and Pose." arXiv:2312.03227v1, https://arxiv.org/pdf/2312.03227, 6 December 2023.

78. Wikimedia Foundation, Inc. "Ultraviolet Photography." Wikipedia, https://en.wikipedia.org/wiki/Ultraviolet_photography#cite_note-1, accessed on 29 October 2024.

79. Horsham, C., H. Ford, J. Herbert, A. Wall, S. Walpole, and E. Hacker. "Assessing Sunscreen Protection Using UV Photography: Descriptive Study." *JMIR Dermatology*, vol. 4, no. 1, https://derma.jmir.org/2021/1/e24653, 26 May 2021.

REFERENCES, *continued*

80. Gibson, H. L. *Medical Photography: Clinical-Ultraviolet-Infrared*. Kodak Medical Publication no. N-18, pp. 123–130, Rochester, NY: Eastman Kodak Company, 1 January 1973.

81. King, R. S. P., L. W. L. Davis, and D. A. Skros. "The Use of Longwave Reflected UV Imaging for the Enhancement of Cyanoacrylate Developed Fingermarks: A Simple, Safe, and Effective Imaging Tool." *Forensic Science International*, vol. 289, pp. 329–336, August 2018.

82. Stoddart, W., K. Georgiou, P. Deacon, L. Nichols-Drew, and K. J. Farrugia. "Technical Note: A Preliminary Assessment of UV-C Imaging Using the Full Spectrum Imaging System (FSIS-II) for the Detection of Latent Fingermarks." *Forensic Science International*, vol. 355, February 2024.

83. Samartzidis, T., D. Siegmund, M. Goedde, N. Damer, A. Braun, and A. Kuijper. "The Dark Side of the Face: Exploring the Ultraviolet Spectrum for Face Biometrics." IEEE Computer Society: 2018 International Conference on Biometrics (ICB), pp. 182–189, Gold Coast, QLD, Australia, 2018.

84. Rickman, D. M. "System and Method for Biometric Identification Using Ultraviolet (UV) Image Data." U.S. Patent Application Publication no. US 2012/0250948 A1, Raytheon Corporation, 31 March 2011.

85. Cong, M., W. Li, Y. Liu, J. Bi, X. Wang, X. Yang, Z. Zhang, X. Zhang, Y.-N. Zhao, R. Zhao, and J. Qiu. "Biomedical Application of Terahertz Imaging Technology: A Narrative Review." *Quantitative Imaging in Medicine and Surgery*, vol. 13, no. 12, pp. 8768–8786, 1 December 2023.

86. Qi, X., K. Bertling, M. S. Stark, T. Taimre, Y.-C. Kao, Y. L. Lim, S. Han, B. O'Brien, A. Collins, M. Walsh, J. Torniainen, T. Gillespie, B. C. Donose, P. Dean, L. H. Li, E. H. Linfield, A. G. Davies, D. Indjin, H. P. Soyer, and A. D. Rakić. "Terahertz Imaging of Human Skin Pathologies Using Laser Feedback Interferometry With Quantum Cascade Lasers." *Biomedical Optics Express*, vol. 14, issue 14, pp. 1393–1410, 2 March 2023.

87. Qi, X., K. Bertling, J. Torniainen, F. Kong, T. Gillespie, C. Primiero, M. S. Stark, P. Dean, D. Indjin, L. H. Li, E. H. Linfield, A. G. Davies, M. Brünig, T. Mills, C. Rosendahl, H. P. Soyer, and A. D. Rakić. "Terahertz In Vivo Imaging of Human Skin: Toward Detection of Abnormal Skin Pathologies." *APL Bioengineering*, vol. 8, no. 1, pp. 016117, 11 March 2024.

88. Theofanopoulos, P. C., and G. C. Trichopoulos. "A Novel Fingerprint Scanning Method Using Terahertz Imaging." 2018 IEEE International Symposium on Antennas and Propagation & USNC/URSI National Radio Science Meeting, pp. 2463–2464, Boston, MA, 2018.

89. Freer, S., C. Sui, P. Penchev, S. Dimov, A. Gorodetsky, S. M. Hanham, L. M. Grover, and M. Navarro-Cia. "Hyperspectral Terahertz Imaging for Human Bone Biometrics." *Terahertz Emitters, Receivers, and Applications XII*, August 2021.

90. Seddon, J. P., M. Natrella, X. Lin, C. Graham, C. C. Renaud, and A. J. Seeds. "Photodiodes for Terahertz Applications." *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 28, issue 2, March/April 2022.

91. Chen, M., Y. Wang, X. Wang, and L. Li. "Editorial: Advances in Terahertz Detection and Imaging." *Frontiers in Physics*, vol. 10, 6 February 2022.

92. Ludwig, F., A. Generalov, J. Holstein, A. Murros, K. Viisanen, M. Prunnila, and H. G. Roskos. "Terahertz Detection With Graphene FETs: Photothermoelectric and Resistive Self-Mixing Contributions to the Detector Response." *ACS Applied Electronic Materials*, vol. 6, issue 4, pp. 2197–2212, 27 March 2024.

93. Ye, C., and J. Wang. "Low Resistance Large Area Terahertz Detector Based on Antimony Telluride Thin Film." Infrared Physics & Technology, vol. 136, pp. 105001, January 2024.

94. State of Michigan. "Statewide Network of Agency Photos (SNAP) Unit." Michigan State Police, https://www.michigan.gov/msp/divisions/bid/dais/statewide-network-of-agency-photos-snap, accessed on 29 October 2024.

95. LACRIS Tech. "LACRIS Mobile Identification Policy." LACRIS, https://www.lacris.org/LACRIS%20Mobile%20ID%20Policy%20V-1%2001.22.pdf#:~:text=The%20Los%20Angeles%20County%20Regional%20Identification%20System%20%28LACRIS%29,subjects%20who%20cannot%20provide%20identification%20in%20the%20field., January 2022.

96. Hill, K. "The Secretive Company That Might End Privacy as We Know It." *The New York Times*, 18 January 2020.

97. Clearview AI, Inc. "Accelerate Your Investigations." Clearview AI, https://www.clearview.ai/clearview-2-0, accessed on 29 October 2024.

98. U.S. Department of Homeland Security. "DHS/OBIM/PIA-001 Automated Biometric Identification System." DHS, https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system, accessed on 29 October 2024.

99. U.S. Department of Homeland Security. "DHS/OBIM/PIA-004 Homeland Advanced Recognition Technology

REFERENCES, *continued*

System (HART) Increment 1." DHS, https://www.dhs.gov/publication/dhsobimpia-004-homeland-advanced-recognition-technology-system-hart-increment-1, accessed on 29 October 2024.

100. U.S. Department of Defense. "DoD Automated Biometric Identification System (ABIS)." *FY14 Army Programs*, pp. 103–106, accessed on 29 October 2024.
101. Federal Bureau of Investigation. "Next Generation Identification (NGI)." Law Enforcement Resources, https://le.fbi.gov/science-and-lab/biometrics-and-fingerprints/biometrics/next-generation-identification-ngi, accessed on 29 October 2024.
102. Federal Bureau of Investigation. "Face/Interstate Photo System." FBIBiospecs, https://fbibiospecs.fbi.gov/biometric-modalities-1/face, accessed on 29 October 2024.
103. CBSColorado.com Staff. "TSA Uses New Technology to Confirm Identity at Denver International Airport." CBS News, https://www.cbsnews.com/colorado/news/tsa-cat-2-technology-confirm-identity-denver-international-airport/, 18 November 2022.
104. U.S. Department of Homeland Security. "DHS/CBP/PIA-056 Traveler Verification Service." DHS, https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service, accessed on 29 October 2024.
105. Wikimedia Foundation, Inc. "Defense Enrollment Eligibility Reporting System." Wikipedia, https://en.wikipedia.org/wiki/Defense_Enrollment_Eligibility_Reporting_System, accessed on 29 October 2024.
106. Deputy Assistant for Global Information Services. "Privacy Impact Assessment: Integrated Biometric System." https://preview.state.gov/wp-content/uploads/2022/02/Integrated-Biometric-System-IBS-PIA.pdf, November 2021.
107. Secure Identity LLC. "A Better Way to Travel." CLEAR, https://www.clearme.com/?utm_source=website&utm_medium=nav, accessed on 29 October 2024.
108. U.S. Government Accountability Office. "Facial Recognition Technology: Federal Agencies' Use and Related Privacy Protections." GAO, GAO-22-106100, 29 June 2022.
109. U.S. Government Accountability Office. "Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training and Policies for Civil Liberties." GAO, GAO-23-105607, https://www.gao.gov/assets/d23105607.pdf, September 2023.
110. Wikimedia Foundation, Inc. "Biometric Identification by Country." Wikipedia, https://en.wikipedia.org/wiki/Biometric_identification_by_country, accessed on 29 October 2024.
111. Qian, I., M. Xiao, P. Mozur, and A. Cardia. "Four Takeaways From a Times Investigation Into China's Expanding Surveillance State." *The New York Times*, https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html, 21 June 2022.
112. Nash, J. "U.S. Loses Appetite for University Research but Not China." *Biometric Update*, https://www.biometricupdate.com/202209/us-loses-appetite-for-university-research-but-not-china, 1 September 2022.
113. The Associated Press. "U.S. Bans the Sale and Import of Some Tech From Chinese Companies Huawei and ZTE." *NPR*, https://www.npr.org/2022/11/26/1139258274/us-ban-tech-china-huawei-zte#:~:text=WASHINGTON%20%E2%80%94%20The%20U.S.%20is%20banning%20the%20sale,systems%2C%20citing%20an%20%22unacceptable%20risk%22%20to%20national%20security., 26 November 2022.
114. McCabe, D. "Biden Acts to Stop Sales of Sensitive Personal Data to China and Russia." *The New York Times*, https://www.nytimes.com/2024/02/28/technology/biden-data-sales-china-russia.html?searchResultPosition=19, 28 February 2024.
115. Federal Bureau of Investigation. "Chinese Government Poses 'Broad and Unrelenting' Threat to U.S. Critical Infrastructure, FBI Director Says." News, https://www.fbi.gov/news/stories/chinese-government-poses-broad-and-unrelenting-threat-to-u-s-critical-infrastructure-fbi-director-says, 18 April 2024.
116. Dwoskin, E. "Israel Escalates Surveillance of Palestinians With Facial Recognition Program in West Bank." *The Washington Post*, https://www.washingtonpost.com/world/middle_east/israel-palestinians-surveillance-facial-recognition/2021/11/05/3787bf42-26b2-11ec-8739-5cb6aba30a30_story.html, 8 November 2021.
117. Amnesty International. "Israel/OPT: Israeli Authorities Are Using Facial Recognition Technology to Entrench Apartheid." https://www.amnesty.org/en/latest/news/2023/05/israel-opt-israeli-authorities-are-using-facial-recognition-technology-to-entrench-apartheid/, 2 May 2023.
118. Corsight Ltd. "Introducing Facial Intelligence." Corsight, https://www.corsight.ai/, accessed on 29 October 2024.
119. Satariano, A., and P. Mozur. "Facial Recognition Powers 'Automated Apartheid' in Israel, Report Says." *The New*

REFERENCES, *continued*

York Times, https://www.nytimes.com/2023/05/01/technology/israel-palestine-facial-recognition.html, 27 March 2024.

120. Corsight Ltd. "Company." Corsight, https://www.corsight.ai/company/, accessed on 29 October 2024.
121. Oosto. "Visual AI Company AnyVision Changes Its Name to Oosto." https://oosto.com/press/anyvision-now-oosto/, 27 October 2021.
122. Mackinnon, A. "Russia's Surveillance State Struggles to Wean Itself Off Western-Made Components." FP, https://foreignpolicy.com/2021/05/24/russia-surveillance-technology-western-companies-facial-recognition/, 24 May 2021.
123. Kruope, A. "The Russian Government's Advance on Biometric Data." Human Rights Watch, https://www.hrw.org/news/2022/07/23/russian-governments-advance-biometric-data, 23 July 2022.
124. Kimery, A. "Russia to Expand Use of Biometrics to Identify Foreign Citizens and Immigrants Seeking Work." *Biometric Update*, https://www.biometricupdate.com/202003/russia-to-expand-use-of-biometrics-to-identify-foreign-citizens-and-immigrants-seeking-work, 10 March 2020.
125. Solovieva, D. "With the Kremlin's Blessing, Russian Companies Embrace Biometric Ambitions." Rest of the World, https://restofworld.org/2021/with-the-kremlins-blessing-russian-companies-embrace-biometric-ambitions/, 28 April 2021.
126. Borak, M. "Leaked Documents Reveal Details on Russia's Upcoming Surveillance System." *Biometric Update*, https://www.biometricupdate.com/202404/leaked-documents-reveal-details-on-russias-upcoming-surveillance-system, 1 April 2024.
127. Hersey, F. "UK Outlines Plans to Increase Biometrics for Immigration, Travel." *Biometric Update*, https://www.biometricupdate.com/202207/uk-outlines-plans-to-increase-biometrics-for-immigration-travel, 21 July 2022.
128. Lomas, N. "UK Urgently Needs New Laws on Use of Biometrics, Warns Review." TC, https://techcrunch.com/2022/06/28/uk-biometrics-legal-review/, 28 June 2022.
129. Borak, M. "Facewatch, Met Police Face Lawsuits After Facial Recognition Misidentification." *Biometric Update*, https://www.biometricupdate.com/202405/facewatch-met-police-face-lawsuits-after-facial-recognition-misidentification, 27 May 2024.
130. Hersey, F. "UK Biometrics and Surveillance Commissioner Submits Damning Report as Job Extended." *Biometric Update*, https://www.biometricupdate.com/202302/uk-biometrics-and-surveillance-commissioner-submits-damning-report-as-job-extended, 9 February 2023.
131. U.S. Department of Homeland Security. "New DHS Facility Tests Biometric Technology, Improves Air Entry/Exit Operations." DHS Science and Technology, https://www.dhs.gov/archive/science-and-technology/news/2014/07/30/st-snapshot-new-dhs-facility-tests-biometric-technology-improves-air-entryexit, 30 July 2014.
132. Vemury, A., J. Howard, and Y. Sirotin. "2022 Biometric Technology Rally Results Webinar." U.S. Department of Homeland Security Science and Technology Directorate, https://www.dhs.gov/sites/default/files/2023-06/23_0615_st_2022_biometric_tech_rally_results_webinar.pdf, 2022.
133. U.S. Department of Homeland Security. "Remote Identity Validation Technology Demonstration." DHS Science and Technology, https://www.dhs.gov/science-and-technology/remote-identity-validation-technology-demonstration, 2024.
134. National Institute of Standards and Technology. "Standards for Biometric Technologies." NIST, https://www.nist.gov/speech-testimony/standards-biometric-technologies, 19 June 2013.
135. Office of the Director of National Intelligence, Intelligence Advanced Research Projects Activity. "BRIAR: Biometric Recognition and Identification at Altitude and Range." IARPA, https://www.iarpa.gov/research-programs/briar, accessed on 29 October 2024.
136. Michigan State University. "Biometrics Research Group." MSU Department of Computer Science and Engineering, https://biometrics.cse.msu.edu/, accessed on 29 October 2024.
137. Michigan State University. "Publications." MSU Department of Computer Science and Engineering, https://biometrics.cse.msu.edu/pub/recent.html, accessed on 29 October 2024.
138. Federal Bureau of Investigation. "West Virginia University Named National Leader for FBI Biometrics Research." FBI, https://archives.fbi.gov/archives/news/pressrel/press-releases/west-virginia-university-named-national-leader-for-fbi-biometrics-research, 6 February 2008.
139. West Virginia University Vision and Learning Group. "Out-of-Distribution Learning." VL, https://vision.csee.wvu.edu/research/, accessed on 29 October 2024.

REFERENCES, *continued*

140. U.S. Department of Homeland Security. "Centers of Excellence." DHS Science and Technology, https://www.dhs.gov/science-and-technology/centers-excellence, accessed on 29 October 2024.

141. Naragn, N., M. Martin, D. Metaxas, and T. Bourlai. "Unconstrained Face Recognition Using Cell Phone Devices: Faces in the Wild." University of Houston Borders, Trade, and Immigration Institute, https://bti.egr.uh.edu/research/unconstrained-face-recognition-using-cell-phone-devices-faces-wild, accessed on 29 October 2024.

142. Kakadiaris, I. "Image and Video Person Identification in an Operational Environment: Phase I." University of Houston Borders, Trade, and Immigration Institute, https://bti.egr.uh.edu/research/Image-and-Video-Person-Identification-in-an-Operational-Environment-Phase-I/, accessed on 29 October 2024.

143. Purdue University. "Image/Video Analytics and Recognition." Purdue University: Vaccine, https://www.purdue.edu/discoverypark/vaccine/research/image-video-analytics.php, accessed on 29 October 2024.

144. National Science Foundation's Center for Identification Technology Research. "Center for Identification Technology Research (CITeR)." NSF IUCRC, https://iucrc.nsf.gov/centers/center-for-identification-technology-research/, accessed on 29 October 2024.

145. O'Brien, K., M. Rybak, J. Huang, A. Stevens. M. Fredriksz, M. Chaberski, D. Russell, L. Castin, M. Jou, N. Gurrapadi, and M. Bosch. "Accentire-MM1: A Multimodal Person Recognition Dataset." Winter Conference on Applications of Computer Vision Workshop, pp. 112–122, https://openaccess.thecvf.com/content/WACV2024W/RWS/papers/OBrien_Accenture-MM1_A_Multimodal_Person_Recognition_Dataset_WACVW_2024_paper.pdf, January 2024.

146. Mordor Intelligence. "Biometrics Companies." MI, https://www.mordorintelligence.com/industry-reports/biometrics-market/companies, accessed on 29 October 2024.

147. IMARC Services Private Limited. "Top Players in the Biometrics Market." IMARC, https://www.imarcgroup.com/biometrics-manufacturing-companies, accessed on 29 October 2024.

148. Fujitsu Ltd. "Biometrics & Biometrics as a Service." Fujitsu, https://www.fujitsu.com/global/services/security/offerings/biometrics/, accessed on 29 October 2024.

149. Biometrics Research Group, Inc. "NEC." *Biometric Update*, https://www.biometricupdate.com/companies/nec, 18 September 2024.

150. Technavio. "Top 10 Mobile Biometrics Companies." Technavio Blog, https://blog.technavio.org/blog/top-10-mobile-biometrics-companies, 8 January 2015.

151. Parson Corporation. "Identity Solutions for national Security." Parsons, https://www.parsons.com/identity-management-and-biometrics/, accessed on 29 October 2024.

152. HID Global Corporation. "Biometrics Authentication &Verification." HID, https://www.hidglobal.com/solutions/biometric-authentication-verification, accessed on 29 October 2024.

153. Biometrics Research Group, Inc. "Leidos Holdings Inc." *Biometric Update*, https://www.biometricupdate.com/companies/leidos-holdings-inc, accessed on 29 October 2024.

154. Mordor Intelligence. "Biometrics Market Size—Industry Report on Share, Growth Trends, & Forecasts Analysis (2024–2029)." MI, https://www.mordorintelligence.com/industry-reports/biometrics-market, accessed on 29 October 2024.

155. Burt, C. "Precise Biometrics: Quarterlies, Annuals, SEC Actions." *Biometric Update*, https://www.biometricupdate.com/202408/precise-biometrics-quarterlies-annuals-sec-actions, 19 August 2024.

156. Nash, J. "More Disconcerting Financial News in Biometrics." *Biometric Update*, https://www.biometricupdate.com/202402/more-disconcerting-financial-news-in-biometrics, 16 February 2024.

157. Grand View Research, Inc. "Facial Recognition Market Size, Share & Trends Analysis Report by Technology (2D, 3D, Facial Analysis), by Application (Access Control, Security, & Surveillance), by End-Use, by Region, and Segment Forecasts, 2023–2030." Grand View Research, https://www.grandviewresearch.com/industry-analysis/facial-recognition-market#, June 2024.

158. Willbrand, M. "The Future of Biometric Authentication and Digital IDs." NEC Today, https://nectoday.com/the-future-of-biometric-authentication-and-digital-ids/#:~:text=The%20future%20of%20biometric%20authentication%20lies%20in%20multimodal,create%20a%20more%20comprehensive%20and%20robust%20authentication%20system., 19 July 2023.

159. Tayib, M. "The Future of Authentication: Multi-Modal Biometrics in a Digital World." KYC AML Guide, https://kycaml.guide/perspective/multi-modal-biometrics-in-a-digital-world/, 26 October 2023.

REFERENCES, *continued*

160. Incode Technologies Inc. "The Future of Biometric Technology." Incode, https://incode.com/blog/future-of-biometrics/, 12 December 2022.

161. Ughade, N. "Everything You Need to Know About the Future of Biometrics." Hyperverge, https://hyperverge.co/blog/future-of-biometrics/, accessed on 29 October 2024.

162. Gibson, M. "M2SYS Multimodal Biometric Identification." M2SYS Blog, https://www.m2sys.com/blog/biometric-technology/multimodal-biometric-identification-system/, 20 May 2022.

163. Reyes, I. "Navigating the Future of Biometric Security: Trends and Innovations." Bioconnect, https://bioconnect.com/2024/02/15/navigating-the-future-of-biometric-security-trends-and-innovations/, 15 February 2024.

BIOMETRIC STANDOFF DETECTION: EXAMINING THE TECHNOLOGIES, IMPLEMENTATIONS, AND DEVELOPMENTS OF BIOMETRIC SYSTEMS

By Megan N. Lietha, Trey Kibodeaux, and Doyle T. Motes III

HDIAC-BCO-2024-579