

Unimodal, Multimodal Biometrics

Access Control Information Brief

asmag.com Security & IoT

Sponsored by: ZKTeco

Table of Contents

3 Introduction

4 Unimodal, Multimodal Biometric Technology FAQ

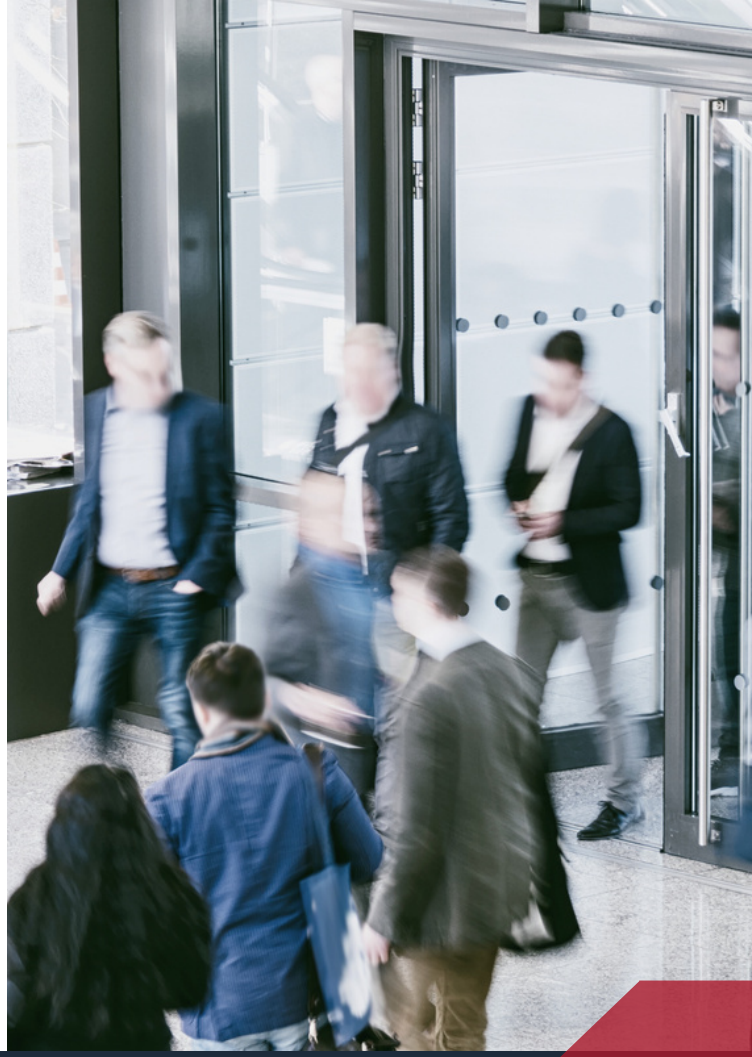
6 Multimodal Biometrics as an Industry Trend

8 Best Practices for Implementing Biometric Technology

9 Future Applications for Multimodal Biometrics

10 Key Considerations When Selecting Multimodal Biometrics Solutions for Projects

11 Biometric Use Cases



About asmag.com

asmag.com is a global online publication for physical security channel professionals: manufacturers, distributors and integrators. We provide the latest product and technology news in video surveillance and access control, in-depth market trend reports, and case studies for different verticals. Our services include targeted, measurable advertising solutions and live events that help our clients reach a qualified audience.

About ZKTeco https://www.zkteco.com/en/

ZKTeco is an internationally recognized enterprise specializing in pioneering biometric recognition techniques and provides products and solutions of smart entrance management, smart identity authentication and smart office. ZKTeco offers services on all fronts to public-service, enterprise-level and personal users.

Introduction

Physical access control is an essential aspect of security for any organization or facility. Using a combination of technologies, policies and procedures, building operators and security personnel can manage access to any physical space, building or area, ensuring that only authorized personnel can enter and use specific resources to ensure security at all levels.

According to current market reports, the access control market is set to grow at a significant rate in the coming years. Research firm MarketsandMarkets estimates that the global access control market will amount to US$9.9 billion in 2023 and reach $14.9 billion by 2028 (CAGR of 8.4%), with the biometric segment expected to show the highest growth rate.[1] Although the segment experienced a slowdown during the Covid pandemic, as things opened up the industry saw increased demand from business organizations across the globe for contactless solutions that can help reduce physical contact and the risk of virus transmission.

In the field of access control, biometric technology in particular has witnessed remarkable growth and innovation, particularly with continuous advancements in unimodal and multimodal biometric technology. Another report by MarketsandMarkets forecasted the biometrics market to grow to $82.9 billion by 2027, citing rising demand for authentication and identification solutions as well as security and surveillance as primary drivers for market growth, with the multi-factor authentication segment set to show the most growth.[2]

In terms of technology, unimodal biometrics has gained vast popularity in the industry due to its simplicity, ease of implementation and widespread application. Compared to traditional credentials such as RFID cards, fobs or keys, biometrics present operators with multiple benefits, including better security, scalability and accountability through features like audit trails.

While unimodal biometrics have been widely used for years, their inherent limitations and vulnerabilities led to the development of multimodal biometric solutions to provide an additional layer of security and accuracy. By using multiple biometric characteristics (e.g., fingerprint and facial recognition), multimodal biometric systems mitigate the risks associated with unimodal systems. Integrating multiple biometric traits does so by increasing the complexity of spoofing attempts, thus enhancing the overall robustness of the identification process.

It is important to note though at this point that unimodal and multimodal biometrics each have their applications and advantages. Unimodal biometrics may be more suitable for scenarios where simplicity and cost-effectiveness are essential, whereas multimodal biometrics excel in high-security environments or when robust authentication is required. The choice between the two depends on factors such as the level of security needed, user acceptance, budget and specific use case requirements.

What this information brief aims to do is present the various aspects of unimodal and multimodal biometrics that users should know: the basics of how the technologies work, the types of end-user organizations that can benefit, and why multimodal biometrics is strongly positioned to be a strong trend now and in the coming years.

asmag.com
Security & IoT

Visit www.asmag.com

Subscribe to the Security & IoT newsletter for the latest news.

Let's connect! **@asmagglobal**

1 MarketsandMarkets, Access Control Market by Offering (Hardware- Card-based, Biometric & Multi-technology Readers, Electronic Locks, Controllers; Software; Services), ACaas (Hosted, Managed, Hybrid), Vertical and Region - Global Forecast to 2028, https://www.marketsandmarkets.com/Market-Reports/access-control-market-164562182.html?gclid=Cj0KCQjwib2mBhDWARIsAPZUn_njfccjPdFill6AFf5xqGRwVXjsfnn8bnM5yQN5kObHXLKFHg8ppE0aArU6EALw_wcB

2 MarketsandMarkets, Biometric System Market with COVID-19 Impact Analysis by Authentication Type (Single Factor, Fingerprint, Iris, Face, Voice; Multi-factor), Type (Contact-based, Contactless, Hybrid), Offering Type, Mobility, Vertical & Region - Global Forecast to 2027, https://www.marketsandmarkets.com/PressReleases/biometric-technologies.asp

Unimodal, Multimodal Biometric Technology FAQ

What is the difference between unimodal and multimodal biometrics?

Simply put, unimodal biometrics rely on a single biometric trait for identification, while multimodal biometrics combine multiple traits for identity authentication.

Is multi-factor authentication the same as multimodal biometrics?

Not exactly. Multi-factor authentication uses multiple authentication factors such as a combination of passwords, security tokens or a biometric characteristic for identity verification. Multimodal biometrics uses multiple biometric characteristics such as a combination of fingerprint and facial recognition. However, both can be used together for enhanced security, now sometimes referred to as multi-factor biometrics.

What types of biometric traits or modalities are commonly used in access control?

Biometric traits can offer both unique and shared advantages as well as challenges. Adoption would vary depending on the application and the level of security required for the project.

Fingerprint recognition

Fingerprint-based recognition systems are widely deployed compared to other biometric traits. An image capture of the person's fingerprint is performed using a scanner or sensor. Optical sensors use light to capture the fingerprint image, while capacitive sensors detect the electrical properties of the ridges and valleys on the fingerprint. Specific minutiae points such as ridge endings, bifurcations and other unique patterns are identified and compared with stored templates in the database to find a match.

Fingerprint patterns are highly individual and the probability of two people having identical ones is nonexistent, making this an excellent biometric for accurate identification. Fingerprint scanners are relatively affordable and easily integrated into various security systems.

Things to consider: Reader accuracy is highly dependent on the quality of captured fingerprint images which can be affected by multiple environmental factors like dust, dirt, moisture, aging or physical damage to the fingertips. Partial or latent prints will make it more challenging to identify individuals and may require advanced algorithms to handle the cases accurately. Fingerprint recognition systems may also be susceptible to spoofing attempts using artificial or latex fingerprint replicas. Countermeasures like liveness detection and multi-factor authentication can help mitigate these.

Facial recognition

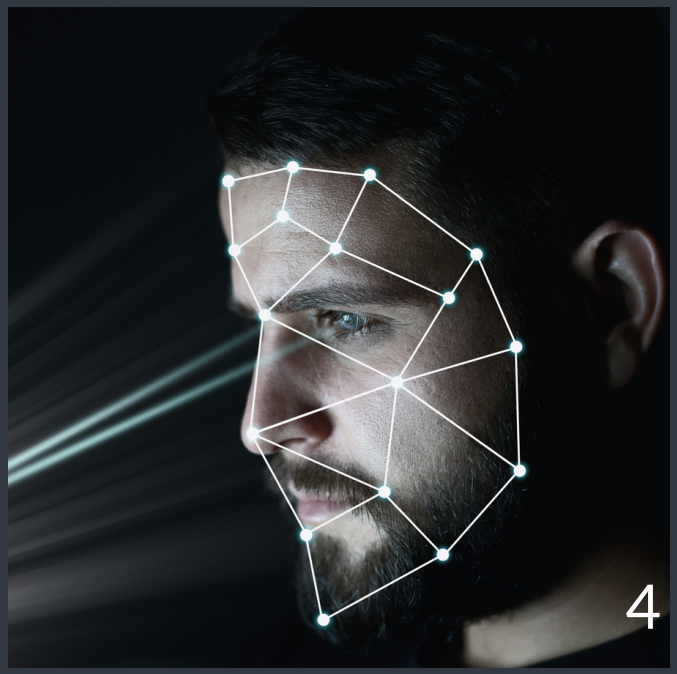
Facial recognition has become another preferred access control modality, especially after Covid-19 which forced business organizations to install touchless access control systems.

Traditional 2D facial recognition systems use infrared cameras and dot projectors to map the face as 2D images, causing a considerable loss in feature information as the face is inherently not flat, leading to inaccuracies with changing facial expressions, lighting

Q: What do you think is contributing to the rise of multimodal biometric trend?

"From my perspective, the preference for multimodal biometric terminals among channel players can be attributed to the benefit of model simplicity. It's important to consider that one of the significant costs for channel distributors is tied to stock management. An increased variety of models not only incurs additional managerial costs but also complicates maintaining an accurate stock level."

Swift Wu
General Manager
ZKTeco International Department



or head orientation. The inability to run liveness detection also makes the technology vulnerable to spoofing using photographs or recorded videos.

For 3D imaging, three technologies are commonly applied: ToF (AKA time of flight, perhaps more applicable for mobility), binocular stereo vision (acquires two images from different positions to calculate depth), and 3D structured light (laser dot arrays are projected on the target object, with the disparities from the original surface pattern read by high-speed cameras with deep learning algorithms). 3D structured light is widely used in facial recognition systems as it offers good accuracy even in short-range (approximately 0.5-1.2m), low-lit indoor applications.

Things to consider: For 3D structured light, the more laser spots projected on the face, the more accurate the results will be. Additional facial data can enhance the accuracy of 3D face recognition and liveness detection and converted into 3D face point cloud maps and 3D facial reconstruction.



Palm recognition

Single spectrum palm recognition uses a single wavelength or spectrum such as infrared, near-infrared or visible light to capture and analyze palm images. However, this may perform suboptimal in low-light or poorly illuminated environments, which can potentially lead to inaccuracies in feature extracting and matching.

Multi-spectrum palm recognition technology on the other hand uses multiple spectral bands or different imaging technologies together (e.g., near-infrared light and conventional visible light) for a more comprehensive capture of the palm's surface. Further combination with a positional calibration system and palm vein recognition algorithms can further test for liveness detection and screen more palm features such as the palm shape, print and vein, thus adding more layers of protection.

Things to consider: Devices with higher angle tolerance mean the system will be more forgiving and recognize the palm accurately even if it is presented at slightly different angles, but too much and the incidence of false positives and security vulnerabilities increases. Also, depending on the technology used, visibility under changing lighting conditions and smearing of images upon accidental movement may affect performance.

Iris recognition

Being the most complicated feature in biometrics, iris recognition is considered one of the most accurate forms of biometric verification. The use of near-infrared light can be used for long-distance identification, providing a flexible, contactless solution that can minimize the influence of ambient lighting conditions and pupil dilation while also detecting iris movement and eye gaze to gauge liveness for anti-spoofing.

It is worth mentioning though that facial recognition now offers similar performance as iris recognition but at a



lower price point. This technology is also easier for most users to implement on existing systems.

Things to consider: As with most biometric modalities on the list, external factors like dirt, reflection or glare onthe camera lens and poor device calibration can affect accuracy, as well as certain eye diseases or conditions like cataracts, glaucoma or even natural aging process that can cause changes to the iris over time. User acceptance might also be an issue as there may be user hesitation due to privacy concerns. Data protection will need to be top of mind.

How do spoofing attacks happen? What is being targeted?

A biometric system typically comprises four modules: sensor module, feature extraction module, template database and matching module.

Spoofing attacks can target any stage to try to gain unauthorized access. Attackers may use 3D printed finger replicas to fool sensor modules or distort their facial features to evade detection. Alternatively, they may try to generate a fake template that mimics the real one or reverse engineer the template generation process to create false templates. During the matching phase, attacks can exploit the matching algorithms tolerance to vulnerabilities to falsify a match.

Multimodal Biometrics as an Industry Trend

Where can multimodal biometrics play a more effective role?

As its name suggests, a multimodal biometrics solution combines more than one biometric modality. The solution typically has an extra “fusion” component integrating data from two (or more) biometric subsystems that can operate at any level i.e., during feature extraction, template comparison or decision-making.



Here are just some of the areas that multimodal biometrics would hold an advantage over unimodal biometrics:

Accuracy
Multiple biometric modalities used means more data points for the system to collect and analyze, enabling a better, more secure system as it can minimize false acceptance rates (FAR) and false rejection rates (FRR). Furthermore, if one modality is compromised, the other may still be used for identity authentication which can enable business and organizational processes to operate smoothly and minimize delays due to error readings.

Multimodal biometric systems are also able to maintain reference thresholds for better accuracy. Reference thresholds refer to a predetermined decision criterion that classifies biometric measurements as real (reasonably matches a reference template) or false. This threshold helps strike a balance between the system's FAR and FRR. This is important because biometric data of the same individual taken at different times will never be identical.

Industry Insight

Q: How should users determine which multimodal biometric modality solution would work best? Does this depend on use cases?

"The choice of multimodal biometric technologies is not one-size-fits-all. There is no 'ideal' combination that universally suits all use cases and users. Rather, the choice of biometric modalities is dictated by the specific requirements of the use case, environmental conditions, and the preferences or needs of the end-users.

For instance, the combination of fingerprint and face recognition is a widespread choice. This combination offers the flexibility to users by allowing them to choose between different modalities based on the situation. Face recognition is a proactive recognition technology, meaning it can automatically recognize individuals without their explicit interaction. However, some users may prefer fingerprint recognition for its passive recognition characteristics, which requires deliberate user interaction.

Moreover, some users might struggle with certain modalities due to individual physiological characteristics. For example, roughly 3.5% of the population has fingerprints of poor quality that can hinder smooth recognition. In such cases, having an additional biometric option ensures these users can still authenticate themselves effectively."

Raymond So
Head of Marketing
ZKTeco International Department

Adaptive security
As the solution uses different levels of biometrics fusion for authentication, it allows users the flexibility to tailor solutions to be more secure (stricter threshold) or more convenient depending on project requirements.

The choice of the reference threshold is critical, as it directly affects the performance and security of the biometric system. A more stringent threshold enhances security by minimizing the risk of unauthorized access but might increase the likelihood of legitimate users being rejected (FRR). On the other hand, a more lenient threshold could increase user convenience but might also raise the FAR. The optimal threshold depends on the specific use case, the desired balance between FAR and FRR, and the overall security requirements of the system.

Anti-spoofing
Combining multiple biometrics also makes the solution more secure as it increases the complexity and difficulty of would-be attacks as attackers must simultaneously replicate and manipulate multiple modalities. Additionally, multimodal biometric solutions are usually equipped with adaptive algorithms that analyze anomalies across various modalities and run liveness detection to discern between real users and fabricated identities. This makes multimodal biometrics an ideal strategy for safeguarding properties and assets from unauthorized intrusion.

What could be standing in the way of the widespread adoption of multimodal biometrics for access control?

On the installer/integrator level: All these biometric modalities need to be integrated into existing systems. Without proper training or knowledge, compatibility, installation and interoperability issues may ensue, which would result in delays or inaccuracies in identity authentication, thus affecting the overall experience for both the operators and users.

On the operator/user side: The cost and perceived complexity of deploying and maintaining multimodal biometric systems due to their specific hardware and software requirements may deter some business organizations from adopting this technology in their security systems.

Concerns over data privacy always come up when biometrics is involved. What measures can be taken to ensure data protection?

Data protection and privacy are important concerns for biometric systems as many organizations and governments understand that this can be used to exploit other systems. Users should make sure that their biometric solutions abide by compliance requirements to ensure privacy.

Data protection can be implemented at multiple levels – algorithm, system and operational levels. Data encryption is a must. Irreversible biometric templates can prevent the original template from being reverse-engineered even if the user key is exposed for an additional layer of protection. On the operational level, users should be mindful and actively control how their data is handled and stored, making full use of security settings, functions and modes to include or hide sensitive information during the verification process. It would be vital for business organizations to use solutions that come with clear privacy policies and meet the requirements of local and international data security regulations such as Data Security Law, Personal Data Protection and the EU GDPR through ISO certifications.

Q: Some users might cite concerns over cost, speed of authentication and trust/ethics issues? Are these legitimate concerns?

"To be frank, the price differences and quality issues between multimodal biometric terminals and unimodal biometric terminals are not as significant as one might think. The price variance is only around 15 to 25 percent, and the difference in recognition speed is practically negligible.

One of the most significant barriers to the adoption of multimodal biometric technology in projects is privacy concerns. There's a prevalent misunderstanding and negative perception of biometric technology.

To overcome these obstacles, we need to focus on educating the market to alleviate unnecessary concerns and promote acceptance of this technology. ZKTeco has always believed that biometrics technology is the most reliable credential one can possess. By dispelling misconceptions and highlighting the benefits of biometrics, we can pave the way for broader adoption of multi-modal biometrics in the security industry."

Jeff Yang
Product Director
ZKTeco International Department

Best Practices for Implementing Biometric Technology

"Users can optimize the results of multi-modal biometric devices and prevent potential privacy and security issues through proper installation and following best practices. The key is to ensure the devices are installed in a way that maximizes their effectiveness while ensuring they are accessible and user-friendly for everyone."

Jack Duan, Product Manager, ZKTeco International Department



Touch Biometrics (Fingerprint and Finger Vein)

The primary consideration for installing touch biometric devices is the installation height. It is crucial to ensure the installation is accessible to everyone, including users with disabilities.

Touchless Biometrics (Facial and Palm)

The installation of touchless biometric devices involves several important considerations:

- **Lighting conditions:** Since touchless biometric technologies use cameras to capture biometric features, the performance of the device can be significantly affected by lighting conditions. Even though all cameras in the biometric terminals are equipped with state-of-the-art WDR technology, performance may be compromised if the terminal is installed in a direction directly against sunlight.

- **Installation position:** The pose angle tolerance for facial recognition is +/- 30° (pitch, yaw and roll), while for palm recognition it is +/- 60° (pitch, yaw, roll and blend). As long as the terminal is installed within these ranges, it should function effectively. However, it is important to be mindful of users with disabilities and ensure the installation accommodates their needs.

Future Applications for Multimodal Biometrics

Multimodal biometrics are already deployed in various projects by users keen on leveraging their advantages in security, accuracy and flexibility that make them especially suitable for entities that are critical in nature. Here are some use case scenarios that we see would benefit the most from multimodal biometrics in the near future.

Border control

Identity checks at borders are of critical importance. In this regard, multimodal biometrics can be useful and are in fact deployed at certain border check points. An example is Kuwait, which is expected to put into place this year a multimodal biometric border control system, utilizing a combination of biometric technology such as face recognition, fingerprint scanning, and iris identification, to strengthen security and simplify its immigration processes.[1]

Prisons

For prisons, access control must take into consideration the safety, security and privacy of prisoners and visitors. In this regard, multimodal biometrics can again be useful. The New South Wales government, for example, is expected to roll out this year at their correctional facilities multimodal biometrics systems combining iris and facial recognition. The new system is said to allow improved experience due to faster processing times and improved categorization of the different types of persons entering a correctional center.[2]

Healthcare

Healthcare is another sector that can benefit hugely from multimodal biometrics. In healthcare facilities, added security is needed for access to patient data or critical areas such as the emergency room. Hygiene is another major requirement, especially in the post-pandemic era. As such, hospitals can be well served by a multimodal solution combining two contactless biometrics, for example facial and iris recognition.

Conclusion

In this paper we've taken a closer look at multimodal biometrics, which entail using more than one biometric for verifying an individual. Compared to unimodal biometrics, a multimodal biometrics solution offers business organizations higher accuracy, security and flexibility, albeit at a slightly higher price point. Deployment has also been on the increase, seen at a range of end user entities. Challenges such as perceived privacy infringement is expected to become less of a concern, once more legislation are in place and the public becomes more educated about the technology. We therefore hold the view that multimodal biometrics will see continued demand and growth in the long run.



1 Kuwait: Biometric system to be implemented at all ports by early 2023, https://www.zawya.com/en/legal/immigration/kuwait-biometric-system-to-be-implemented-at-all-ports-in-early-2023-hkrxf3hf
2 NSW deploys facial recognition systems into prisons, https://www.innovationaus.com/nsw-deploys-facial-recognition-system-into-prisons/

Key Considerations When Selecting Multimodal Biometric Solutions for Projects

"When choosing multi-modal biometrics, users should consider several key factors:

- **Touch vs Touchless:** Some users may have a preference for or against physical contact with the biometric device. Touchless biometrics like face or iris recognition do not require physical contact, making them more hygienic and convenient in certain situations.
- **Application Scenarios:** The choice of biometrics can depend on whether the application is meant for indoor or outdoor use. Different environmental conditions can affect the performance of certain biometric modalities. For instance, face recognition might struggle in poor lighting conditions, whereas fingerprint recognition may be less affected.
- **Biometric Capacity:** Different biometric modalities have varying capacities for unique identifiers. The user base size and the required level of security can dictate which biometric modality is more suitable.
- **Installation Environment:** The physical environment where the biometric system will be installed can impact its effectiveness. For touchless biometrics, factors such as lighting conditions can significantly affect performance.

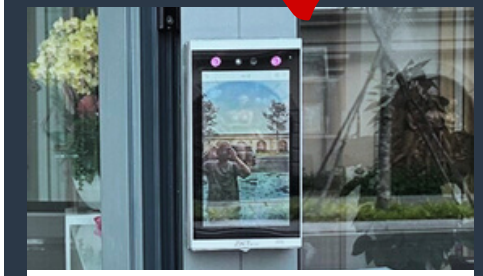
The choice of multi-modal biometric combinations should be dictated by the specific requirements and constraints of each use case, rather than attempting to find a universally 'ideal' combination."

Paul Yang
Senior Product Manager
ZKTeco International Department



Biometric Use Cases

Click image to read full case study



Commercial office

Vietnamese logistics company Seahorse Shipping installed ZKTeco's face recognition-based access control and timekeeping project integration with elevator control to secure and monitor their whole facility.



Education

STAN Polytechnic of State Finance in Indonesia deployed a ZKTeco solution with ProFace X [TD] access control terminals at the entrance for reliable identity authentication and adherence to mask regulations during Covid.



Manufacturing

Solar cell manufacturer Jiangsu Runergy New Energy Technology installed hybrid biometrics terminals linked to InBioPro Series access controllers and centrally managed by ZKTeco BioCVSecurity software.



Banking

Transline Technologies integrated Armatura's touchless palm recognition sensors into their time and attendance solution for biometric identity and access management for Indian banking institutions world-wide.