An assessment of dynamic signature forgery creation methodology and accuracy

Luiz Felipe Belem de Oliveira, Richard Guest

An assessment of dynamic signature forgery creation methodology and accuracy

Luiz Felipe BELEM DE OLIVEIRA and Richard GUEST
School of Engineering, University of Kent, Canterbury, Kent, UK, CT2 7NT
r.m.guest@kent.ac.uk

Abstract. Signatures provide a convenient and widely accepted method of authentication, however they are prone to attack by forgery. This can be mitigated to an extent by analysing both the static and dynamic biometric aspects of construction, however the possibly for accurate forgery from a static image of a genuine signature still exists. In this study we explore initial forgery accuracy of a range of genuine signatures and how accuracy changes as a forger receives feedback from a commercial signature engine in terms of a 'match score'. We also explore the effects of genuine signature complexity on forgery performance alongside the image size of the genuine signature to be forged. Our results show that forgers are able improve performance over time on simple signatures (including those with less pen travel distance) and that a magnified genuine sample enables more accurate forgery for these class of signatures. More complex signatures result in lower forged verification scores and irregular patterns of improvement across the five forgeries. Overall verification match scores were typically less than 80% for most attempts regardless of signature complexity, thus indicating the resilience of dynamic systems to unskilled forgery attempts.

1. Introduction

Signatures are a widely used form of behavioural biometric authentication. They have the advantage over other biometric modalities as being an acceptable and pervasive form of identification, being legally admissible in terms of formal authentication and exhibit intentional ceremony in sample donation (Impedovo et al., 2008). Most signature samples are written directly on a sheet of paper (or other signing surface) using a pen and are checked/verified by human inspection of the completed signature. This *static* form of assessment may be automated in a computer-based analysis using image processing and measurement techniques (Chapran et al. 2008). Conventional computer-based signature biometric systems use a combination of these static assessments and *dynamic*, or temporal, elements of signature construction. To enable a dynamic analysis requires the collection of signatures on a tablet device that samples pen position (and other data) at regular intervals. It has been shown that verification performance can be enhanced by combining both static and dynamic features (Jain et al, 2002). Signature however does have the disadvantage that samples can be relatively easy to forge, particularly in the static form. Very often a forger will be able to access a static image of the signature being forged whilst the learning process occurs, providing the ability to study both the shape of the signature and also to infer dynamic aspects of the signature construction such as stroke order, pen pressure and speed (Guest et al, 2009).

Assessing the forgery creation process using a dynamic method allows us to see how a forger adjusts production to achieve more accurate results in terms of a closer match to a genuine signature. In this study we assess how forgers modify their forgery behaviour given a static model of a signature and dynamic feedback on the forgery score between attempts. By using a number of source signatures of varying complexity it is possible to identify a) the dynamic performance at an initial forgery attempt, b) the effect of complexity on the ability to form an accurate forgery and c) how dynamic performance changes as feedback is provided. Feedback is only given in the form of an accuracy match score, without information such as velocity or pressure profiling, thereby replicating a conventional dynamic forgery scenario. Furthermore, by using a magnified genuine static sample as a model, we can assess the effect of physical sample size on forgery performance.

2. Methodology

The initial stage of the investigation involved obtaining a series of genuine source signatures that were used as models for forgery. Nine subjects agreed for their signature to be used for this purpose. Each of the nine subjects donated six signatures as dynamic enrolments to a commercial dynamic signature verification server system (which, for the purposes of this experiment, was treated as a black-box system). An internal checking process within the server ensured the stability of the donated signatures in forming an enrolment template. Signatures were captured using a back-projected LCD signature tablet (a Wacom STU-300) that provided virtual ink to the signing process. Signers were also asked to sign on a sheet of paper using a *biro pen* to provide a static signature in a format replicating a conventional pen-on-paper donation methodology. A second stage involved a static signature image from each of the enrolled nine signers providing the source signatures was categorised by 10 independent assessors as being either simple, medium or complex on the basis of 'difficulty to forge'. These 10 assessors were separate from the nine providing the model signatures. Categories were assigned by assessing the modal category given to each signature. Figure 1 shows the finalised categories of each of the source

signatures. The authors' note that legibility of text seems to be the primary driver for assigning to the simple group, whereas complex signatures tend to be symbolic representations of a name and contain a potentially unclear ordering of pen strokes. Assessing the complexity responses there was generally a high agreement between assessors *resulting in a clear modal response for each signature*.

The third phase of the methodology was to assess the forgery performance of a group of subjects (forgers). A total of 15 forgers took part in the experiment. These subjects were not part of the pool of subjects that donated source signatures or took part in the signature complexity categorisation. Each forger undertook the following protocol:

1. Presented with a randomly selected static 'model' image (from the biro-based collection) of a signature from the 'simple' pool, the subject is able to spend as long as they require studying the signature. The biro-based collection was used to replicate the conventional method of finding a signature to forge.
2. The forger tries to forge the signature using the verification system, signing on the STU-300 device.
3. The verification system provides a verification score, based on dynamic and static information, of between 0 (no match) and 100 (maximum matching). The forger used this score to assess their performance and encouraged to improve their verification score indicating an enhancement to the forgery.
4. The forger makes four more attempts, the score feedback being provided for each attempt.
5. Steps 1-4 are repeated for a different randomly selected 'simple' signature but with the 'model' image quadrupled in size, replicating examination under magnified conditions.
6. Steps 1-5 are repeated for two signatures (one normal sized, one magnified) from each of the 'medium' and 'complex' groups.

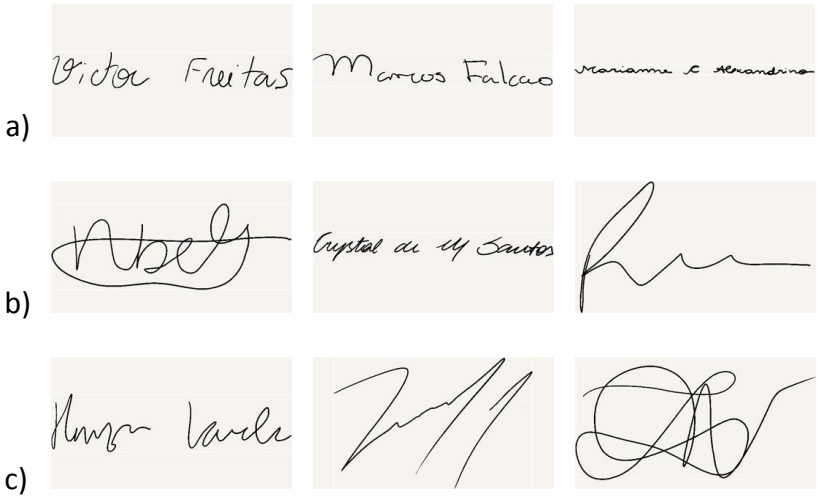

Figure 1: a) Simple 1,2 and 3, b) Medium 1, 2 and 3, and c) Complex 1, 2 and 3 Source Signatures

Results were analysed by assessing the performance of forgers on each of the signatures across multiple attempts and model sizes. The analysis focuses on overall performance in terms of verification thresholds, improvements over time and the effect of signature complexity on ability to forge. Full ethical approval was granted for this study.

3. Results

Figure 2 show the individual verification score results from the three *simple* signatures. In each of the charts the five sequential attempts of the five forgers (F1-F5) that were randomly selected to forge each signature are shown, initially using a standard sized genuine model signature, followed by a magnified model signature. It can be seen that, in most cases, a forger was able to improve their performance across the five attempts. Indeed, examination of Figure 3, which details the average performance for each attempt on each simple signature, shows this improvement. It can also be seen that for two of the signatures (Simple 2 and 3) the large/magnified signature produced a higher performance. The only constant factor that seems to determine match score is the amount of attempts that the forger produces a signature. It is also important to note that in general most forgeries were below a match score of 80%. In imposing such a threshold it is possible to demonstrate the effectiveness of the dynamic engine to distinguish between forgeries and genuine signature even on signatures deemed to be "simple" in complexity.

Figure 4 shows the results of the *medium* signature verification scores, whilst Figure 5 indicates the average performance across the three signature for the two sizes of model signature (note that there was only

four forgery attempts for these signatures). Here it is clear that the best results were obtained when the forger was copying from a real sized model signature. It is also possible to note that, compared to the simple signatures, the average scores related to medium signatures is relatively flat and thus not directly related to the amount of attempts that the forger undertakes. It can also be noted that for Medium Signatures 1 and 3, which have relatively lower ink travel length, the ability to obtain a high verification score (and hence successfully verify on the system) is enhanced. It is seen that an average score is maintained for all the attempts when dealing with a normal size image. However when the forger is viewing a magnified model image, the verification scores are not as stable as when copying from a normal size image. The amount of detail that is shown in a magnified image of a medium signature may affect the way the forger approaches their copy, leading to poorer results.

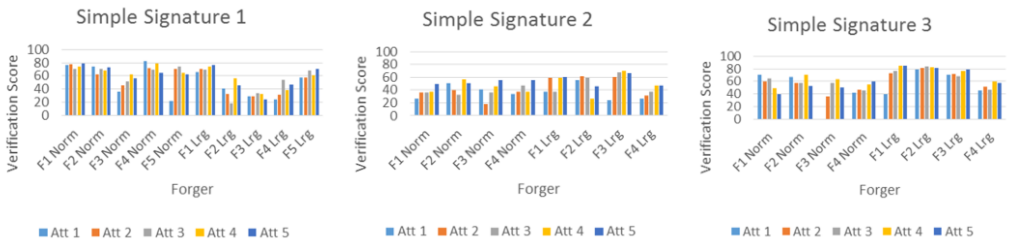

Figure 2: Simple Signature Attempts (Norm=Normal modal size, Lrg=Magnified model size, Att=Attempt)

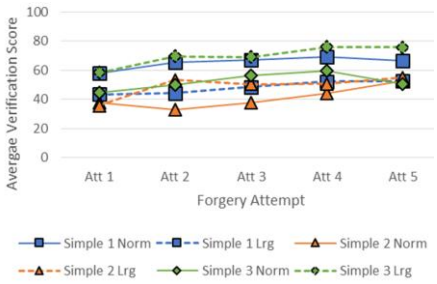

Figure 3: Simple Signatures – Average Verification Score per Attempt

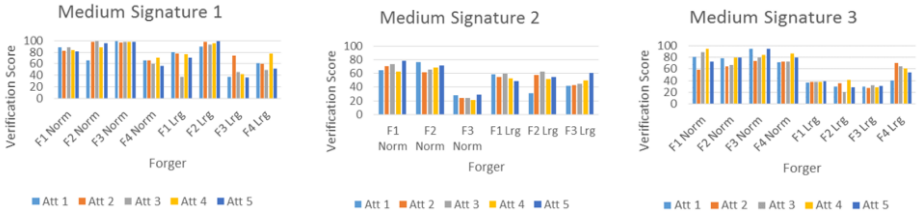

Figure 4: Medium Signature Attempts

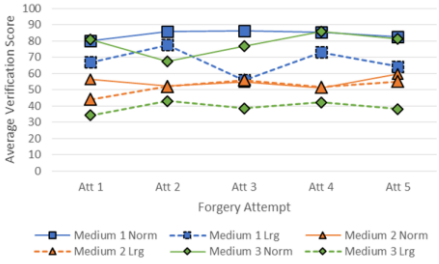

Figure 5: Medium Signatures – Average Verification Score per Attempt

Complex signatures are, in theory, the hardest to analyse and forge. By examining Figures 6 and 7 it can be seen that each signature has its own level of ability to be forged. Assessing the attempts using Complex

Signature 2 it is possible to establish that forgers produce a signature a similar profile to those in the Medium group – indeed this signature contained lower ink travel distance and thus is directly comparable to Medium Signatures 1 and 3. The average scores also vary considerably across attempts indicating that the forger is trying to copy the signature by trial-and-error. Analysing the average scores obtained for Complex Signature 1 the results show that the number of attempts for this signature is not too import, since both graphs indicate little improvement over the five attempts. It is interesting to see that in this case the size of the model signature does not have an effect on performance, as normal and magnified signatures produce interchangeable results. Complex Signature 3 is the hardest to assess. It is possible to see an enhancement of verification scores but the low values associated with these attempts shows the difficulty associated with forging this signature.

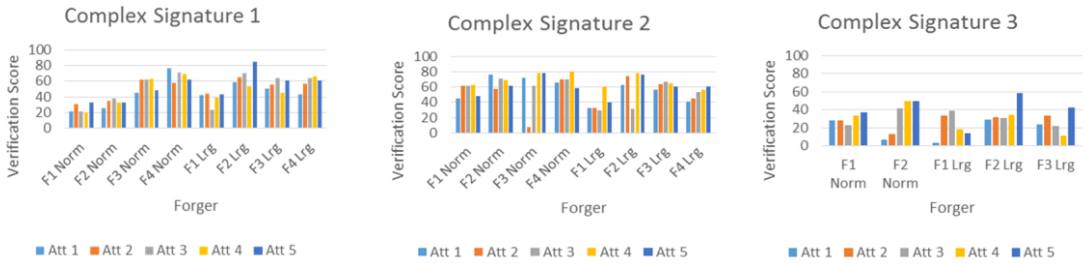

Figure 6: Complex Signature Attempts

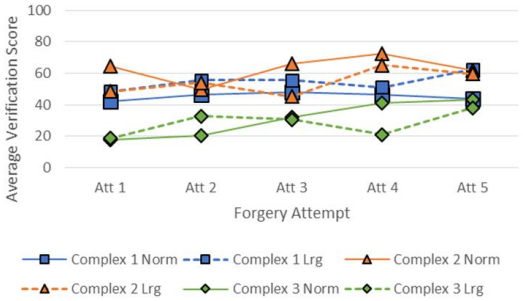

Figure 7: Complex Signatures – Average Verification Score per Attempt

4. Conclusions

The main conclusions from this study are:

- Perceived ease of forgery seems to be related to the readability of the signature.
- Signatures rated as *simple* show improvement across the five attempts with forgers being able to produce more accurate results using magnified images.
- Overall verification match scores were typically less than 80% for most attempts regardless of signature complexity.
- Signatures containing less ink were typically easier to dynamically forge.
- Complex signatures result in lower forged verification scores and irregular patterns of improvement across the five forgeries.
- For more complex signature the size of the source signature does not modify overall performance.

This study has also pointed to unskilled levels of forgery performance which can be incorporated as thresholds within dynamic signature engines. Future work will analyse the dynamics of the changes made by the forgers between attempts to identify patterns relating to perceived accuracy enhancements made.

References

Impedovo, D., & Pirlo, G. (2008). Automatic signature verification: the state of the art. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, *38*(5), 609-635.

Jain, A. K., Griess, F. D., & Connell, S. D. (2002). On-line signature verification. Pattern Recognition, 35(12), 2963-2972.

Guest, R.M, Fairhurst, M.C., Linnell, T, Towards an Inferred Data Accuracy Assessment of Forensic Document Examination Methodologies for Signatures, In Proc. IGS 2009, Dijon, France, September 2009

Chapran, J., Fairhurst, M. C., Guest, R. M., & Ujam, C. (2008). Task-related population characteristics in handwriting analysis. Computer Vision, IET, 2(2), 75-87.