

SECURITY WITH CONVENIENCE - IS IT REALLY TOO MUCH TO ASK FOR?

Finding a balance between delivering security while at the same time providing convenience for users has long been problematic.



OUR PRIMARY FORM OF USER AUTHENTICATION TODAY REMAINS THE PASSWORD, WHICH FAILS AT BOTH: SECURITY BECAUSE PASSWORDS ARE EASILY STOLEN OR GUESSED AND CONVENIENCE BECAUSE THEY ARE SO CUMBERSOME TO USE. TECHNIQUES LIKE ONE TIME PASSWORDS AND TWO FACTOR VERIFICATION BY SMS MIGHT HELP WITH SECURITY, BUT AT SIGNIFICANT COSTS IN TERMS OF USER EXPERIENCE.

ISN'T IT POSSIBLE TO DELIVER BOTH SECURITY AND CONVENIENCE TOGETHER?



Biometric techniques are now entering the mainstream and offer this promise: secure identification with the utmost convenience to the user. Since biometrics are measurements of personal characteristics, the user doesn't have to remember anything, type anything, carry anything.

Amid a bewildering landscape of new and not so new biometric techniques now available, what metrics can we use to sort the good from the bad, those that will solve our problems from those that will just give us more problems?

It's useful to break down our overall categories of security and convenience into more fine-grained requirements.

THE KEY FACTORS AFFECTING THE SECURITY OF A BIOMETRIC MODALITY

- The accuracy must be high. Specifically, the false accept rate (FAR) must be very low so that imposters are not admitted incorrectly.
- It must be difficult for an attacker to acquire a person's samples without their consent.
- It must be extremely difficult for an attacker to play back samples to the system in order to pose as another person. This is called "spoofing".

THE KEY FACTORS AFFECTING THE CONVENIENCE OF A BIOMETRIC MODALITY

- The accuracy must be high. Specifically, the false reject rate (FRR) needs to be low so that the system can be accessed without having to retry multiple times.
- The biometric device must be ergonomic to use.
- Acquiring the samples needs to be fast.

This paper explains how Hitachi's finger vein technology (VeinID) is unique in meeting all of these requirements, setting it clearly apart from other biometric techniques.

ACCURACY IS FUNDAMENTAL

Accuracy heads our list for both security and convenience. It is a fundamental requirement that our authentication method is accurate.

All biometric techniques perform “fuzzy” matching – the human body is constantly changing and never gives the same sample twice. This means that there is always a chance of falsely accepting an imposter, or falsely rejecting a genuine user.

Usually there is a trade-off. If the criteria is tightened so as to exclude more imposters then the chance of genuine users being excluded is greatly increased. If the criteria is relaxed to improve user experience then there is a greater risk of imposters accessing the system.

Playing off security and convenience like this just puts us back at step one. What we need is a biometric technique that is fundamentally sufficiently accurate so we don't need to make this trade-off at all.

ISO STANDARD TESTING HAS SHOWN HITACHI'S FINGER VEIN BIOMETRIC TO BE MARKET LEADING FOR ITS INHERENT ACCURACY, ACHIEVING:

- False accept rates of one in one million (0.0001%).
- False reject rates of one in ten thousand (0.01%).

This places finger vein as orders of magnitude more accurate than modalities like fingerprint, face or voice recognition. When a fundamentally more accurate biometric technique is used, it means that fewer compromises need to be made in the implementation.

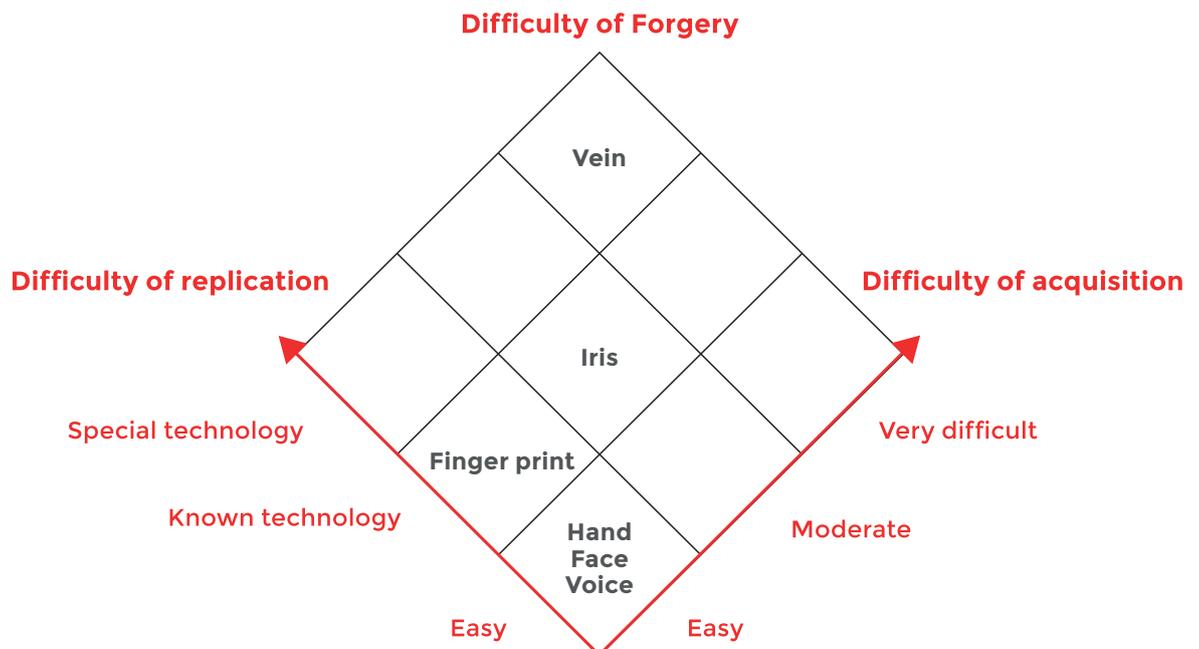
HOW TO RESIST ATTACKS

Security that is resistant to attack is formed of layers. In biometric systems, two of the layers are the difficulty of an attacker acquiring a person's sample and the difficulty of an attacker replaying a person's sample to the biometric system.

Most biometrics are very easy to acquire without the knowledge or consent of the subject. We leave our fingerprints everywhere and they are simple to lift. Voice samples, face and even iris images can all be acquired from a distance of several metres, without the subject's knowledge.

Finger vein biometrics, however, are unique in being based on data from inside the body – the blood vessels within the finger. It is impossible to acquire samples from a distance or without specific action by the subject.

In addition to being acquisition resistant, finger vein biometrics are also highly spoof-resistant. In varying degrees, biometric techniques have historically been shown to be vulnerable to attack with fake samples. Ways of presenting fake prints to fingerprint scanners are well known and not difficult to perform. Even going to the extreme of cutting off somebody's finger would not fool a VeinID scanner: without blood under pressure the vein pattern is not maintained and the attempt would fail.



ERGONOMICS MATTER. TO GAIN WIDESPREAD ACCEPTANCE, YOUR CHOICE OF BIOMETRIC IDENTIFIER HAS TO PRESENT A FRICTIONLESS PROCESS TO USERS.

Hitachi's VeinID achieves this by being fast - it takes around a second to read a sample - and intuitive to use. Placing a finger on the scanner is natural and comfortable, with minimal contact.

VeinID scanners are available in a variety of formats to suit different use cases and user-bases, such as embedded, desktop and portable.

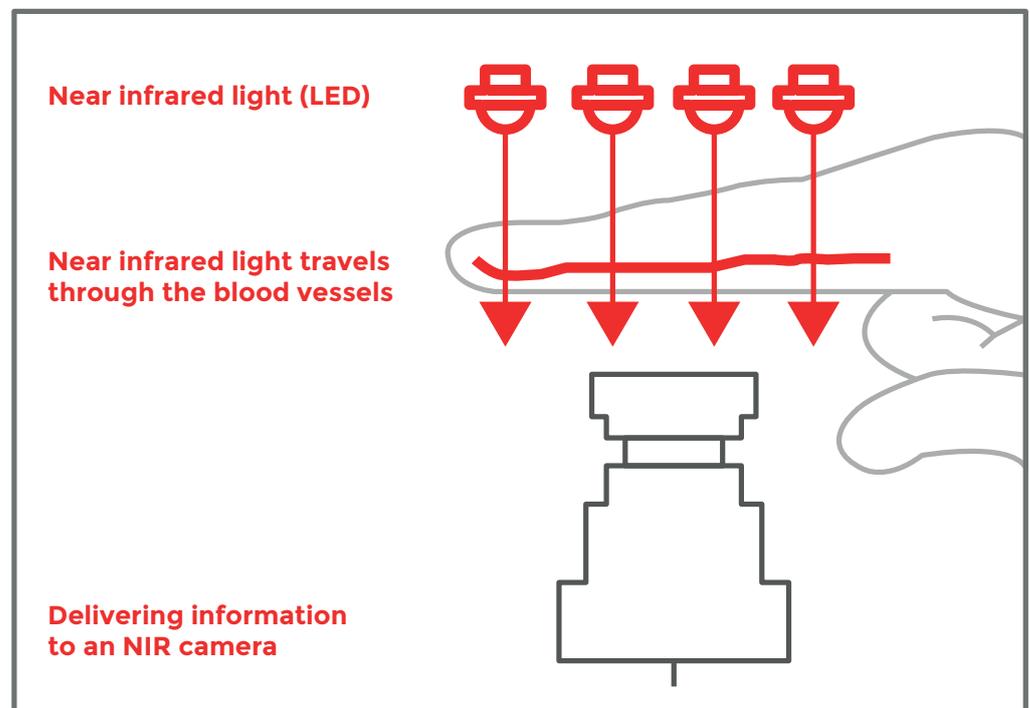


HOW DO WE ACHIEVE THIS?

As described, Hitachi's finger vein technique is unique among mainstream biometrics in genuinely imaging internal features of the body.

To do this, we shine harmless infrared light through the finger. The infrared light is strongly absorbed by the blood in blood vessels, and we are able to acquire clear shadow images of the subsurface veins.

Using Hitachi's patented image analysis techniques we are able to extract each finger's unique branching pattern of blood vessels. This is further processed into a biometric template which is used to verify the user's identity. Every finger has a unique pattern of blood vessels, whether fingers on the same hand, fingers on left and right hands of the same person, fingers of twins or siblings or fingers of unrelated people. This allows VeinID technology to be highly accurate, as well as secure, fast and easy to use.



NO COMPROMISE

Security and convenience do not have to be alternatives to one-another. The promise of biometrics is that it is possible to achieve both together. But not all biometrics are equivalent. There is an increasingly wide choice available with significantly varying characteristics.

This paper argues that when considering all the factors that underpin both security and convenience, the unique characteristics of Hitachi's VeinID technology give the right combination of strengths to deliver both, without compromise.

HITACHI FINGER VEIN BIOMETRICS

	ACCURACY	SECURITY	SPEED	EASE OF USE	PRIVACY	USER RESISTANCE	SIZE	COST
 FINGER VEIN	High	High	Fast	High	High	Low	Small	Low
 FINGER PRINT	High	Low	Fast	Fast	Very Low	Medium	Small	Low
 IRIS	High	Medium	Slow	Low	Medium	High	Large	High
 FACE	Low	Low	Medium	Low	Low	Low	Medium	Medium

ALL OF THE STRENGTHS OF OTHER BIOMETRICS, WITHOUT THE WEAKNESSES

FURTHER INFORMATION

Please contact Hitachi Europe Limited for further information about Hitachi's finger vein technology, applications and devices.

© 2016 Hitachi Europe Limited. All copyrights and intellectual property rights are owned by and reserved by Hitachi Europe Limited and its subsidiaries.

Hitachi Europe Limited's prior written consent is required before any part of this document is reproduced.

CONTACT DETAILS

Information Systems Group,
Hitachi Europe Limited,
Whitebrook Park,
Lower Cookham Road,
Maidenhead,
Berkshire,
SL6 8YA.

digitalsecurity@hitachi-eu.com
<http://digitalsecurity.hitachi.eu>

HITACHI
Inspire the Next

Hitachi Digital Security