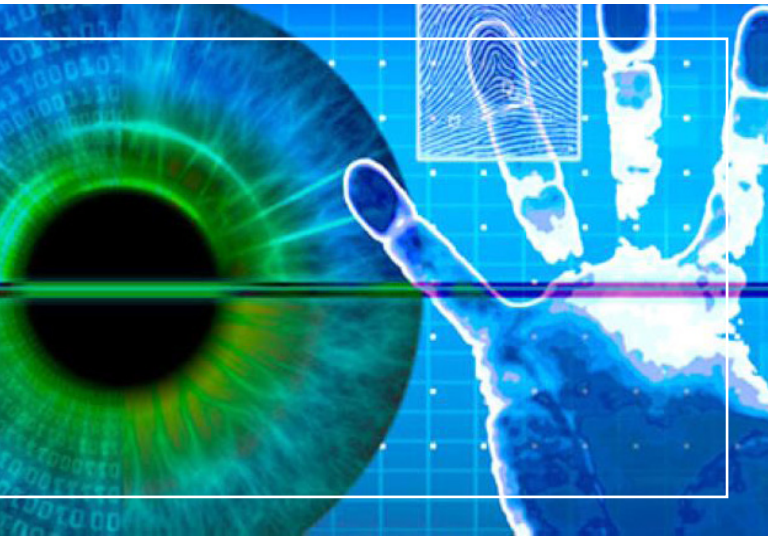
techtalk.travel

Biometrics in the Hospitality Industry

July 2020

In the hotel industry, there are certain inconveniences that most frequent travellers have just accepted. Many of us have had to wait patiently at a front desk while our documents are checked, passports are photocopied and details verified. Once that process has been completed, I don't know about you, but many times I've been frustrated after making the long walk to the room, only to find that the keycard responds with that annoying little blinking red light and remains locked. As a way of expediting this process and making life easier for the guest, biometric technologies are being considered as a possible solution, and with COVID-19 not going anywhere soon, any technology that offers a contactless experience may start to be even more necessary.



WHAT ARE BIOMETRICS?

Biometrics are biological measurements or physical characteristics that can be used to identify individuals. Fingerprint mapping, facial recognition, and retina or iris scanning are all forms of biometric technology, but these are just the most well-known options. Most people, even the end users, who are not directly associated with biometric technology in any way, know it to be a technology that makes use of fingerprints, face, voice or eyes to recognize an individual. The level of familiarity with biometrics has improved recently due to the rise of biometric recognition on mobile devices. Biometric recognition, however, is not limited only to the most common known methods.

There are various other biometric methods that we generally do not hear much about, such as :

- Pattern formed by a person's lips
- The shape of an ear
- A person's gait
- Thermography

BIOMETRICS IN PRACTISE.

Check-in and door access

Biometrics in hospitality is not new technology and is already in use to a small degree. A handful of hotels have already introduced guest room access via biometric solutions such as fingerprint scanners. Marriott International in 2018 together with Alibaba introduced facial recognition check-in services to some of their hotels in China.

Using Biometric technology in the future could very well be another way hotels can ensure a guests stay can be a safe one by minimising the number of touch points they have when at the hotel. For example, let's take the check-in process. Relevant data can be provided before guests arrive at the hotel, offering the option to check in and access their room in a much more expedited and "contactless" way, while still maintaining the necessary level of security.

It would not be too far fetched to think of a future where guests will use facial recognition to unlock the room door, or even pay for meals and other services the hotel provides.

Prior to COVID-19, these technologies would have been applied in different ways to different styles of hotels. For example, minimum service properties vs. luxury properties.

1. Minimum Service; using biometrics could increase convenience to the guest whilst also minimising the hotels operating and running costs.
2. Luxury Property; looking to create a luxury experience with guests staying in a high-tech hotel or resort, offering seamless access to services and guest service outlets across the property with minimal touch points.

Yet whilst these features sounded cool in the past, today thanks to COVID-19, there is a much more practical reason for biometric technology.

Employee attendance, tracking and payroll efficiency

Biometric technology doesn't just have to make the guests experience better or more secure. It can be applied to back of house technology needs and assist with employee attendance, time tracking and improve payroll efficiency. Keeping track of employees in and out times can bring greater payroll transparency, helping hotels ensure their employees are being paid accurately for the hours worked. Taking away the manual process of managing timesheets through biometrics can also prevent timesheet manipulation. Using a biometric based clock-in and out system eliminates the possibility of timesheet fraud as employees have to be present to clock in or out.

Yotel was a very early adopter when they, in 2015 introduced biometrics for the purpose of tracking employee attendance. Yotel implemented biometric handprint scanners across some of their European properties, in order to enhance shift monitoring and employee scheduling, with the expectation that by improving employee-facing technology it could lead to increased guest satisfaction.

Security

With the recent number of high level data breaches experienced across the hotel industry, the need to protect both company and guest information is always present and ever increasing. One fundamental expectation of every hotel guest and employee is their personal privacy, yet given the current online marketplace for selling everything from credit card numbers to private photos, it's a consistent challenge to lock this data down and ensure its security.

IDs and other printed identity documents can be counterfeited; passwords or PINs can be guessed, stolen or hacked, but biometric identifiers can neither be counterfeited or stolen. It has been shown that fingerprints and or facial recognition systems can be hacked, however, newer systems are equipped with more advanced technology that don't accept anything other than a live biometric identifier, making biometrics more secure than other identification methods.

ADVANTAGES AND DISADVANTAGES OF USING BIOMETRIC IDENTIFICATION

ADVANTAGES

Advantages of biometric technology is that it is less time consuming, dependable, user friendly, hard to falsify, requires minimal training and accesses distinctive recognition features of individuals resulting in accurate verification.

Speedy identification and authentication

Biometric technology eliminates the need of a person carrying what most of us consider traditional items of proof of identity. Every person has their own unique characteristics that make us who we are. By using the obvious biometric characteristics such as face or fingerprint, proving a person's identity can be a seamless and almost non invasive process. It goes without saying that it is a much more secure way of validating a person's identity, especially now with the ever increasing numbers of identity theft and counterfeiting of IDs.

Accountability

Accessing a biometrically secured area such as a guest room or employee back office facility requires the physical presence of the authorized person after a biometric scan. Reliable and fully auditable logs can then be generated from all those who accessed these areas. If for any reasons these logs are required for validation of access or proof of non-access, this data will clearly show proof of access or not.

Convenience

Convenience is of course a big advantage when using biometric identification, however, some still ask at what privacy cost, yet managing our user IDs and passwords can often be an annoying task. Passwords and PINS are easy to forget, causing people to write them down, consequently opening them to theft and exposing them to potential hackers. With biometrics technology, fingerprints won't be lost and can't be attained or copied by someone aiming to illegally gain access.

DISADVANTAGES

All technology based systems have their limitations and biometrics is no exception. Biometric identification offers a lot of benefits, however, the current disadvantages should also be reviewed when considering biometric technology.

Some of the current major disadvantages associated with biometric identification consist of:

Biometric identifiers cannot be changed, if compromised

Physical traits can't be altered. Like any technology, biometric systems are not perfect. Users can't rely on the safety of their data, if the data is stolen, people can't change their identification traits like they can change passwords during a security breach. PINs and passwords can be changed if compromised, biometric identifiers of a person cannot be changed if stolen.

Changing of a person's physical traits

The authentication system only recognizes traits that were entered and would fail to recognize the user if their physical traits change even the slightest. Here are a few reasons why traits might change:

- A burnt or damaged finger
- Retina transplants
- Tattooed hands
- If the user is wearing lenses (and usually doesn't) or vice versa

To resolve issues such as these the authentication method needs to be changed to grant authorized user access, which can be inconvenient.

Hardware and Scanner Issues

Some biometric systems can face scanning issues if there is even a slight change, especially if retina scanning is used. Iris scanning is still not 100% reliable, failure can occur if the user has long eyelashes, different eye color, or there is a reflection in the cornea.

Software Malfunction

Like all software based systems there is an element of unreliability due to it being an automatic system dependent on electricity. If there is a power shortage, and no method of backup power via a generator or UPS then users would not be able to access the system.

On top of this, should the software have a bug or fail due to any reason, access to users will be restricted until the software is restored.

Cost

Like all technology, as it becomes more mainstream it tends to get cheaper to buy and deploy. Despite this, biometric technology can still be an expensive solution to implement for smaller hotels or businesses. Especially if they have a smaller number of people (guests) to identify and staff to manage. As with all technology, regular maintenance is important to ensure optimum performance, and this too comes at an extra cost.

Technical complexity

Biometric technology may require onsite administrators to have a certain level of tech-friendliness or a dedicated IT resource to maintain the system and perform any required day-to-day back-end operations. Some smaller hotel operations may not be comfortable with this, finding the maintenance and daily management of biometric systems too complex to receive any real perceived value.

CONCLUSIONS

Whatever method is used, what all biometric techniques have in common is that they all collect human characteristics, which are:

1. **Universal, as they can be found in all individuals**
2. **Unique, as they make it possible to differentiate one individual from another**
3. **Permanent, allowing for change over time**
4. **Recordable (with or without consent)**
5. **Measurable, allowing for future comparison**
6. **Forgery-proof (a face, a fingerprint)**

Adoption of biometric applications has grown exponentially in a very short space of time and it has been deployed for a variety of use cases across different industry types. Guests will continue to expect hotels to offer the very latest in technology and security. At this point, mobile biometrics are the most advanced way to achieve this.

For staffing, hotels may face opposition from employee unions and employees due to privacy issues. Part of a hotel's research and due diligence before procuring and installing biometrics technology should include obtaining legal advice.

Modern times we live in now will demand that biometrics become more and more prevalent as travel begins its recovery process. With more people using biometrics in their normal everyday lives, e.g unlocking their iPhone or other technology devices, the added expectation, convenience and security of using biometrics will only increase. The days of standing at a Front Desk while the hotel attendant fusses over your documents will be coming to an abrupt end.

SOURCES

Bayometric

Thales Group