

*Your quest for the ideal biometric:
is it in vain?*

Introducing Hitachi's Finger Vein Technology
A White Paper

Ben Edgington

May 2007

© 2007 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.

SYSTEMS SOLUTIONS DIVISION

Hitachi Europe Ltd, Whitebrook Park, Lower Cookham Road, Maidenhead, Berkshire, SL6 8YA.

Tel: +44 (0) 1628 585000, Fax: +44 (0) 1628 585440

www.hitachi-eu.com

1. What makes a good biometric?

The search for the Holy Grail, the perfect biometric, continues.

Every previously proposed physical biometric identifier has turned out to have issues of one sort or another — whether it be fingerprint, iris, facial, voice, hand geometry, ear shape, or the rest — each one presents us with a compromise at some point.

But we must ask, what characteristics would the ideal biometric possess? Of course, to an extent, that depends on your application, but there are some fundamental properties that we can assume are desirable for all physical biometric identifiers. These might be broadly grouped into the areas of *security* and *practicality*.

1.1 Security

Security is the whole point. If you are not concerned about security then why use biometrics at all? There are two main aspects of security that our ideal biometric must satisfy:

- *Resistance to forgery.*

An “internal” biometric will by nature be more secure than an “external” biometric, since it will be essentially impossible to duplicate or modify. An example of the potential insecurity of external biometrics was found by Japanese researchers who were able to lift fingerprints from glass and authenticate to fingerprint scanners using fake fingers made from household ingredients^[1].

- *Accuracy.*

A low false acceptance rate (FAR) is crucial to security; it is critical that unauthorised individuals are not misidentified as authorised. The FAR depends on several factors, such as the distinctiveness of the chosen biometric between individuals (essentially, its uniqueness), the ability to capture the biometric information accurately, and the ability to match it correctly.

From this point of view, the iris is a good biometric; there is a high degree of randomness and complexity in iris patterns that underpins its uniqueness and distinctiveness between individuals.

However, the FAR covers only one side of accuracy. The false rejection rate (FRR – incorrectly rejecting individuals who are actually authorised) also matters, but is more of a practicality issue, and is discussed in the next section.

1.2 Practicality

Obviously, we can propose an authentication process that is as *secure* as we like, but unless it is also *practical* then it will never succeed.

Practicality and security are often at odds with each other, and any final system will be a trade-off between them. The point at which we are prepared to make the compromise will depend on the value of what we are protecting — the security systems guarding the Crown Jewels would not be practical to implement in the average UK home. Ideally, our chosen biometric should possess characteristics that limit the need for compromise by enhancing both security and practicality.

Significant areas of practicality that we should consider are as follows.

- *Speed.* A practical biometric needs to be quick to use and quick to match. An illustration of this is given by a UK school who implemented iris recognition for their lunchtime payments system^[2]. After a year the system was abandoned^[3] for being too slow. “We do not want pupils' meals getting cold while they wait in the queue”, said the head teacher.

- **Accuracy.** A system that rejects legitimate users may be secure, but is certainly inconvenient. The perfect biometric will never reject an authorised individual (zero FRR) and never accept an unauthorised individual (zero FAR). Among technologies with the worst FRRs are face and voice recognition.

Sometimes extraneous factors can affect the accuracy of a biometric method. A voice recognition system may fail to identify a user with a cold. A fingerprint system may be sensitive to dirt or grease or abrasion on the finger. An iris system may be affected by the presence or absence of spectacles. An ideal biometric will be as insensitive as possible to extraneous factors.

- **Cost.** There will always be a compromise between the security a system offers and its cost. For example, fingerprint readers are now a commodity, low-cost product; however, they do not offer a high level of security. An ideal biometric will be “cost-effective”, able to offer a relatively high level of security at a relatively low cost.
- **Size.** Many security applications have size constraints, such as PC login or door access. The need to accommodate a large reader device (such as in the case of palm recognition) is a practical issue.
- **Enrolment.** The more people who can enrol with our chosen biometric, the better. Some biometrics are less suitable than others: fingerprints can wear or wrinkle with age to the point where they become unusable; drooping eyelids can be a problem for iris recognition. This is particularly an issue for the disabled, where the chosen biometric may not be present, or bodily position may be an issue. For example, a UK Passport Service study^[4] showed a 39% failure to enrol (FTE) for disabled people using iris recognition.
- **Convenience.** Of course our ideal biometric should be easy and convenient to use. The present author encountered this issue when trying to use iris recognition at Heathrow Airport. The technology used there demands that people remove their glasses; unfortunately for the very short sighted, this makes the “target area” impossible to see. Several minutes spent trying and failing to get aligned results only in frustration.
- **User acceptance.** There are a number of reasons users may resist a biometric technique:
 - Privacy concerns. For example, worries that it might lead to remote tracking. A biometric that cannot be read from a distance (unlike face, voice, iris) is preferable.
 - Hygiene issues – applies to contact techniques such as fingerprint.
 - Safety concerns. If my car starts only with my fingerprint, then thieves might chop off my finger. Fanciful? It happens^[5].

1.3 A compromising position

All of the standard biometrics have issues in one or more of the areas listed above. A biometric that shines in one area will be a let-down in another.

This ensures that the choice of biometric for a particular application will be a compromise: typically a compromise between security and practicality. Often this compromise will be uncomfortable, and getting the compromise wrong will inevitably lead to the failure of a biometric project.

So the question remains — is there a biometric technique that is able to perform in all of the areas listed above, naturally limiting the need for compromise?

2. Introducing Finger Vein Recognition

2.1 Ticking the boxes

In answer to this question, this paper introduces a new form of biometric developed by Hitachi: *finger vein recognition*.

Although, no doubt, not perfect, the use of finger vein patterns as biometric identifiers goes a long way towards ticking all the boxes, as shown in Table 1.

	Security		Practicality				
	Anti-forgery	Acc-uracy	Speed	Enroll-ment	Conven-ience	Cost	Size
Fingerprint	X	●	●	X	●	✓	✓
Iris	●	✓	●	●	X	X	X
Face	●	X	●	●	✓	X	X
Voice	●	X	●	●	✓	●	●
Finger Vein	✓	✓	✓	●	●	●	●

Key: X Poor, ● Average, ✓ Good

Table 1 Qualitative Comparison of Major Biometric Methods

Hitachi's finger vein technology meets the anti-forgery requirement by being an *internal* biometric, invisible except under very special conditions. It also ensures the presence of live blood vessels, further raising the barrier to forgery.

The accuracy requirement is met because, under the correct illumination, finger vein patterns are clear and distinct. There is a high degree of variation between patterns, which underpins their uniqueness. In addition, finger vein patterns remain constant throughout the adult years. See section 3 below for some actual test data to demonstrate the accuracy claims of the finger vein technique.

Furthermore, the accuracy of finger vein recognition is relatively insensitive to extraneous factors such as dirt, sweat or grease on the finger, or surface injury. It is even possible to use the method while wearing latex gloves, which adds greatly to its convenience in specialised settings.

Finger vein recognition is fast, and, as long as a finger is available, has no enrolment problems. Its convenience is similar to that of fingerprint – it involves simply placing the finger on a scanner.

Perhaps most significantly in today's commercial market, the cost-effectiveness is excellent: finger vein technology can deliver a disproportionately high accuracy when compared to its cost.

In every respect, then, finger vein recognition appears to be a good candidate for an ideal biometric identifier.

2.2 Origins

Finger vein recognition technology arose out of Hitachi's extensive research activities in the area of medical scanning. While studying infant brain activity, researchers found that changes in blood flow could be monitored using high-intensity near-infrared light.

As this technology was developed it was found that each individual's vein pattern is unique, and thus could provide a useful biometric identifier. Further research led to the development of finger vein pattern recognition as a practical biometric authentication technology for the commercial market.

After eight years of research and development commercial application of finger vein technology began in 2005 in the form of ATM end-user verification. Finger vein recognition is now in use in 75% of bank branches in Japan making it by far the market-leading biometric technique in that sector.

Finger vein readers are now available in a variety of formats, with devices suitable for both logical control applications such as PC Login and Single Sign On, and physical applications such as door entry control.

2.3 Technology

2.3.1 Obtaining the image

Finger vein recognition works by shining invisible near-infrared light through the finger. The infrared light is absorbed by the haemoglobin of the blood in the veins. The result is an image of the unique pattern of veins which can be captured by a sensor placed below the finger. See Figure 1.

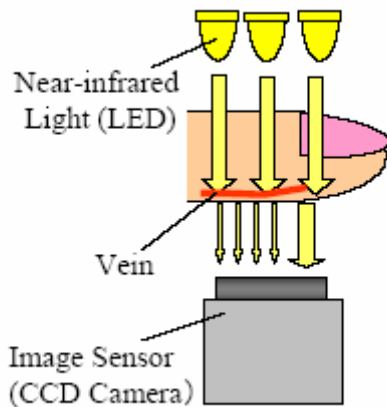


Figure 2 H-1 FV reader

Figure 1 Capturing the finger vein pattern

Since haemoglobin strongly absorbs infrared light, the best images are obtained by shining light *through* the finger. In Figure 1 the light source is placed above the finger, with the sensor below. A practical device in this form-factor is Hitachi's H-1 reader, designed for PC logical access applications (Figure 2 – the H1 reader).

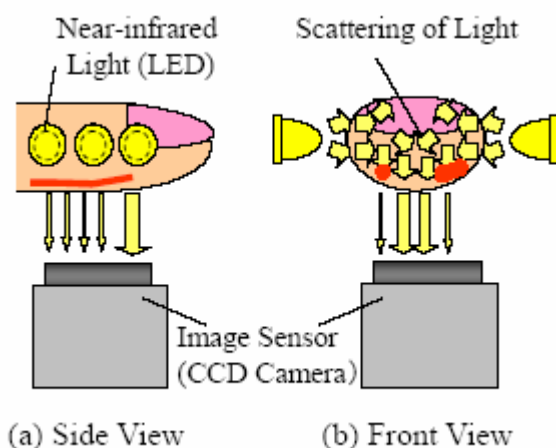


Figure 4 Embedded FV reader

Figure 3 The side-illumination technique

For many applications, however, users would prefer simply to place their finger onto the device rather than into it, in which case illuminating from above becomes a limitation. Hitachi has ad-

dressed this issue by developing a “side-illumination” technique (Figure 3). This technique combines the advantages of using transmitted light with the advantage of having an open, convenient device. A device in this form-factor is Hitachi's embedded reader, which is suitable for incorporating into a wide range of applications (Figure 4 – the embedded reader).

To enable the finger vein device to cope with a wide variation in finger size and operating environment the light source intensity is adjusted adaptively. This enables the optimisation of image contrast and detail, and the minimisation of noise — an important issue due to the very high sensitivity of the image capture CCD.

2.3.2 The authentication process

There are four stages in finger vein authentication. These have analogues in most biometric techniques:

1. Capture of the finger vein image pattern
2. Normalisation of the image
3. Feature pattern extraction from the image
4. Pattern matching and outcome decision

Figure 5 shows a block diagram of these stages. In stage 1 the sensor captures finger vein images, as described above, and passes them to the CPU memory. The CPU in turn dynamically adjusts the brightness of the infrared LED to optimise the image quality.

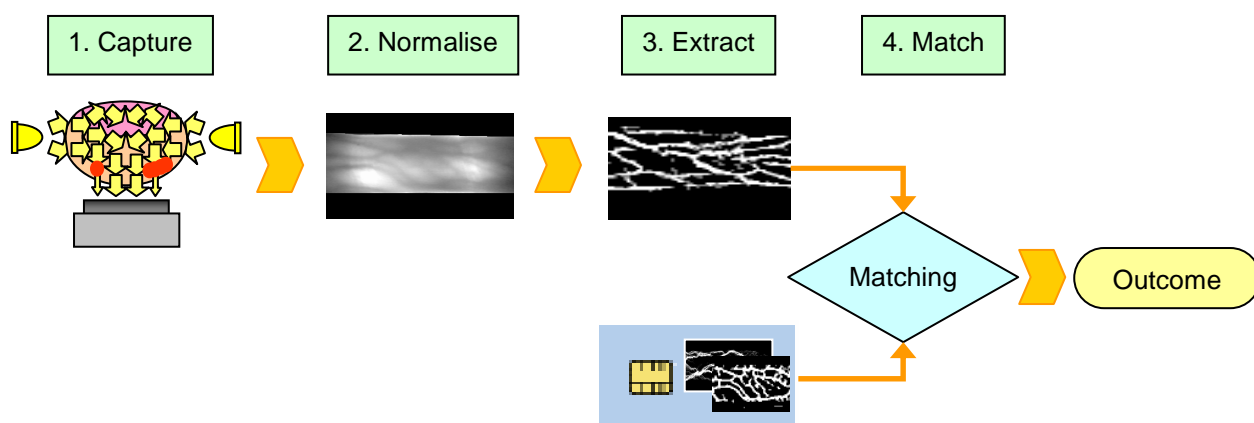


Figure 5 Block diagram of finger vein authentication

In stage 2 the finger vein image is normalised to accommodate geometric changes in position or angle of the finger. This is done by detecting the outline of the finger in the image, and rotating the entire image to normalise the slope of the outline.

Distinctive features of the finger vein pattern are extracted in stage 3. This is an essential step for eliminating variations in the captured data due to changes in body metabolism or imaging conditions. The result is a standard finger vein template of approximately 400 bytes which is suitable for passing to the matching algorithm.

In stage 4 the captured finger vein template is matched against a previously stored reference template. If a sufficiently close match is found then the user is authenticated.

In the example above, the reference template is stored in a smart card. If a capable enough smart card is used then the matching can take place on the card itself. This enhances security since the

reference template never leaves the card. Alternatively, the reference templates can be stored in the finger vein device itself, on an attached PC, or elsewhere on the network.

3. Comparison between biometric methods

3.1 Accuracy comparison

As discussed above, accuracy of a biometric method is crucial to both its security and practicality. The ideal biometric will rarely reject an authorised individual (low false rejection rate, FRR) and rarely accept an unauthorised individual (low false acceptance rate, FAR).

The International Biometric Group^[6] undertakes independent testing of biometric devices and makes the results available. Table 2 compares accuracy results from a number of different biometric methods^[7]. For clarity, the data are also plotted in Figure 6.

	Finger Vein	Palm Vein	Iris	Fingerprint	
Manufacturer	Hitachi-Omron	Fujitsu	IrisGuard	Precise Biometrics	Bioscrypt
Device	UBReader	PalmSecure	H100	Precise100MC	Lifeview
Failure to Enroll (FTE, two samples)	0.55%	1.63%	7.01%	3.73%	0.00%
False Rejection Rate (FRR)	1.26% (N=11,341)	4.23% (N=21,867)	1.76% (N=19,389)	6.47% (N=232)	1.67% (N=239)
False Acceptance Rate (FAR)	0.01% (N=14,368,975)	0.0118% (N=27,834,104)	0.01% (N=23,764,127)	5.83% (N=480)	1.46% (N=478)
Device accuracy setting	FMR 0.01%	Default threshold	FMR 0.01%	FRR: Middle FAR: Low	FRR: Middle FAR: Low
Test time	CBT-6 (2006)	CBT-6 (2006)	CBT-6 (2006)	CBT-5 (2003)	CBT-4 (2002)

Note: In CBT-6 FRR and FAR are not evaluated directly, so results quoted are "same day" attempt level of FNMR and FMR respectively

Table 2 IBG Comparisons of the Accuracy of Biometric Techniques

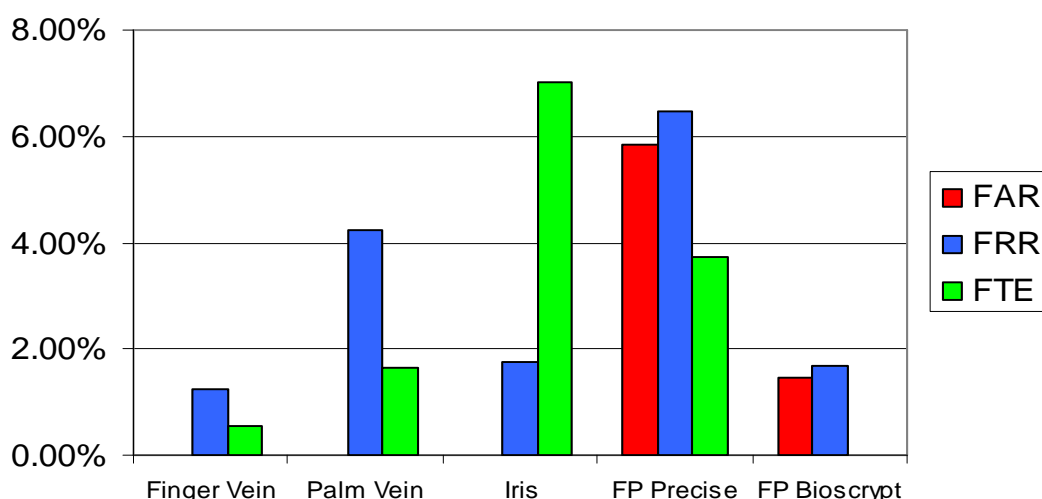


Figure 6 Comparison chart of FAR, FRR and FTE across biometric techniques (IBG)

The IBG results have been obtained in test situations designed to mimic reality to some extent, and demonstrate that vendors' catalogue claims about FAR and FRR ought to be taken with a pinch of salt — those are obtained in controlled laboratory conditions and bear little relation to real life installations.

For the non-fingerprint technologies, the false acceptance rates are tiny; but both of the fingerprint technologies show significant false acceptance rates. A FAR of 5%, say, means that there is a one-in-twenty chance that a random individual, possibly malicious, will be authenticated. Clearly, a device with this characteristic is suitable for only the lowest security applications. Fingerprint vendors are obviously aware of this: as a workaround they have begun to introduce multi-finger authentication^[8]. This may increase security, but at the expense of decreased convenience and increased false rejection rate.

The false rejection rate (FRR) is a usability issue, as is the failure to enrol rate (FTE). The Hitachi finger vein device shows the lowest FRR of all the methods, and the lowest FTE of all but the Bio-crypt fingerprint.

3.2 Finger vein and palm vein

The reader may be aware that Hitachi's finger vein recognition is not the only vein-recognition technology on the market. A palm vein recognition device is also available from Fujitsu. How do these devices compare?

One of the key differences is that the palm vein reader relies on *reflected* infrared light rather than the *transmitted* infrared light that finger vein uses. As described above, the Hitachi finger vein method relies on shining light *through* the skin. There are three reasons why the transmitted light technique can be expected to provide higher accuracy:

- When using reflected light, the skin's high reflectivity dramatically reduces the image contrast. Since haemoglobin absorbs infrared light, the use of transmitted light in the finger vein device allows the capture of high contrast images, which are much more suitable for further processing by the matching algorithms to give an accurate match.
- Reflected light penetrates only a shallow way under the skin; the use of transmitted light permits the capture of much deeper vein patterns.
- Reflected light is susceptible to noise in the form of dirt and roughness of the skin. The transmitted light technique has some tolerance to these.

In addition, the amount of data collected by palm vein is greater than that collected by finger vein, which presents a challenge to the matching algorithms. To see the effect this has on the matching times, consider the following data from the IBG CBT-6 report^[7]:

	Hitachi Finger Vein	Fujitsu Palm Vein	IrisGuard Iris
Median recognition attempt duration (s)	1.23	2.13	4.22
Median enrolment duration (s)	33.3	61.7	44.5

Table 3 Recognition and Enrolment timings from IBG CBT-6

The third key difference between the palm and finger vein techniques is the size of the device necessary to capture the images. A device that scans the entire palm will inevitably be larger than a device that scans a single finger.

4. Conclusion

An ideal biometric solution must satisfy many, often competing, criteria. All previously proposed biometric identification methods present a compromise in one or another area of security or practicality.

Hitachi has developed a novel technology around finger vein recognition. This finger vein technology has inherent properties that enable it to perform well in all of the areas that matter, both in security and practicality. Although novel, this technology has been proven with extensive use in applications in Japan.

It has been shown both qualitatively and quantitatively that finger vein recognition combines the convenience of finger print with an accuracy as high as, or superior to, iris and palm vein. Above all, it is cost-effective.

Practical devices are now available for both logical and physical security applications. Finger vein recognition has a compelling claim to being an ideal biometric for a wide range of purposes.

5. References

1. Doubt cast on fingerprint security <http://news.bbc.co.uk/1/hi/sci/tech/1991517.stm>
2. Eye scan school opens doors <http://news.bbc.co.uk/1/hi/england/wear/3115428.stm>
3. Eye scanner project is scrapped <http://news.bbc.co.uk/1/hi/england/tyne/3652638.stm>
4. UK Passport Service Biometrics Enrolment Trial
http://www.passport.gov.uk/downloads/UKPSBiometrics_Enrolment_Trial_Report.pdf
5. Malaysia car thieves steal finger <http://news.bbc.co.uk/1/hi/world/asia-pacific/4396831.stm>
6. The International Biometric Group: <http://www.biometricgroup.com/>
7. Full test reports available from the International Biometric Group
http://www.biometricgroup.com/reports/public/reports_and_research.html
8. See, for example, <http://www.fingerpin.net/>: "fingerPIN enables secure access and verification through the use of a sequence of fingerprints, not just one."

6. Further Information

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

Website: <http://www.hitachi-eu.com/veinid>

Email: veinid@hitachi-eu.com

Telephone: +44 (0)1628 585581

Address:

Hitachi Europe Limited,
Whitebrook Park,
Lower Cookham Road,
Maidenhead,
Berkshire. UK.
SL6 8YA