PARASCRIPT®

Strategic White Paper

Increase Security Through Signature Verification Technology

Takeaway

- Understand the benefits of automatic signature verification
- Learn about the types of automatic signature verification
- Compare online and offline signature verification techniques

Introduction

Today's technology equips forgers and other unscrupulous individuals with powerful tools to pass counterfeit signatures off as the real thing. However, while technology has enabled theft, it has also armed businesses with the highest level of automatic signature verification solutions – both online and off.

The advantages for businesses now lie in their ability to set rules for signature verification, customize them across the organization, and tier them for risk factors. This means that the volume of high-risk checks that receive manual review declines, which increases efficiencies and allows staff to focus on other important functions.

What's in this Paper?

6273 Monarch Park Place, Longmont, CO 80503 USA
T: 303.381.3100 | toll free: 888.225.0169
F: 303.381.3101 | info@parascript.com

Today's Environment

People and businesses recognize signatures as the primary way of authenticating transactions. People sign checks, authorize documents and contracts, validate credit card transactions and verify activities through signatures. As the number of signed documents – and their availability – has increased tremendously, so has the growth of fraud.

According to recent studies, check fraud costs banks about $900M per year with 22% of all fraudulent checks attributed to signature forgeries[1]. Clearly, with 27.5 billion checks written each year in the United States,[2] visually comparing signatures on the hundreds of millions of checks processed daily proves impractical. As the need to guarantee the authenticity of each document remains urgent, this task requires more efficient, controlled and reliable methods of signature verification than visual comparison provides.

Check fraud costs banks about $900M per year with 22% of all fraudulent checks attributed to signature forgeries.

The physical act of signing a signature requires coordinating the brain, eyes, arms, fingers, muscles and nerves. With all of this in play, it's no wonder that people don't sign their name exactly the same every time: some elements may be omitted or altered. Personality, emotional state, health, age, conditions under which the individual signs, space available for the signature and many other factors all influence signature-to-signature deviations.

Ironically, skilled forgeries created with sophisticated techniques can generate fewer deviations than a genuine signature. This underscores why it's virtually impossible that two authentic signatures appear exactly alike in terms of style, slant, spacing and so forth.

Examples of inconsistent authentic signatures

The Rise of Fraud

Fraud runs rampant everywhere a transaction requires a signature for authentication. Schemes and scenarios vary from situations when the forger neither knows the victim's name, nor has access to the victim's signature – to cases when the forger can view and thoroughly practice with an authentic signature.

1 ABA Deposit Account Fraud Survey Report, 2011

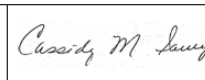
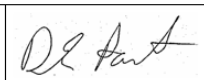
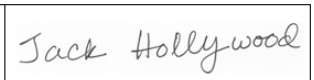
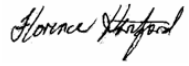
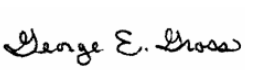
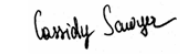
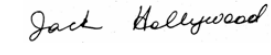
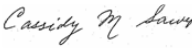
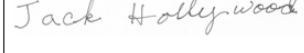
2 The 2010 Federal Reserve Payments Study

The range of signature forgeries falls into the following three categories:

1. Random forgery – typically has little or no similarity to the genuine signatures it is supposed to represent. This type of forgery is created when the forger has no access to the authentic signature.

2. Blind or simple forgery – occurs when an imposter knows the name of the person whose signature must be authenticated, but does not know the actual style or pattern of the original signature. In this case, the signer writes the name of the victim in his or her own style.

3. Skilled forgery – produced by a perpetrator that has access to one or more samples of the authentic signature and can imitate it after much practice. Skilled forgery is the most difficult of all forgeries to authenticate.

Genuine Signature			
Random Forgery			
Blind Forgery			
Skilled Forgery			

A viable automatic signature verification product must have the ability to detect all these types of forgeries by means of reliable, proven algorithms.

Types of Automatic Signature Verification

Businesses primarily use automatic signature verification for checks, although it has additional applications such as loans, point-of-sale, and vote by mail. The main advantage of automatic signature verification stems from leaving the error-prone human review behind; gone are the risks that stem from tired humans, inconsistent training and different levels of capabilities. Instead, the same algorithm applies to all signature verification, which users can customize for different departments or tiered thresholds for varying levels of risk.

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 *offline*.

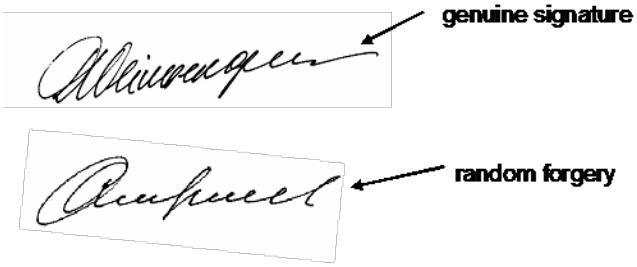
The second type embraces applications that allow tracking the motion in the process of signing at the point of presentation. Accordingly, systems that treat the signature as a series of movements and can be used with both locally or remotely originated transactions are called *online* or *dynamic*.

Automatic Versus Visual Verification

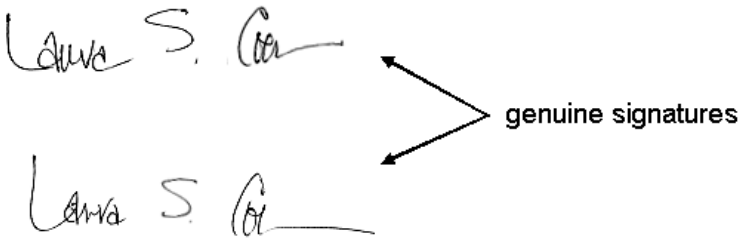
One of the most common fraud prevention methods, visual signature verification, has remained unchanged for decades. Human factors influence the efficiency and accuracy of visual verification, making it slow and error prone. Although criticized, visual verification is the final arbiter when automatic signature verification cannot make a reliable conclusion, or makes the wrong conclusion about signature authenticity. Visual verification, however, has proven an inexact science and varies heavily depending on human factors such as expertise, fatigue, mood, working conditions and others. Finally, it is not economically feasible to have humans verify every signature in the organization, so operational rules, such as check-amount thresholds are required.

The way to decrease human error begins with relying on people with higher expertise and reducing the number of signatures they verify.

Operator's mistake: genuine signature and random forgery that operator accepted as an authentic signature:



Operator's mistake: one of two genuine signatures was rejected as a forgery:



The way to decrease human error begins with relying on people with higher expertise and reducing the number of signatures one operator verifies within a specific time frame. This proves expensive; however an automatic system that handles the bulk of verifications makes it feasible.

The most advanced signature verification software takes advantage of artificial intelligence systems to imitate the type of analysis that humans perform, and combines this approach with the strengths of computer systems. In this way, automatic systems make definitive measurements and give a more accurate appraisal of signature characteristics that some experts can only estimate using traditional techniques. Comparing enrollment signature measurements to signatures submitted for verification lets automatic signature verification outperform back office personnel at banks and show more accurate and consistent results in real-life applications. As a result, institutions can verify a larger number of signatures within a limited time frame.

Signature Accuracy

Based on different principles and different strengths, a person and automatic signature verification software may make inconsistent conclusions about a particular signature. The benefits then come from assigning highly specific parameters for automatic signature verification to any application that requires fast verification of a large number of signatures. These systems verify the majority of images, sending only a smaller number of suspect signatures for further human verification. The reduced burden on human operators allows them to examine signatures more thoroughly and deliver more accurate results, which improves the overall accuracy of the verification process.

Offline Signature Verification

In applications that scrutinize signed paper documents, only a static, two-dimensional image is available for verification. This poses challenges for an automatic solution, because the software has to address two kinds of forgeries; random forgeries produced without knowing the shape of the original signature and skilled forgeries generated by people who, looking at the original instance of the signature, imitate it as closely as possible.

Accurate forgeries take far longer to produce than genuine signatures, but analysis does not consider speed characteristics. 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.

One of the key characteristics needed in signature verification software centers around its ability to detect signature forgeries, particularly skilled forgeries. By having a reference signature image – a genuine signature previously collected from the signer – a solution can make a conclusion about the authenticity of the input signature based on:

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

Users should incorporate multiple reference signatures for verification, and may

include signature snippets cut from a document and check image. Additional reference signatures increase overall accuracy but it should be noted there is a trade off between the number of reference signatures and throughput time.

Online Signature Verification

The key to online verification of signatures lies in reconstructing the writing motion and its elements. Signing is a reflex action based on a repeated action, rather than deliberately controlling muscles. A copy machine or an expert forger may duplicate what a signature looks like, but it is virtually impossible to mimic unique behavior patterns and characteristics of the original signer, such as the succession of touches to the writing surface, speed, acceleration and pressure.

Therefore, dynamic signature verification records and captures a handwritten signature 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, software captures the signature and its vector-based metadata, and derives the elements and behavioral characteristics that make it unique.

During the act of signing, software captures the signature and its vector-based metadata, and derives the elements and behavioral characteristics that make it unique. Online signature verification checks the detailed characteristics of the questionable signature against a referenced signature, which can be performed either real-time or afterwards. By drawing on behavioral characteristics of the signing process that make each signer unique, highly accurate online solutions deliver dynamic signature verification.

Conclusion

Automatic signature verification bridges the gap between the long-recognized practice of manual signature verification and the need for fast, reliable authentication needed in today's high-volume, transaction-oriented environment. The right solution addresses the objectives and business rules that need to be addressed, and often prove a business's biggest consideration.

The ideal solution provides a highly reliable forgery detection system that surpasses manual verification, and streamlines current processes and adjusts to the needs of departments within an organization. The right technology provides efficiencies that remain stable with time, unlike results achieved in high-volume situations with human operators.

Ultimately, relying on automatic signature verification enables institutions to safeguard customers through the most reliable, accurate signature verification practices available today.

About Parascript

Parascript software toolkits make automated form processing, check fraud prevention, medical imaging, Check 21 and remittance processing, and postal automation possible with the highest levels of recognition accuracy and the lowest error rates in the industry. No other technology captures all character types from any image, including cursive, handprint (ICR) and machine print (OCR).

Parascript's partner-centric business model enables solution providers to solve complex recognition problems, critical to helping organizations remain competitive in today's business environment. With decades of experience applying image analysis and pattern recognition to a broad range of markets, we continue to lead the way with proven technology and capabilities that maximize recognition rates and accuracy. Learn about the unique theories and methods that set our products apart and collectively create the Parascript Difference at parascript.com.

6273 Monarch Park Place, Longmont, CO 80503 USA
T: 303.381.3100 | toll free: 888.225.0169
F: 303.381.3101 | info@parascript.com