Parascript Automatic Signature Verification

December 2010:

Signature Authentication Techniques for the Information Age

Environment

Over 2000 years ago, Aristotle noticed the connection between handwriting and personality. How we make our loops in letters, the alignment of upper, middle, and lower sections of text, our letter spacing, and many other characteristics of writing are inherent in each individual. Accordingly, a signature or the way people write their names is unique and cannot be repeated by others. This phenomenon originated a centuries-old tradition for important documents to be signed as proof of their authenticity. Simultaneously, for centuries visual signature verification served as a reliable and efficient means to detect fraud.

Today the signature is still acknowledged as a principal means of authenticating financial and other business transactions. People use signatures every day to sign checks, to authorize documents and contracts, to validate credit card transactions, etc. The number of signed paper documents has increased tremendously; simultaneously the growth of fraud through forgery has become one of the biggest security problems challenging almost any large modern organization, including insurance companies, banks and other financial and government institutions.

According to recent studies, check fraud costs banks about $1 billion per year with 22% of all fraudulent checks being signature forgeries[1].

Clearly, with 27.5 billion checks written each year in the United States[2], it is not practical or cost-effective to visually compare signatures on the hundreds of millions of checks processed daily. Nor has visual comparison proved to be reliable; many banks have found that due to the high quality of forgeries, many pass through a visual review undetected. Consequently, as the need to guarantee the authenticity of each document remains urgent, this task requires more efficient, controlled, and reliable methods of signature verification.

The emergence of the Internet as a premier growth medium for the new e-business and e-commerce environment has provided modern organizations with another challenge. To keep a competitive advantage they have to do business and conduct commercial transactions electronically, while they are still required to provide positive user identification and guarantee secure authentication of documents that have been filed online. Unlike the trusted handwritten signature, which securely identifies a person in a natural way, passwords, PINs, or "digital" signatures can be easily lost, stolen, shared, or forgotten and are not adequate to provide personalized document authorization, increased privacy and enhanced trust for electronic commerce.

As always with new technology, there are challenges but also many opportunities. This time the answer is in contemporary advances in pattern recognition technology and dynamic biometric

[1] ABA Deposit Account Fraud Survey Report, 2009.

[2] The 2010 Federal Reserve Payments Study.

authentication techniques that allow the trusted method of handwritten signature verification to meet the requirements of the information age.

Automatic Signature Verification

Comprehensive signature verification systems analyze two different areas of an individual's signature: the specific features of a static image of one's signature and the specific features of the process of signing.

The first type includes applications dealing with the two-dimensional static image of the signature resulting from an action of signing that has already taken place. Systems that analyze only the static data of a signature image are called *off-line*.

The second type embraces applications that allow tracking the motion in the process of signing at the point of presentation. Accordingly, systems that treat the signature as a series of movements and can be used with both locally or remotely originated transactions are called *on-line* or *dynamic*.

Off-line Signature Verification

In applications that deal with signed paper documents, the signature's biometric characteristics of motion are unobtainable, and only its static, two-dimensional image is available for verification. This poses a real challenge for developing an automatic solution, especially considering that it has to address not only *random forgeries* that were produced without knowing the shape of the original signature, but also *skilled forgeries*, generated by people who, looking at the original instance of the signature, imitate it as closely as possible. It is a well-known phenomenon that accurate forgeries take far longer to produce than genuine signatures, but speed characteristics are not considered in the analysis. In order to account for the loss of these important data and produce highly accurate signature comparison results, off-line signature verification systems have to imitate the methodologies and approaches used by human forensic document examiners.

Until recently, proposed technology for automated off-line signature verification was not ready to offer an industrially mature solution, which could even match visual verification, let alone surpass it. Especially challenging was the task of detecting skilled forgeries – this is where all existing technologies have failed to offer anything coming even close to visual verification results.

But now there is a solution that detects random and skilled forgeries of signatures with an accuracy that not just equals but far surpasses visual verification.

Parascript® *Signature*Xpert® - A State of the Art Solution for Off-line Signature Verification

The latest achievement is Parascript's award winning[3] *Signature*Xpert – a reliable and cost-effective solution that outperforms both other products and visual verification in its ability to detect signature forgeries. An especially striking advantage over other signature verification technologies is its superior detection of skilled forgeries. This performance breakthrough allows users to automatically process accurately up to 99% of suspects, reducing the number of signatures that have to be manually reviewed to 1%.

Innovative Technology

*Signature*Xpert leverages artificial intelligence and exploits the most comprehensive and advanced methods available in the art of signature verification. Automatic comparison is executed by a powerful combination of verifiers using seven fundamentally different algorithms and techniques. In particular, they combine a human-like holistic analysis of a signature and signature segmentation with a subsequent analysis of the signature elements. In addition to the specific signature verification methods, *Signature*Xpert adapts the proven Parascript Intelligent Recognition technology that enabled Parascript to hold on to its leadership position in handwriting recognition for more than a decade.

The whole verification process can be described as a work of a group of highly skilled experts. Each of them has a favorite approach, which is especially efficient in some cases and produces good enough results in the others. When they work together as a team, their areas of expertise complement each other resulting in the excellent overall performance.

Similarly, all signature verifiers described below apply various approaches to analyze dozens of features of a signature. And additionally each of them has a special area of expertise and exploits a unique method, which may be viewed as distinctive characteristic of a particular verifier.

Thus, a human-like, holistic approach to signature interpretation uses Parascript's proprietary patented technology based on a special descriptive language. This language consists of a set of formative characters (XR-elements) that embody the essence of all styles of writing signatures. Suspect and reference signatures are presented as sequences of XR-elements and compared using multiple parameters. Linear transformation is used to allow correlation between XR elements belonging to different signatures. A system of estimates is built and passed through several neural-networks-based learning and interpretation agents to execute a highly refined analysis and make a sophisticated conclusion about the similarity of two signatures. An example of the correlation between the XR elements belonging to two signatures is shown in Figure 1.

[3] The 2010 Forensic Handwriting Competition

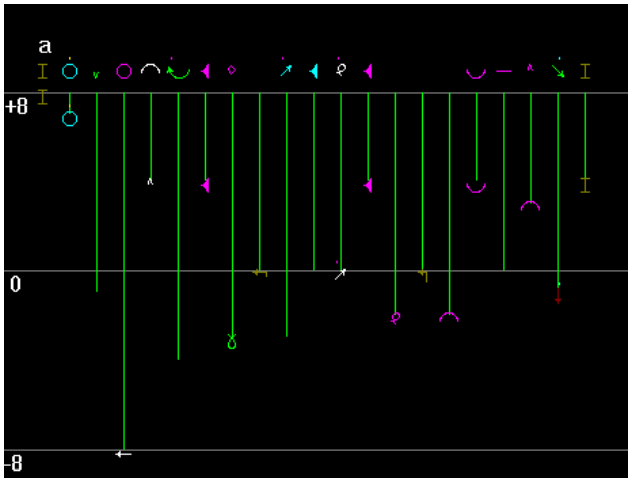

Figure 1. XR-interpretation of two signatures.

Geometrical analysis of suspect and reference signatures complements the holistic approach and makes it more efficient. In this method the similar nodes that are distinctive elements of a signature are located on the suspect and reference signatures (see Figure 2). Triads of these nodes are used to build triangles with apexes located in the selected nodes. The similarity of the triangles belonging to different signatures is analyzed and used to make a conclusion about signature genuineness.

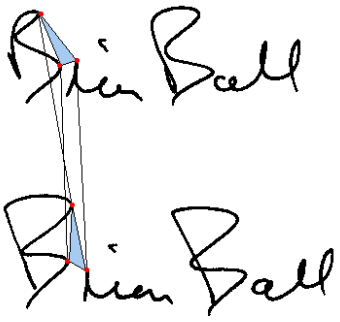

Figure 2. Geometrical interpretation of signatures.

Besides the holistic approach, an analytical method based on signature segmentation and finding correlations between the fragments of reference and suspect signatures is applied (Figure 3). This method complements the holistic approach and is especially efficient in those cases where the holistic approach cannot ensure the required reliability of the result.

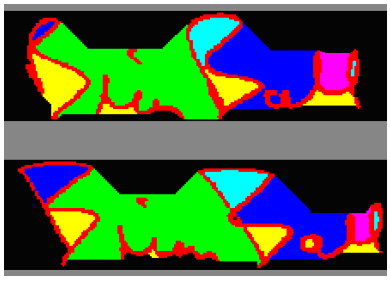

Figure 3. Signature fragments comparison.

A global verifier based on neural networks estimates and compares more than 30 different characteristics of the whole image, including aspect ratio, orientation, slants, curves, etc.

A verifier that employs 2D matching of vectorized signature images. In this algorithm the signature handwriting is represented as a set of vectors. This algorithm searches for the best match between the sets of vectors representing reference and verified signatures. Matching takes into account length and direction of vectors, their mutual positions, and many other characteristics. Additionally the curvature of the segments, local width of a pen, and other features of handwriting are considered in the further fine analysis of the matching parts. This verifier is extremely helpful for complex (for example, European-style) signatures (Figure 4), which can not be precisely described as one-dimensional sequence of elements of handwriting.

Figure 4. Complex European signature.

Another verifier applies fine Fourier analysis of shape and pen width variations of signature elements which proved to be effective in case of skilled forgeries. It uses Fourier transform of X and Y coordinates of the pen trajectory to precisely compare the shape of elements of handwriting. The shape of such elements is unique for the writer because it is produced by unconscious motor movement learnt by an individual.

The last verifier uses Radon transform to distinguish between natural variations in a person's genuine signature and distortions and subtle variations inherent in the skilled and random forgery. Radon transform permits to globally detect lineal singularities in an image, being a very important source of information in these images. Compact descriptors created due to this transform are very efficient for detection of subtle distortions inherent in skilled forgeries.

What it does

*Signature*Xpert verifies signatures on the following items:

- Signature snippets cut from any document
- Personal and business checks with one signature or two signatures
- Image Replacement Documents (IRDs)

*Signature*Xpert compares an image of a signature presented for verification against a reference signature image – a genuine signature previously collected from a signer - and makes a conclusion about the authenticity of the input signature. The product may compare images having different

resolution. Multiple reference signatures can be used for verification and may include signature snippets cut from a document and check images.

The main steps in the signature verification process are presented in Figure 5.

If both prototype signature and suspect signature are presented in the form of clean signature snippets each having just one signature, automatic comparison begins immediately. If signature snippets contain noise, *Signature*Xpert preprocesses the images, cleaning the document and removing lines, prints, pictures, noise, and other intrusions around the signature. For check and IRD images or snippets containing two signatures, *Signature*Xpert automatically locates each signature on a document and then removes noise from the image before matching begins.

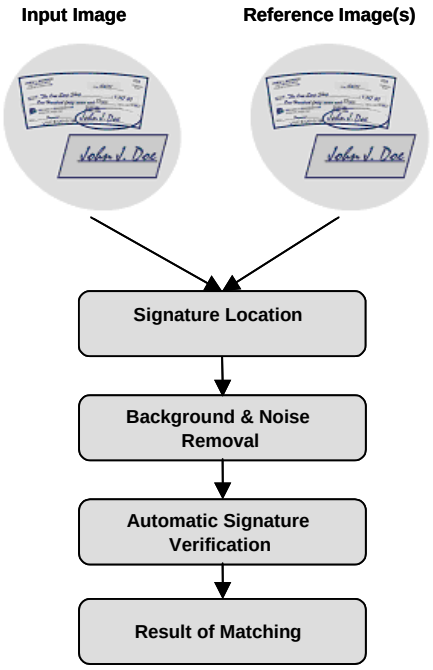

Figure 5. Signature verification stages.

Verification Results

*Signature*Xpert issues a confidence value that ranges from 0 (zero) to 100 and indicates how confident the verification process is about the match between the signature presented for verification and the corresponding reference prototype. A high confidence value indicates a high probability that the signature presented for verification resembles the reference prototype.

The confidence value serves as a basis for making a decision about signature genuineness and coming to a conclusion about a probable fraud type. A certain confidence value is chosen as a threshold: those signatures that match prototypes with a confidence value equal to or higher than the chosen threshold are considered to be genuine; the signatures that match prototypes with a confidence value lower than the threshold are considered to be suspects and will require further human verification.

If a few reference prototypes are used for comparison, *Signature*Xpert issues the result of the best match. If a check with two signatures is used as an object for verification, *Signature*Xpert produces the result for the signature which has the lower match score.

Additionally, *Signature*Xpert allows the following data to be retrieved:

- the number of signatures that were found on the document presented for verification or on the reference document;
- a preprocessed (cleaned from noise) snippet of a signature on the document presented for verification or on the reference document;
- the coordinates of a rectangle that contains a signature found on the document;
- a reference signature that is the best match for a specified signature presented for verification.

Features and Benefits

Image Preprocessing

*Signature*Xpert provides advanced capabilities to eliminate background and remove all kinds of noise from check images, IRD images and snippets. In particular, it efficiently removes lines, preprinted text, intrusions from other fields, stamps and other undesired elements around the signature, leaving a clean signature image and ensuring the safety of informative data.

Due to its ability to successfully clean even the most challenging images, *Signature*Xpert may be applied in a wide range of applications and deal with signature snippets cut from documents having diverse and unpredictable layouts, such as voting cards, forms, and reference cards.

Automatic Signature Location

*Signature*Xpert automatically locates one or two signatures on check images, IRD images and snippets allowing the software to efficiently detect fraud on a variety of documents.

Multiple Verification Engines

It is not possible to produce an exact simulation or tracing of a subject's signature which would have the graphical appearance of a genuine signature, identical signature elements and an authentic signature's segment timings. Therefore, to reliably detect fraud it is important to evaluate different parameters and characteristics of a signature.

*Signature*Xpert combines seven verifiers based on fundamentally different approaches. Each of them focuses on the analysis of a certain range of informative signature features from generic characteristics like similarity of signature histogram and presence and number of typical elements to detailed comparison of geometrical shapes of signature fragments or directions of trajectory sections.

This approach allows unprecedented accuracy of verification by taking into consideration all informative data that can be extracted from a signature image, including biometric characteristics restored from the still image. For example, signature tremor indirectly indicates slower speed and tension while signing, which is inherent in the procedure of signature forgers. Such biometric characteristics as the speed of writing are also reconstructed and compared through the analysis of trajectory width fluctuations/changes.

Multiple Reference Images

An individual's signature is never entirely the same every time it is written. Signatures vary depending on fatigue, mental and physical state, and writing position, and they can also change substantially over an individual's lifetime. However, the consistency created by natural motion and practice over time creates a recognizable pattern unique to each individual. The major problem facing signature verification technology is differentiating between the consistent parts of the signature and unstable parts of the signature that vary with each signing. Therefore, the signature verification process has to have a certain tolerance, but it must also be sensitive enough to pick out a needle in a haystack when it is, in fact, distinctive evidence of a forgery.

*Signature*Xpert's technological edge over the competition is its ability to use multiple references. This allows it to consider more data to detect stable distinctive characteristics in a signature and to focus on them in the verification process simultaneously, ignoring random distortions and variations inherent in genuine signatures. It is possible to update reference signatures and add new ones to ensure the availability of complete and current data for verification.

The ability to work with multiple reference images also provides flexibility in implementation of different rules for processing company checks, signed by different people. For example, if signatures of different individuals are included in the set of reference images, it is possible to verify that a check with an amount higher than a chosen threshold is signed by a particular individual or two individuals entitled to sign checks of a certain value.

The Confidence Value Mechanism

The goals of authentication based on signature verification are different for different applications. For example, in some applications the primary concern of verification is to minimize "false negatives" (genuine signatures that are erroneously considered to be fraudulent). Others have to have near zero "false positives" (fraudulent signatures that are accepted as genuine).

The *confidence value mechanism* provides flexibility and allows implementation of different scenarios of interpreting results. Depending on the confidence value chosen as a threshold, it is possible to regulate the percentage of "false positives" versus the percentage of "false negatives" to make them optimal for a specific application.

Diverse/Multiple Output Options

Applications that may benefit from signature verification are diverse and so are the requirements, purposes, and scenarios that have to be implemented in these applications. SignatureXpert produces multiple types of output results, enhancing product flexibility and adaptability to any environment and application needs.

Online Signature Verification

Parascript exploits many years of experience in online handwriting recognition and applies knowledge accumulated in developing the most advanced off-line signature verification technology to online signature verification.

The key to the online verification of the authenticity of questionable signatures lies in the reconstruction of the writing motion and its elements. Signing is a reflex action based on prior repeated experience (training) and not influenced by deliberate muscular control. In particular, when signing, the hand often moves faster than an individual could volitionally control it to move through hand-muscle coordination. The practiced and natural motion of the original signer would be required to repeat the signature pattern. A copy machine or an expert forger may be able to duplicate what a signature looks like, but it is virtually impossible to mimic such unique behavioral patterns and characteristics of the original signer as succession of touches to the writing surface, speed, acceleration, and pressure. Thus, for dynamic signature verification a handwritten signature is recorded/captured using a variety of pen-enabled devices such as digitizing tablets, membrane touchpads, capacitive touchpads, LCD touchscreens, computer displays or other contact-sensitive technologies. During the act of signing, a signature is captured and elements and behavioral characteristics that make it unique and identifiable are derived. Signature verification checks biometric characteristics of a questionable signature against biometric characteristics of reference signature(s) and can be executed either in real-time or afterwards. The availability of behavioral characteristics of the signing process that unambiguously distinguish an individual makes it feasible to create robust signature verification systems. Based on this approach, a number of dynamic signature verification products demonstrate similar efficiency, which in most cases is a direct function of the quality of the utilized writing tablet.

Parascript® *Signature*Online™ - A State of the Art Solution for Dynamic Signature Verification

Online Signature Verification based on the analysis of unique biometric data inherent in a particular individual is the most natural solution to the authentication problem. Signature verification is strongly ingrained in our social, legal and commercial lives, and this allows the method of dynamic signature verification to be seamlessly integrated into existing working processes and be socially accepted. The fact that this method is also accurate, operates with compact data, is intuitive and fast makes it ideal for document authentication and enterprise workflow.

Parascript's newest fraud detection product, *Signature*Online, provides signature verification to detect signature fraud in a variety of online applications, such as workflow automation, document management, and electronic transactions in banking, financial, health care, retail, government, and other sectors. Award winning[4] *Signature*Online traces the movement of a pen and recognizes the differences in legitimate signing style or behavior making it possible to quickly and reliably detect fraud while reducing the number of authentic signatures that are erroneously considered to be fraudulent.

*Signature*Online combines multiple engines that analyze temporal biometric characteristics such as speed, acceleration, deceleration, stroke sequencing and length, pen pressure and timing information received directly during the act of signing together with a proven innovative technology that scrutinizes signature shape. Therefore, unlike other on-line signature verification products, the success of automatic online signature verification in *Signature*Online does not solely rely on velocities or forces. *Signature*Online uniquely benefits from a synergy of the most advanced methods of analysis of spatial characteristics of a signature image and the opportunities provided by the ability to exploit biometric characteristics of the process of signing.

The product supports virtually any form of pen-enabled device such as palmtop or PDA-type devices, digitizer tablets and smart phones. The diversity of characteristics involved in the analysis, and the product's ability to ensure a high efficiency of verification even if certain characteristics of signing (for example, pressure) are not tracked, reduces dependence on the type, specifics and quality of pen-enabled devices and allows usage flexibility.

Features and Benefits

Robustness and performance

*Signature*Online uses a powerful combination of seven independent engines based on different principles for comprehensive signature verification. Each engine analyzes multiple biometric characteristics of a signature in question to compare it against a reference signature trajectory and to measure the confidence value of the signature's genuineness. If several reference signatures are available, the measure of the stability of the particular feature is developed and used to estimate how probable the deviations observed in the questionable signature are if it was supposedly signed by the same person.

Finally, the results received by each engine are combined to provide a reliable measure of the likelihood of coincidence between the signature in question and genuine reference signature(s). Usage of several independent engines leads to a dramatic performance improvement and adds substantial robustness to the whole verifier.

[4] The 2009 Netherlands Forensic Institute Test

Universality

*Signature*Online is a versatile and powerful tool that enables software developers to add dynamic signature verification capability to a variety of online applications. The product is language-independent and is able to verify a signature captured using any device, such as a mouse, a touchscreen or pen tablets.

Flexibility

Like *Signature*Xpert, *Signature*Online has a confidence value mechanism that allows the implementation of different scenarios for interpreting results. Depending on the confidence value chosen as a threshold, it is possible to regulate the percentage of "false positives" versus the percentage of "false negatives" to meet the requirements of a particular application.

Conclusion

Parascript's automatic signature verification represents an ideal bridge between the long-recognized practice of signing a document and the reliable authentication and authorization that are increasingly needed for many commonplace activities. The solution can support virtually any application, from Homeland Security to banking and retail applications, providing organizations and individuals with enhanced security and control over the documents and transactions that are originated, transacted and stored in today's business environments.

Based on state-of–the-art technology, *Signature*Xpert and *Signature*Online extract maximum data concealed in a static image of a signature or a signature trajectory captured with a digitizer and convert the data to information that allows a more reliable detection of forgery than any other solution available on the market, including manual verification. Results are especially impressive when dealing with skilled forgeries, as the technology provides efficiencies that remain stable with time. This reliability of results cannot be achieved by a human operator, whose productivity inevitably decreases because of the fatigue factor.

Relying on this technology enables banks and other institutions to safeguard customers through the best signature verification practices available today.

About Parascript

Parascript® Intelligent Recognition engines capture, interpret and transform paper-based data into actionable information. Uncovering the hidden meaning of information, we help commercial and government organizations drive higher accuracy and productivity while automating costly data entry. The first to solve the cursive handwriting puzzle, Parascript has grown to be the Intelligent Recognition solution for the U.S. Postal Service and other Global 2000 organizations including Böwe Bell & Howell, Carreker, Elsag, Lockheed Martin, NCR, Siemens and Unisys. Parascript is online at www.parascript.com.

For more information about Parascript's products and services, please contact us at:

- info@parascript.com
- www.parascript.com
- Phone: 888.772.7478

Parascript, *Signature*Xpert and *Signature*Online registered trademarks of Parascript, LLC.