Article

Electronic Signature Forensics

Overview

Excerpts from a report by: William J. Flynn, B.S., D-ABFDE
Handwriting and Signature Examinations, Affiliated Forensic Laboratories, Inc.

Background

Over the past 90 years, forensic document examiners in the US have continuously developed tools and methodologies which allow them to produce highly accurate (and legally accepted) handwriting and signature comparisons. Over this time period, many technological and legal events have affected the forensic community. An example of a paradigm shift in the handwriting world occurred when the writing instrument of choice changed from a nibbed pen (such as a fountain pen) to the ballpoint pen in 1945. Because the ballpoint pen uses highly viscous ink and a non-flexing tip, it produces a writing line with little or no shading (stress). Forensic document examiners in the late 1940's had to adapt their analysis techniques in order to account for the loss of this traditionally important data.

A rapid change to e-commerce and eSignatures will represent another paradigm shift for the forensic community. Because I have been a forensic document examiner for more than 31 years and also have a BS in Computer Science, I have been acutely aware of the need to develop working tools which can be used to provide the same level of confidence in eSignature verification as is now expected in "normal" signature comparisons. My purpose in working with Topaz has been to help develop these electronic signature examination tools.

Scope of the Study

During the course of the study, I visually compared the captured signatures to their original ink versions using SigAnalyze software on my lab's computers. All of the original signatures were examined using magnification loupes and a binocular microscope (also in my laboratory). The purpose of this evaluation was to determine if Topaz Systems' software would provide sufficient information to permit a forensic analyst to authenticate digitally captured signatures by comparing them to either original (non-captured) signatures, other digitally captured exemplar signatures, or some combination of the two.

Results of the Evaluation

Although an original (ink on paper) signature will always provide the best 3-dimensional view of the writing, the actual speed of the strokes can only be inferred in a subjective way. All digital signature captures will also display the captured signature at a lower resolution than could be

seen in an examination of the original signature. The Topaz software, however, provides far more forensically valuable data about the dynamics of the writing than could ever be determined from an examination of the original.

Data is not information. All of the captured data is useless until it is logically organized and analyzed. In order to provide a means of quickly and accurately evaluating the dynamic data, the Topaz software [presents in a unique and patent pending way the segment timing, speed of signature data and] ... the exact sequence of movements made by the author during the original signature execution. In my preliminary testing, I found this system (namely, the representations of signature dynamics and the sequence of movements) to provide a wealth of forensically valuable information.

Forgeries by tracing or simulation take far longer to produce than genuine signatures. These dramatic differences in the dynamics of the forgery samples (made by the undersigned) were immediately obvious in my side-by-side comparisons using SigAnalyze. Even when attempts were made to speed up the forgery process, it was not possible to reproduce the segment timings to coincide with those in the genuine signatures. The combination of the high sample rate signature captures and the [unique, patent-pending] ... line representations of the segment speeds, made it very easy to detect differences between normal signatures and attempted simulations or tracings.

In general, a forgery can be accurate and slow or fast but inaccurate. The ... [genuine] captured signatures displayed the natural changes in speed which would be expected in normally executed writings. In all of the attempts made by the undersigned to accurately reproduce the subjects' signatures, however, there was far less difference in the segments timings than was true in the natural signatures. This slow drawing effect is a well-known phenomenon in the forensic document community.

Because the forgeries may be attempted as a rapid series of movements (which typically fail to graphically depict the victim's signature style), it is equally important that as high a capture rate as possible be employed in the digitizing process. This captured data must accurately represent the writing shapes, sizes, connecting strokes, and proportions of the original signature. In other words, a forgery which is done rapidly (in the hope of re-creating the victim's dynamic writing pattern) will typically have a much different graphical appearance than a true signature. The high resolution of the Topaz system appears to be sufficient to show these graphical differences between a rapidly-made forgery and rapidly-made genuine signature.

It was not possible to produce a simulation or tracing or a subject's signature which would have both the graphical appearance of a genuine signature and an authentic signature's segment timings.

The beauty of a signature as a form of identification is that it is dynamic, not static. All other proposed forms of biometric identification such as retinal scans and fingerprints rely on the exact matching of fixed data. Signature identification, however, depends upon pattern recognition principles because no two signatures are exactly alike. In my opinion, this may be the single most important reason to use signatures to identify an individual through a computer linkage. Because of the pattern of fluctuations found in a normal signature, any digital signature that is fraudulently captured or stolen can only be used once. The second usage of a "stolen" signature would prove it is non-genuine since it would be an exact (or near-exact) match to a signature used for an earlier transaction. This is in direct contrast to a stolen fingerprint file which would be expected to be exactly the same on each transaction.

William J. Flynn
Questioned Document Examiner

1 Moshe Kam, Gabriel Fielding and Robert Conn, "Writer Identification by Professional Document Examiners," Journal of Forensic Sciences, Vol. 42, No. 5 (Sept 1997): pp. 778-786

Editor's Comments and Notes:

1. The Topaz SigAnalyze software and SigPlus electronic signature capture system are patented. All rights are reserved. [ ] and ... marks are an indication of editing.
2. Topaz SigAnalyze software is available only to forensic document examiners.
3. Topaz signatures provide both forensic and biometric electronic signature data for analysis. This is very valuable information for handwriting analysis. The Topaz system records the original electronic signature that was converted at a high sample rate utilizing patented hardware tablets and patent-pending methods for highly accurate measurement of time associated with each point. With Topaz, biometric measurements can be made at any time from the original forensic data.
4. Some electronic signature capture systems discard the original data through a 1-way transformation and record only summary biometric measurements at the point of signature capture. This provides limited information to the document examiner. Topaz recommends the use of the SigPlus ActiveX control for electronic signature capture to ensure that you are not losing valuable data.