A Computer to Check Signatures

R. S. Watson and P. J. Pobgee

A growing need to check people's identity automatically — as a safeguard against crime — has led to the development of a computer that verifies signatures by the speed and sequence of pen movements as well as by the finished sample.

Modern technology has, ironically, increased the opportunities for crime and its rewards. Easier and more widespread facilities for getting goods on credit and the introduction of electronic fund transfer systems have made it possible to make money directly by fraud.

Nowadays, too, there are many places where people cannot be allowed to enter unless they are authorized. These may house stocks of valuable or dangerous material or stores of confidential information, often in the form of computer records. Providing guards to check people's identity costs a lot of money so there is a need now for some automatic system of checking that people are, indeed, who they are supposed to be.

There are two ways of tackling the problem. First is the method of providing tokens, such as credit cards or pass cards or even secret codes. But, of course, tokens can be lost or stolen and, on occasions, lent to other people. The second method is to make use of some human property such as fingerprints, body weight, or other physical dimension. Unfortunately, people often object to such things being used. In any case, measurement can be expensive to automate, and together with voice prints these visible attributes can still be imitated.

Pen Movements

Signing is the traditional method for authorizing documents, and signatures represent a well practised human behaviour pattern. In the Computer Science Division at the National Physical Laboratory (Teddington, England) we realized that, although the visible

mark can be easily copied or traced, the way in which it is written is also characteristic of the writer. This means that additional information can be obtained by measuring the speed and sequence with which the pen is moved across the paper.

It followed that in any automatic system for recognizing signatures as they were written the first requirement was for an economic way of obtaining this hidden information without upsetting the writer's natural rhythm. This was obtained by inventing a simple electronic notepad that produced a sequence of electrical signals corresponding to the signing action without being connected to the writer's pen. This pad has been further developed commerically and is marketed by Quest Automation (Dorset, England) as a data entry device under the name Datapad.

The second stage was the study of a great number of signatures to choose a method of measurement that could ignore minor variations between samples from the same writer, while preserving his distinguishing features. Over 10,000 signatures were collected from more than 500 writers from all walks of life. When we examined these with a view to isolating the variables, four rather obvious factors emerged. These were *name*, *style*, *context*, and *noise*.

The *name* forms the basic structure. It may be short, such as B. Nye, or long with 30 letters or more — Sir Frederick Marmaduke Bertwhistle. The name may be written in different languages or scripts such as Russian, Arabic, Japanese, Hebrew, or for that matter any well practised group of symbols. In some cases a person's initials are acceptable.

By *style* we mean the variations about the name form. Many people have a repertoire of styles which they use on various occasions. A number of common examples which we met were a "working or everyday use" style, a "cheque book" style and what might be called an "impress the boss" style.

Context is the modification to a given style caused by what the individual is doing at the time. The rhythmic properties of a person's signature can vary according to his attitude to the transaction. The signing of an important document will affect the way he writes more than a trivial event such as the receipt of articles worth a few pence.

All the other influences that may affect the signing behaviour we have called the *noise* factor. The weather may be included in this category and a number of signatures were collected from peo-

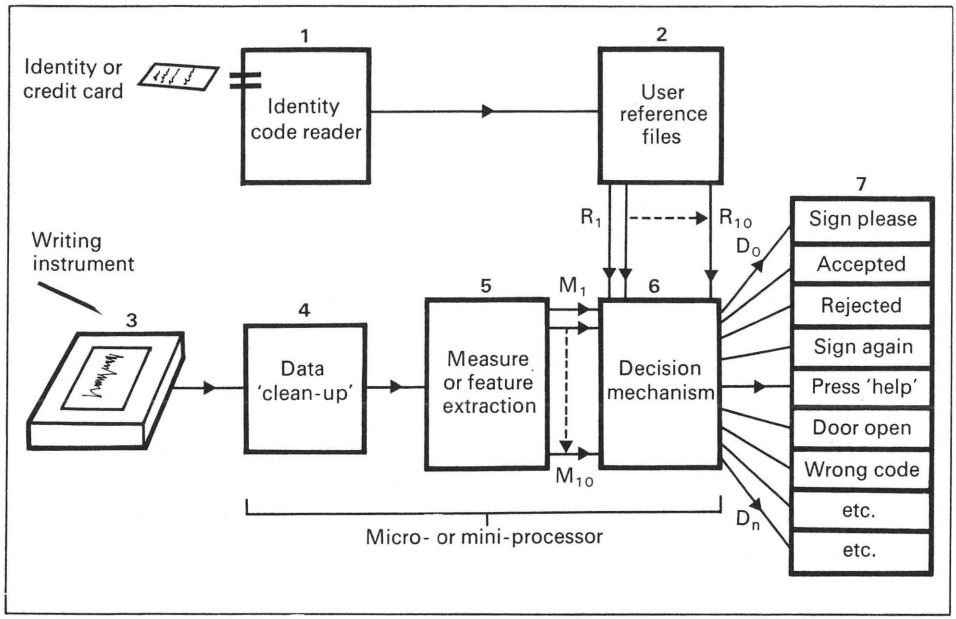


Diagram 1. Basic signature validation machine.

ple arriving at the laboratory in midwinter. Other samples were obtained from people in various states of health. In one case drugs were being taken to alleviate the symptoms of a nervous condition. Then, of course, there is always the "after business lunch effect" which can influence the signing rhythms!

Our large data bank of signatures was supported by other experience from NPL research into interaction between man and machine. This enabled a team led by J. Parks of NPL to develop powerful techniques to overcome many of the difficulties.

Peter Hawkes of the UK's National Research Development Corporation and Stephen Dennis of Inter-Bank Research Organisation had been following our progress with interest, and a joint venture was formed between NRDC, IBRO, and NPL to construct a prototype machine for VERIfication of SIGNatures (VERISIGN).

Diagram 1 illustrates the basic building blocks of the Verisign machine. A user first enters his personal identity code either through keyboard or badge reader (1). The code, which in our case is a four digit number, is used to extract the user's reference file (2) containing a set of ten reference parameters (R1-R10). These are passed to the decision mechanism (6) and a request flashed to

the output display (7) for the person to sign his name on the notepad (3).

The notepad has an electro-sensitive surface on which movements of the writing stylus are converted into a string of interleaved x, y co-ordinates. This data string is then processed (4) to remove artifacts such as marks made accidentally by the user.

Analysis of the cleaned up data occurs at (5) in which measurements are made on certain properties which characterize the signing pattern. Examples of possible measurements are the number of crossings made by the x or y co-ordinates over a datum line or the total time spent in writing. Many other functions of position and time may be chosen.

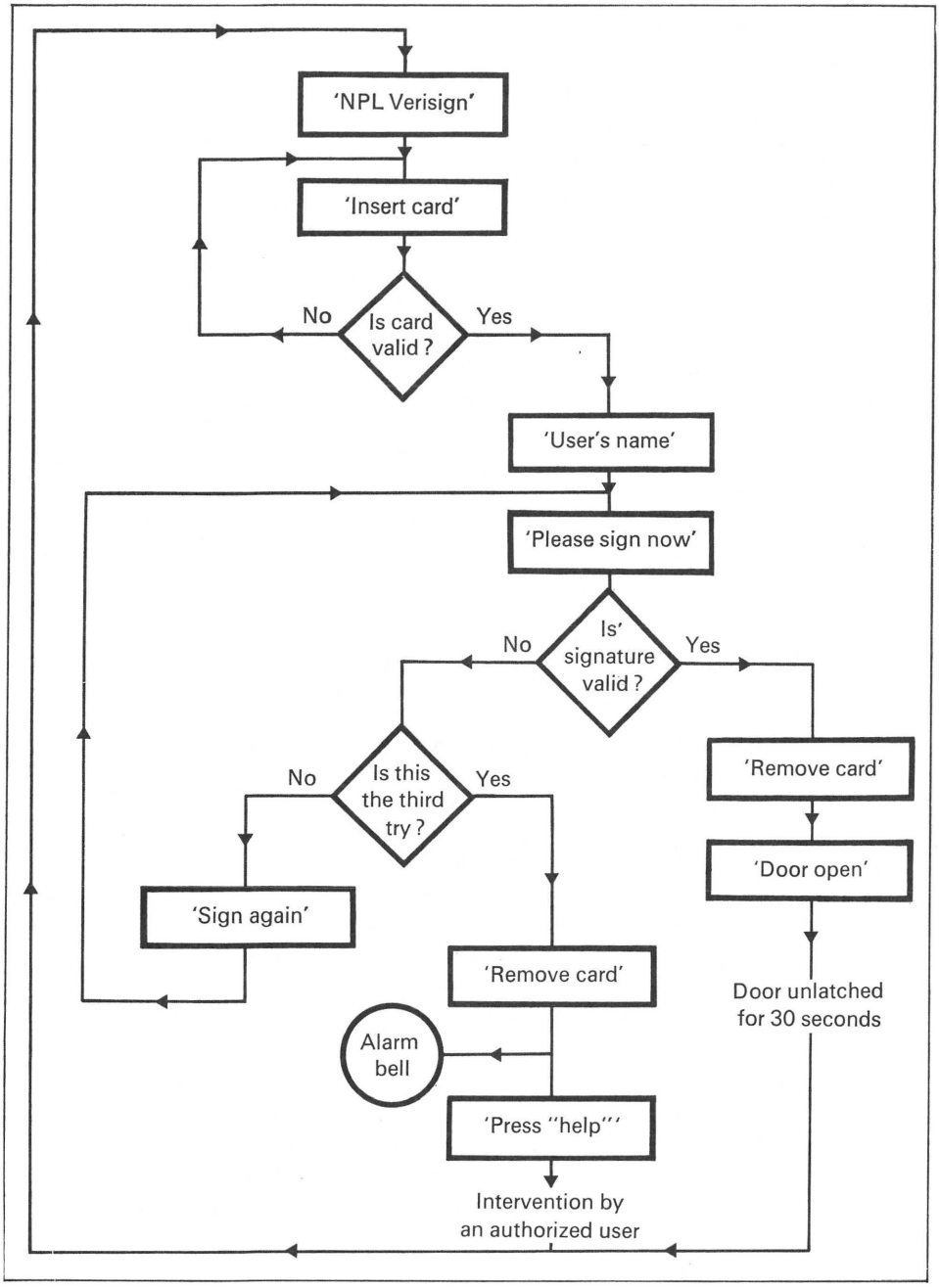
The properties or parameters can be selected locally, that is within certain areas, or globally, with the measurements taken over the whole signature.

Over 100 measures were tested for their ability to discriminate between writers, while remaining insensitive to each person's own variation. From these ten measures were selected and used to generate the values M1-M10 which are passed to the decision mechanism (6). Here a comparison is made with those obtained from the claimed reference set (R1-R10). The degree of similarity or closeness of fit in relation to a set threshold value determines one of number of decisions (D1-Dn). A close fit, that is below the threshold value, is accepted. A poor fit causes the signature to be rejected and displays a request for further samples.

A heirarchy of decision procedures is used allowing context factors such as customer importance or the value of the transaction to be incorporated. The decision mechanism can be easily organized in a number of different ways to suit individual requirements.

Establishing a set of measures to use as a reference for one person is a vital part of the smooth functioning of the machine. Security against impersonation, without the rejection of genuine attempts, will depend on how well the reference measures characterize the writer.

Anyone who will be using the machine is first asked to submit five specimen signatures. The spread of this group is then examined by the machine for any gross inconsistencies. Signatures that lie outside a given tolerance band are rejected and further samples requested to make up the number. The variation in the reference group (variability factor, VF) provides a useful means of assessing what the chances are for successful impersonation by


'NPL Verisign'
'Insert card'
No
Is card valid ?
Yes
'User's name'
'Please sign now'
No
Is' signature valid ?
Yes
No
Is this the third try ?
Yes
'Remove card'
'Door open'
'Sign again'
'Remove card'
Door unlatched for 30 seconds
Alarm bell
'Press ''help''
Intervention by an authorized user

unauthorized users. The lower this factor the higher the security and, of course, the reverse is true.

Knowledge of the degree of security is unknown to either the user or impersonator, and in any case the rating value together with the reference list is updated each time a test signature is accepted. This updating mechanism can also keep track of long-term variation in the way a person writes his signature.

The basic flow chart of the Verisign machine is shown in Diagram 2. Three attempts at writing a signature are permitted before some form of alert is given.

The computer program, apart from a few modules, is written in standard Fortran IV language and occupies about 12,000 words of core store. 20 words are required for each person's reference parameters plus an extra 10 for performance logging.

We used a 16k mini-computer which provided reference file space for up to 120 people. The time to verify a signature was less than 100 milliseconds. This meant that a complete transaction, including the entry of a personal identity code, could be completed inside 20 seconds.

Tests

The system was tested in various situations including remote operation over public telephone lines. In addition, two full-scale experiments were carried out. For the first, in the entrance hall at our laboratory, the participants identified themselves as they entered and left the building. The 71 people who took part included typists, security officers, members of the services, professional engineers, and scientists. Out of 2,000 attempts made at identification by signing, 96% were successful.

The second experiment controlled entry to the computer room of a different government establishment. Here, the 47 passholders, often carrying equipment or trays of cards, used the Verisign terminal over a period of several weeks. The results of this experiment were similar to the first.

It is, of course, one thing to ensure that the genuine person is identified correctly with the minimum fuss or bother. It is another to prevent the less scrupulous artist practising his art! With this in mind, at the end of both experiments we displayed a number of

Diagram 2. Simplified flow chart of operations.

target signatures and invited everyone to try his hand at copying them. With the first experiment at NPL, although one or two came very close, no-one was able to obtain a "signature valid" signal. A lower threshold was used for the second experiment and the decision scores were displayed as an incentive. No limit was placed on the number of attempts allowed and under these less rigorous, unrealistic conditions a few people were eventually successful.

No security system is perfect but the hierarchy of this one allows the degree of security to be balanced against the possibility of rejecting an authorized user.

Reprinted with kind permission from *Spectrum*, Number 138, 1976, pp. 12-13.