Strategies for exploiting signature verification based on complexity estimates

M. C. Fairhurst and E. Kaplani

Department of Electronics,
University of Kent,
Canterbury, Kent CT2 7NT

1. Introduction

Biometrics is a diverse and increasingly important field, covering many modalities and types of individual characteristics. The biometric modality with perhaps the longest history, and one which certainly enjoys the widest degree of public acceptance, is the handwritten signature [1]. However, checking and analysing handwritten signatures as a means of establishing or verifying identity is both a challenge for technology (i.e. algorithms for robust *automatic* signature verification are constantly sought) and for the powers of human perception, since there are many situations where signature checking by machine might be inappropriate or, at least at present, insufficiently reliable, for routine use. This is especially the case when the risk of forgery is high, or where acceptance of a non-authentic signature could have serious consequences. Furthermore, it can reasonably be claimed that a better understanding of human ability in analysing and authenticating signatures can lead indirectly to the specification of more accurate and perhaps more robust techniques which can be implemented automatically.

This paper will report on some important aspects of our work in the field of signature verification and, in particular, addresses some important issues relating to the human and machine identification of signature imitations/forgeries. We can envisage the handwritten signature playing a key role in two related broad scenarios. First, human checking (by direct visual inspection) is still a common means of determining/confirming identity or authorising transactions, and the pervasiveness of this type of activity should not be underestimated. Secondly, there is an increasing need for *automated* (machine-based) verification of the handwritten signature (e.g. in electronic sign-on systems, or where improved objectivity and accuracy, such as in point-of-sale applications, is at a premium). It is this continuing need for both human and machine-based signature verification which provides the focus for the work reported, addressing issues concerning the form and structure of the signature in relation to the reliability with which genuine and fraudulent samples may be distinguished.

2. Signature characteristics and signature complexity

Signatures and signing styles can differ significantly, both within samples from the same signers, but self-evidently to a very large degree across a population of signers, and the susceptibility of a signature to false imitation is clearly a function of the nature of the signature itself. This paper reports specifically on some experiments in human signature analysis.

Five writers were selected to use as reference or target signers, whose signatures were of varying length, number of strokes, and with differing degrees of embellishment in signing execution. The aim was to generate five target signature groups which could intuitively be expected to have a wide spread of “complexity” in visual appearance. A group of 36 subjects were then presented with a sample from each of these groups and asked to assign a score to each sample (on a scale of 1 to 10) to indicate its perceived degree of complexity. Even this simple data will be shown to be revealing, since it demonstrates that, while at the extremes of the scale there is a modest spread in the perceived degree of complexity, with a relatively sharp “cut off”, the intermediate signature samples appear to be much more difficult to assess and categorise quantitatively. This, in itself, represents an interesting problem which supports the notion of the desirability of some more objective or algorithmic means of analysing samples if complexity is to be considered for practical exploitation in increasing the robustness of signature checking procedures. More important, however, is to consider the implications of complexity in relation to the susceptibility to compromise of an individual signature model.

In order to investigate this aspect of signature perception, in a further experiment subjects were asked to view a range of signatures for each of the sample groupings, some of which were genuine samples and some of which were forgeries (generated in a separate experiment with a disjoint set of subjects who produced the imitations from a visual inspection of a genuine sample). In total each subject viewed 10 genuine and 10 forged samples from each of the five target groups. Each subject was asked simply to classify each sample as "genuine" or "forgery", in comparison with a genuine sample which was in view simultaneously, as would be the case, for example, in checking a signature against a "model" written on the back of a credit card.

We will show how an assessment of the relation between perceived complexity and the likelihood of errors in judging sample authenticity can lead to two (essentially opposing) hypotheses. On the one hand, it could be predicted that low complexity leads to ease of imitation and therefore potentially higher FAR. On the other hand, an alternative supposition might be that higher complexity makes imitation more difficult, and therefore more flexibility in assessment, leading to more errors in perceived authenticity, might be expected. Although the former hypothesis was the more popular among subjects tested, it is the latter hypothesis which is supported by the results of our study, as will be described in our presentation.

3. Discussion and conclusion

It is known that measures of signature "complexity" can be defined and computed objectively and algorithmically, and the relations between some of these measures, the assessed similarity between test and target samples, and their likelihood of correct authentication have been explored, particularly from the point of view of "expert" analysts [2]. However, our study shows the nature of the problem to be confronted in routine situations where human signature checking is required. It also points to the value of devising an inspection protocol which could be adopted where human evaluation for authentication is necessary, where the procedures which may lead to greatest security and reliability may be seen as to some extent counter-intuitive. Strategies for human authentication may therefore benefit from a clearer understanding of the elements of complexity and, indeed, other features of a signature model which better reflect a justifiable confidence in judging authenticity.

Finally, there is an important issue raised here connected with a much more important question for the future, relating to the potential for the introduction of automated signature verification, since evaluations based on human perception and machine-based processing do not necessarily coincide, and the relations between the form and complexity of signature samples, human perception and interpretation, and algorithmic signature processing require considerably more investigation.

These distinctions may be very important in developing appropriate support for signature checking in different applications and different operational environments. This may especially be the case where automated systems and human intervention are likely to be integrated, a scenario which is likely to become increasingly common in practice. The results presented here therefore identify some important elements in a strategy to support improved human-machine interaction in relation to biometric identity checking.

4. References

1. Fairhurst, M.C. (1997). Signature verification revisited: promoting practical exploitation of biometric technology. Electronics and Communication Engineering Journal, 273-280.
2. Brault, J-J. & Plamondon, R. (1993). A complexity measure of handwritten curves: modeling of dynamic signature forgery. IEEE Trans. Syst. Man Cybern., Vol. 23, No. 2, 400-413