Usando Firmas Artificiales en Sistemas de Adquisición y Reconocimiento Web

Sergio Rodriguez-Vaamonde[1], Carlos Vivaracho-Pascual[2], Juan Manuel Pascual Gaspar[3] y Valentín Cardeñoso Payo[2]

[1] Unidad Infotech, Robotiker-Tecnalia, srodriguez@robotiker.es
[2] Departamento Informática, Universidad de Valladolid, {cevp,valen}@infor.uva.es, www.infor.uva.es/{~cevp,~valen}
[3] Dep. Informática, Hospital Clínico Universitario de Valladolid, pascualgaspar@gmail.com

Abstract. En el presente trabajo se muestran una serie de ataques realizados a sistemas de adquisición y/o reconocimiento de firma manuscrita vía web. Estos ataques se han realizado tanto a sistemas experimentales como a demos de sistemas comerciales, basados en distintas tecnologías de adquisición del movimiento del puntero de ratón para la realización de la firma. El ataque propuesto consiste en sustituir los eventos de ratón generados por el movimiento real del dispositivo usado para ello (ratón, smart pen, stylus, puntero de PDA, etc.), por un sistema que realiza el envío artificial de estos eventos. Se verá, por un lado, la debilidad de los sistemas de adquisición de firma si no se añaden mecanismos para verificar que al otro lado hay un ser humano, pero, por otro, se mostrará la robustez de los sistemas de reconocimiento ante ataques como el indicado cuando el imitador no cuenta con la dinámica de la firma.

Keywords: firma on-line, ataques a sistemas biométricos, web.

1 Introduction

La biometría se presenta como na alternativa o un complemento a los sistemas actuales de reconocimiento del usuario basados en clave y/u objeto, para mejorar su seguridad.

Sin embargo, es de sobra conocido que uno de los riesgos del uso de la biometría, tanto en su versión estática como dinámica, es la utilización de partes “no vivas” del cuerpo humano y la generación de patrones artificiales. Existen numerosos estudios al respecto para rasgos como iris [2][5][6], huellas [2][3] o geometría de la mano, en el presente trabajo nos centramos en firma manuscrita.

No son muchos los trabajos publicados al respecto y muchos se centran en texto manuscrito, más que en firma. Además, la mayoría aborda el problema del ataque desde el punto de vista de la creación de patrones artificiales y no tanto de cómo esas muestras se introducen en el sistema, que es una de las partes importantes en el trabajo que aquí presentamos.

En [8] se muestra una herramienta para la evaluación de imitaciones en texto manuscrito. La herramienta permite la imitación en dos entornos (dispositivos) diferentes: PC y PDA, y para varios escenarios de ataque:

- **Blind**: sólo se ve el texto.
- **Low-Force**: se posee el papel con el texto.
- **Brut-Force**: se tiene la dinámica.
- **Accidental**: no se intenta la imitación.

Estudios más similares al aquí mostrado se pueden encontrar en [1][7], donde se estudia la creación y el ataque basado en muestras artificiales tanto para firma como para texto manuscrito. En [1] se aborda el problema en dos escenarios diferentes: i) se conoce la respuesta del sistema (hill-climbing attack), ii) se tiene acceso al patrón o a texto manuscrito y a partir de ahí se intenta deducir/generalizar (la prueba se hace independiente de texto) información acerca del cliente (template-based attack). Para el primer escenario se usan firmas, mostrando el número de iteraciones necesarias para lograr atacar al sistema. Este número oscila, en promedio, entre las 460 y las 1900, lo que hace inviable este ataque desde un punto de vista práctico. En nuestro trabajo se muestra un escenario similar, mostrando que nuestra propuesta logra atacar al sistema en un número de iteraciones totalmente realista.

En [7] se intenta reconstruir la dinámica de la forma de escribir del usuario, partiendo de texto off-line (texto escrito sobre papel) suyo, al que se aplica los resultados de un estudio estadístico realizado sobre textos de un conjunto de desarrollo (distinto del de prueba) para los que sí se tiene la dinámica. El objetivo del estudio es doble, ya que no sólo se busca analizar la vulnerabilidad de los sistemas, sino, también, la creación de muestras artificiales que permitan mejorar el entrenamiento de los sistemas de clasificación. Los resultados muestran que se logran imitaciones cercanas a las humanas. En nuestro trabajo analizamos, también, un escenario similar a éste, pero para firmas, y mostrando como resultado si la firma sintética creada es capaz de atacar al sistema o no.

Una de las principales contribuciones del estudio que aquí presentamos es que en todos los casos se realiza un ataque real a sistemas reales, es decir, se aborda el problema tecnológico de introducir la firma sintética en el sistema, mostrando que las actuales tecnologías de adquisición de firma son vulnerables ante un ataque tan sencillo como la captura y envío de eventos de ratón.

El resto del artículo se organiza como sigue. En el apartado 2 mostraremos los escenarios de ataque tratados, desarrollando cada uno en los siguientes apartados 3, 4 y 5. Acabaremos en el apartado 6 se pueden ver las conclusiones extraídas tras el estudio realizado.

2 Entorno experimental

Se han planteado los siguientes escenarios de ataque:

- **Sustitución**. Existen numerosos sistemas comerciales que permiten que un formulario o envío de un documento vía web pueda ser firmado mediante firma manuscrita, sin reconocimiento de esta, es decir, se captura la imagen

de manera similar a como se hace en un documento escrito. En este ataque se pretende sustituir la firma manuscrita por otra artificial sin que el sistema lo detecte.

- **Ataque con dinámica**. En este caso se ataca a un sistema de verificación de usuario basado en firma, cuando se tiene la dinámica de la firma. Este ataque surge de una situación real que se dio en el "concurso de imitaciones" planteado en las IV Jornadas de Reconocimiento Biométrico de Personas 2008. En un escenario real, este caso se podría dar cuando se tiene una grabación del usuario firmando.
- **Ataque sin dinámica**. Es similar al anterior, pero ahora sólo se tiene la imagen de la firma, sin la grabación dinámica de la misma.

A continuación, vamos a mostrar los resultados obtenidos en cada caso. Antes, comentar que para realizar la verificación de la firma considerando la información dinámica se ha utilizado el sistema enviado a BSEC'09 [4], quedando en segunda posición.

3 Sustitución

En la tabla 1 aparecen distintas tecnologías usadas para la captura de una firma on-line vía web y que han sido utilizadas para las pruebas de sustitución. Cada caso se acompaña de la URL que se ha usado para realizar el ataque. En la última columna se muestra si se ha logrado sustituir la adquisición de firma real debida al movimiento del puntero de ratón por una acción del usuario, por una firma artificial mediante el envío de eventos de ratón sin intervención humana.

Tabla 1. Ataques por sustitución realizados. En la primera columna aparece la tecnología usada para la captura del puntero de ratón por parte del sistema de verificación, en la segunda la URL del sistema de verificación usado para probar el ataque y en la tercer el resultado de éste

Tecnología	URL	Resultado
Applet Java	www.greidi.uva.es/BioSignWeb	Logrado
Javascript	www.websignaturecapture.com	Logrado
	www.realsignature.com	Logrado
Silverlight	www.onlinesignaturepad.com	Logrado
Flash	www.mylivesignature.com/mls_sigdraw.php	Logrado

Como se puede ver en la tabla se ha logrado introducir la firma artificial con todas las tecnologías, mostrando la debilidad de los sistemas existentes actualmente para la captura de la firma vía web y la necesidad de añadir mecanismos de verificación de que es un humano el que está realizando la firma.

4 Ataque con Dinámica

El ataque a un sistema de verificación de firma que utiliza información dinámica de la misma se ha planteado sobre dos escenarios distintos:

- Escenario 1) El atacante posee la dinámica de la firma y, además, el sistema realimenta al atacante con el resultado de la verificación.
- Escenario 2) El atacante tiene la dinámica, pero no la realimentación del resultado.

A continuación se va a describir el proceso y resultado obtenido en cada caso.

4.1 Con realimentación del resultado

Es la situación planteada en el concurso de imitación realizada en las IV Jornadas de Reconocimiento Biométrico de Personas 2008. En la web el usuario podía ver la dinámica de la firma a distintas velocidades y tras la realización de la imitación se mostraba la puntuación, con respecto al umbral, obtenido por la imitación realizada. En la figura 1 se pueden ver las firmas a imitar.

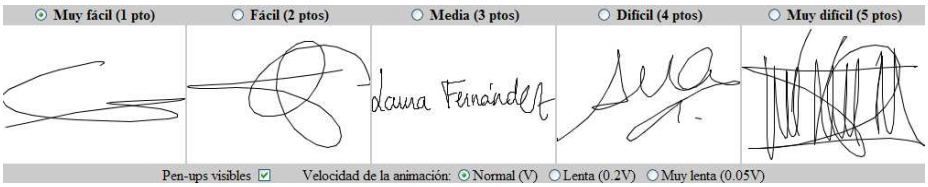

Figura 1. Firmas a imitar en el concurso realizado en las JRBP 2008

Para realizar el ataque, se grabó con una cámara la animación realizada de la firma. A continuación esta grabación se reprodujo a velocidad lenta en un ordenador, siguiendo con el ratón el trazado de la firma, mientras se capturaba este movimiento. Una vez capturada la secuencia de eventos de ratón, éstos se enviaban, a la velocidad adecuada, al applet de captura de la firma del concurso.

Se intentó el ataque a las tres primeras firmas de la figura 1, logrando el acceso en todos los casos.

4.2 Sin realimentación del resultado

Este caso es más aproximado a la realidad. En él, el sistema web no daba información de la puntuación de la firma al atacante. Para realizar el ataque sólo se proporcionaron grabaciones realizadas con cámara de varios usuarios firmando.

Se realizaron pruebas con 8 firmas, de las cuales se logró el ataque en 6 casos. En la figura 2 se muestran dos ejemplos representativos de este escenario: firma atacada

con éxito a la izquierda, no se logró el acceso para la firma de la derecha, que curiosamente es inventada.

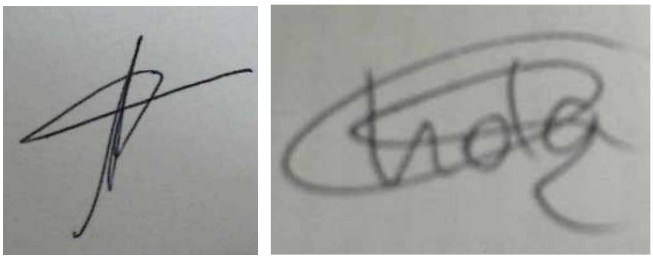

Figura 2. Ejemplos de firmas usadas para el escenario 2 de ataques con dinámica. La de la izquierda fue atacada con éxito, no pudiendo conseguirlo con la de la derecha.

5 Ataque sin Dinámica

En este caso, al atacante no poseía el video de los usuarios firmando. El ataque al sistema ha sido dividido en dos fases. La primera de ellas se ha centrado en un "entrenamiento" del sistema partiendo de una firma previamente conocida y conociendo la puntuación del sistema. En la segunda, a partir de la información obtenida en la primera fase, se ha intentado la falsificación de una firma conociendo únicamente la forma de la misma. La única herramienta utilizada para el ataque ha sido un software propio cuya función principal era proporcionar información del trazo (velocidad y posición) y poder variar las velocidades en cada tramo de la firma pudiendo adecuar la imitación a la real.

4.2 Fase 1 – Ataque a firma previamente conocida

En esta primera fase, la firma a falsificar es previamente conocida y es la mostrada en la figura 3. En esta fase se ha intentado atacar al sistema con la firma conocida previamente para poder analizar qué aspectos son los que más influyen en el ataque. En esa figura también aparece el análisis de velocidades realizado. En dicho análisis se ve cómo la velocidad aumenta progresivamente hasta que disminuye para volver a aumentar en la curva de la "S" y marca un máximo al final de la misma; de tal forma que vuelve a acelerar para empezar la "e" frenando brevemente en la mitad de su trazada.

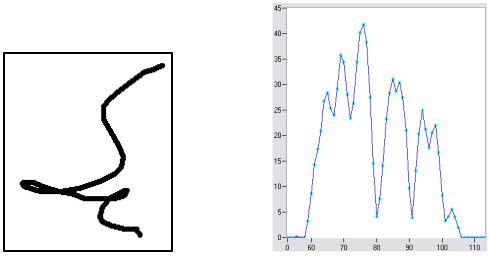

Figura 3. Firma usada en la fase 1 y Análisis de velocidades (en píxeles/ms)

Para realizar el ataque sobre esta firma se ha realizado una imitación pero a diferente velocidad. Como se puede ver en la figura 4 la topología de la firma es parecida (pero no igual) a la original, pero la velocidad del trazo es muy diferente.

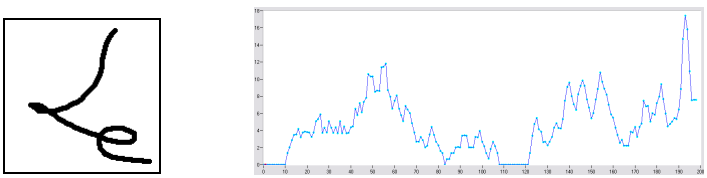

Figura 4. Imitación de la firma de la figura 2.

A partir de esta firma se ha procedido al ataque. El umbral de la firma era de 6,04 mientras que la puntuación obtenida por la firma falsificada era de 9,44. A continuación se describen los pasos realizados para lograr disminuir la puntuación para conseguir traspasar el umbral de aceptación.

El primer paso que se dio fue filtrar la firma para que no existan muchas variaciones debido al pulso de la mano del firmante. Para ello, el software de imitación posee varios filtros lineales que utilizan entre 1 y 6 muestras anteriores y posteriores a la muestra de trabajo. Con la firma falsa que teníamos se comprobó que la puntuación más baja que se puede obtener es mediante un filtrado con 3 muestras delante y detrás, y la puntuación obtenida fue de 9,34.

El segundo paso realizado fue aumentar la velocidad de la firma. Para mantener la topología de la firma se varió el tiempo existente entre las muestras. Tras realizar varias pruebas nos quedamos con una velocidad de 60 pix/ms ya que daba la menor puntuación: 7,93.

A partir de este punto comienza la modificación de la velocidad dependiendo de los tramos de la firma. En un principio se obvió la firma real, así que se dividió la firma en 4 tramos en los que se supuso una configuración determinada de la velocidad.

El primero de los tramos fue desde el inicio de la “S” hasta la mitad de la misma. Como tiene forma curva se ha supuesto que al principio aumenta la velocidad hasta que en la mitad disminuye hasta llegar a un mínimo al final del tramo (es decir, en la mitad de la “S”). Tras sucesivas pruebas se logró una puntuación final de 7,11.

El segundo de los tramos se corresponde a la segunda sección de la letra “S”. En ella se buscó una aceleración en el centro de dicho tramo, coincidiendo con la segunda curva de la letra “S”. Finalmente se obtuvo una puntuación de 6,25.

La siguiente sección de la firma hace referencia a la parte final de la “S” y el inicio de la “e”. En esta parte se hace una desaceleración brusca para a continuación acelerar mientras se llega a la letra “e”, logrando una puntuación mínima de 6,04

Tal y como se ha visto, con la última puntuación de 6,04 se ha alcanzado el valor umbral, así que todavía había que mejorar un poco para lograr bajar la puntuación. Para ello, se actuó sobre la parte final de la “e” aumentando un poco la aceleración y el frenado en dicha sección. De esta forma se ha obtenido una puntuación mínima de 5,96 con la gráfica de velocidad de la figura 5.

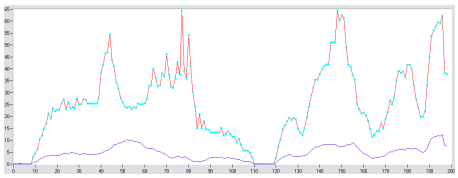

Figura 5. Valores de velocidad usados para lograr la imitación de la firma de la figura 2.

Tal y como se puede comprobar, conociendo las puntuaciones del sistema es bastante sencillo poder modificar la velocidad de la firma y atacar al sistema. Además, se ha comprobado que los valores absolutos de la velocidad no son los más importantes, ya que comparando los valores de figura 4, con los valores reales (figura 2) se comprueba que son bastante diferentes: por ejemplo, en la parte final de la “e” en la firma real se alcanzan los 25 pix/ms mientras que en la imitación esta velocidad es de unos 60 pix/ms. Por otra parte, también ha comprobado que lo que mayor importancia tiene es la dinámica de la firma, es decir, que los picos y valles de la firma real (en cuanto a velocidad) estén en la misma posición en la imitación.

4.2 Fase 2 – Ataque a firma estática

Esta segunda fase se ha centrado en simular el ataque al sistema en unas condiciones más reales, conociendo únicamente la topología de la firma y sin que el sistema devuelva puntuación alguna. Las firmas a imitar se muestras en la figura 6. Como se puede ver se empezó por una imitación sencilla, en principio.

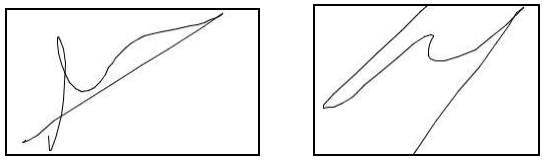

Figura 6. Firmas a imitar sin dinámica

Tras trasladar la topología de la firma al software de imitación, se procedió a variar las velocidades de los diferentes tramos de la firma, así como a filtrar los mismos, siguiendo los pasos aprendidos en la primera fase. En primer lugar, se identificaron los diferentes tramos en base a los puntos de inflexión existentes. En estos puntos de inflexión de la firma, presuntamente el firmante reducirá la velocidad o será máxima.

Así en la primera de las firmas anteriores hemos identificado un punto de inflexión encima de la “l” en donde se ha supuesto que el usuario disminuía la velocidad. Entonces desde el principio de la firma hasta ese punto la velocidad debe ir en aumento, y tras ese punto también deberá aumentar. El problema planteado es cómo aumenta/disminuye la velocidad. Una forma muy típica es una disminución y aumento progresivo, así que en ese punto se le dio a la velocidad una forma gaussiana invertida centrada sobre el punto de inflexión. A continuación, se identificaron otros puntos de igual forma y también se les dio dicha forma a la velocidad. Tras llevar al sistema la firma con esta velocidad, dio como resultado *usuario rechazado.*

La misma dinámica se trasladó a la segunda firma, con el mismo resultado: *usuario rechazado.*

Tras realizar numeras pruebas y análisis no se logró una aceptación del usuario, y el sistema siempre rechazó las imitaciones. Debido a que no se disponía de puntuación, no se sabía si las modificaciones que se realizaban eran correctas o no por lo que fue imposible la aceptación del usuario.

Se intentó una tercera firma con el mismo resultado.

5 Conclusiones

En el presente trabajo se han mostrado varios escenarios de ataque a un sistema de adquisición/reconocimiento de firma manuscrita vía Web

Se ha mostrado la debilidad de los sistemas de adquisición de firma basados en captura de eventos de ratón si no se incluyen sistemas de verificación de que el que produce el movimiento del cursor es un ser humano. Ninguna de las tecnologías actuales evita este problema.

En cuanto a las pruebas con verificación de la firma artificial, se ha comprobado que el sistema es bastante robusto cuando el imitador no tiene la dinámica ni la puntuación de la firma. Sin embargo, cuando se puede acceder a la dinámica el sistema ha podido ser atacado con éxito.

Bibliografía

[1] Ballard, L., Lopresti, D., Monrose, F.: Forgery quality and its implications for behavioral biometric security. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Special Edition) 37 (5), pp. 1107-1118 (October 2007).

[2] Faúndez-Zanuy M., Osuna-Silvestre S.: Experimentos sobre la vulnerabilidad de sistemas biométricos. Actas de las III Jornadas de Reconocimiento Biométrico de Personas. Sevilla 2006.

[3] Matsumoto, T., Matsumoto, H., Yamada, S. y Hoshino, S.: Impact of Artificial ‘Gummy’ Fingers on Fingerprint Systems. Proc. Int'l Soc. Optical Eng. (SPIE), vol. 4677, Jan. 2002.

[4] Pascual-Gaspar, J.M., Cardeñoso-Payo, V., Vivaracho-Pascual, C.E.: Practical on-line signature verification. ICB '09: Proceedings of the Third International Conference on Advances in Biometrics, pp. 1180-1189. Springer-Verlag, Berlin, Heidelberg (2009)

[5] Ruiz-Albacete, Virginia y otros: Ataques Directos Usando Imágenes Falsas en Verificación de Iris. Actas IV JRBP'08, pp 93-102 (2008)

[6] Santos Sierra, Alberto, Sánchez Avila, Carmen y Jara Vera, Vicente: Nuevos Algoritmos y Ataques a Sistemas de Identificación Biométrica basados en Reconocimiento de Iris. Actas IV JRBP'08, pp 83-92 (2008)

[7] Yamazaki, Y., Nakashima, A., Tasaka, K., Komatsu, N.: A Study on Vulnerability in On-line Writer Verification System. Proc. of the International Conference on Document Analysis and Recognition, pp. 1520-5263, (2005)

[8] Zoebisch, F., Vielhauer, C.: A test tool to support brute-force online and offline signature forgery tests on mobile devices. Proc. of IEEE International Conference on Multimedia and Expo, pp. 225-228 (2003).