An electronic security application for the authentication of Android phones based on the biometric analysis of human locomotion

Daniel E. Hernández[a], Víctor E. Gil[a], Fabián Robledo*[,b]

[a]*Escuela de Ingeniería de Telecomunicaciones, Facultad de Ingeniería, Universidad de Carabobo, Venezuela.*
[b]*Departamento de Electrónica y Comunicaciones, Escuela de Ingeniería Eléctrica, Facultad de Ingeniería, Universidad de Carabobo, Venezuela.*

Abstract.- This article presents the development and results of an electronic security app running in real time and in background, aimed at Android phones that, based on human locomotion as a signature and the use of the triaxial accelerometer of the mobile, it allows detecting its unauthorized use, and manage the corresponding reaction. The biometric locomotion pattern of the owner is stored, being used as a reference for authentication when comparing it by multiple means with the user's pattern. For this purpose, two methods of pattern recognition were developed, the first of an experimental type designed based on statistical criteria, and the second based on the K-Nearest Neighbor algorithm (K-NN) of machine learning. Variations in walking patterns due to factors such as gender and footwear/terrain types were analyzed. Authentication involves a decision-making process where a hypothesis test on the user is applied repeatedly. A probability of correctly authenticating the user of more than 80 % and a probability of detection error of unauthorized individuals less than 5 % was obtained. The reaction includes the automated sending of e-mail and SMS to preset addresses informing of possible theft or loss of the mobile phone and the GPS coordinates of its location. Finally, it was determined that the application does not detrimentally affect the performance of the mobile (RAM, CPU) and may run in the background.

Keywords: Android app; authentication; biometry; K-NN algorithm; locomotion; security.

Una aplicación de seguridad electrónica para la autenticación de teléfonos Android basada en el análisis biométrico de la locomoción humana

Resumen.- En este artículo se presenta el desarrollo y resultados de una app de seguridad electrónica, de tiempo real y segundo plano, destinada a teléfonos Android que, basada en la locomoción humana como firma y el empleo del acelerómetro triaxial del móvil, permite detectar su uso no autorizado y gestionar la reacción. Se almacena el patrón biométrico de locomoción del propietario empleándose como referencia para la autenticación al compararlo por múltiples medios con el patrón del portador. A tal fin se desarrollaron dos métodos de reconocimiento de patrones, el primero de tipo experimental diseñado en base a criterios estadísticos, y el segundo a partir del algoritmo K-Nearest Neighbor (K-NN) de machine learning. Se analizaron las variaciones de los patrones de marcha debidos a factores como el género y los tipos de calzado/terreno. La autenticación implica un proceso de toma de decisiones donde se aplica recurrentemente una prueba de hipótesis sobre el portador. Se obtuvo una probabilidad de autenticar correctamente al usuario de más de 80 % y una probabilidad de error de detección de individuos no autorizados menor a 5 %. La reacción incluye el envío automatizado de e-mail y SMS a direcciones prestablecidas informando de un posible hurto o pérdida del móvil y de las coordenadas GPS de su ubicación. Finalmente se determinó que la aplicación no afecta perjudicialmente el desempeño del móvil (RAM, CPU) y puede correr en segundo plano.

Palabras clave: Android app; autenticación; biometría; algoritmo K-NN; locomoción; seguridad.

Recibido: 10 de mayo, 2019.
Aceptado: 29 de julio, de 2019.

1. Introducción

El avance tecnológico ha impulsado el desarrollo de técnicas de reconocimiento de patrones biométricos y estos sistemas se han extendido desde el campo de la medicina hasta la seguridad, donde la biometría toma mayor relevancia [1]. Las técnicas

*Autor para correspondencia:
*Correo-e:*frobledo@uc.edu.ve (F. Robledo)

computacionales y de los sensores han permitido a la biometría madurar en las aplicaciones de seguridad electrónica, implementando tecnologías como el reconocimiento facial, de voz, de marcha, etc. [2]. En las aplicaciones iniciales del reconocimiento de patrones biométricos era necesaria la explícita interacción del sujeto con los sensores. Estudios psicofísicos demuestran que es posible reconocer a una persona a partir de su forma de caminar [3]. De esta forma surge el estudio de la locomoción humana como potencial firma biométrica debido a propiedades como la de ser un método de identificación no invasivo [1].

La incorporación a los móviles de sensores inerciales para recolectar información del entorno y del usuario ha abierto la posibilidad de adquisición de datos biométricos. Ciertos estudios han sido realizados para el reconocimiento de la actividad humana, como caminar, trotar y saltar, usando los sensores para diversas aplicaciones de seguridad [4]. El incremento de la información privada almacenada en teléfonos inteligentes ha generado preocupación sobre la confidencialidad. En Venezuela de acuerdo al informe de 2015 de la Asociación Civil Paz Activa, un 39 % del mercado ilegal está dedicado a la venta de celulares robados en distintas comunidades [5]. Por lo tanto, la autenticación del usuario del teléfono móvil es esencial para la prevención de fugas de información. Las contraseñas o PINs son una forma de autenticación, pero son vulnerables a los ataques de fuerza bruta y al olvido [6]. Los sistemas biométricos para autenticación surgen como opción a considerar.

Se efectuó el desarrollo y evaluación de una aplicación (app) de seguridad implícita en segundo plano para teléfonos Android que permite la autenticación en tiempo real del usuario, realizada en base a la firma biométrica de locomoción humana. En esta investigación se implementó un prototipo capaz de llevar a cabo la autenticación del usuario del móvil en base al procesamiento de patrones de locomoción para así proveer un mecanismo de seguridad a los teléfonos que permita la reacción ante su robo o hurto. Para tal fin se programó un módulo de adquisición de datos de las señales biométricas de locomoción que provienen de los sensores del teléfono, se construyó una base de datos de señales de locomoción humana de los sujetos de prueba, se seleccionaron las técnicas computacionales de reconocimiento de patrones para la identificación asertiva de las señales biométricas, se desarrolló un módulo de procesamiento principal para lograr la autenticación del sujeto portador, basada en el análisis estadístico que permite obtener indicadores de precisión y fiabilidad de la app, y se diseñaron los protocolos de notificación remota y reacción ante un posible hurto, programados en un módulo de seguridad. También se evaluó el impacto de la app en el desempeño general del teléfono.

El estudio se limitó al porte del móvil en un bolsillo del pantalón, ya que éste es el lugar donde se obtienen mejores resultados según algunas investigaciones [4]. La reacción de seguridad incluye el envío de la información de la ubicación del dispositivo perdido (vía sensor GPS) a través de mensaje de texto o correo. La investigación fue realizada en la Universidad de Carabobo, en la Escuela de Telecomunicaciones de la Facultad de Ingeniería, con soporte de la Escuela de Ingeniería Eléctrica de esa misma Facultad.

2. Metodología y desarrollo de las aplicaciones de software

Las etapas en el desarrollo de la app requerida para llevar a cabo el proceso de autenticación del usuario del teléfono móvil se presentan en la Figura 1.

Figura 1: Diagrama de bloques de la app de autenticación.

Para la adquisición de datos se emplea un acelerómetro triaxial que detecta la aceleración inercial producida por movimiento e incluye la gravedad, y es capaz de cuantificar la aceleración en tres ejes perpendiculares entre sí. El eje X corresponde a un eje horizontal respecto a la pantalla del teléfono, el eje Y corresponde a un eje vertical, y el eje Z es perpendicular (en

base a developers Android, documentation for app developers, 2018.), según la Figura 2.

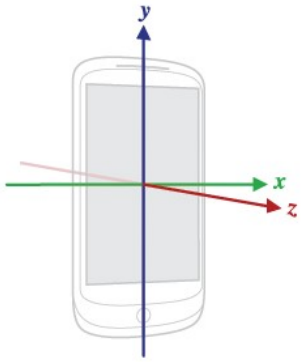


Figura 2: Ejes del acelerómetro triaxial en teléfonos Android.

Para usar el sensor se usó un *método oyente* de Android que permite a la app acceder a los datos del acelerómetro y configurar el retardo para una adecuada frecuencia de muestreo (con cambios de hasta un 5 %). Para el retardo se optó por el valor dado por la constante *SENSOR_DELAY_GAME*, con una frecuencia nominal de 50 Hz para prevenir el aliasing. Una vez activado el oyente del acelerómetro se obtienen los valores adquiridos a través del método llamado *onSensorChanged*, pudiendo tomar las muestras de los ejes X, Y y Z de manera individual a través de un vector dado por el sistema llamado *event*. En relación a la orientación espacial del teléfono, las muestras de aceleración deben ser recolectadas mientras el dispositivo se encuentra en el bolsillo del pantalón. En general, hay dos eventos que pueden afectar la adquisición de datos: el error por desplazamiento y el error por orientación [7]. El error de desplazamiento se desprecia y el error de orientación es tomado en cuenta ya que afecta significativamente las señales en el eje X y Y (Figura 3).

Desplazamiento Orientación Ambos

Figura 3: Errores de orientación y desplazamiento.

Se optó por calcular la magnitud total de aceleración, ya que los errores mencionados son mínimos para esta señal [7], de modo que fueron la aceleración en el eje Z y la magnitud total de la aceleración las señales usadas en el estudio. Los valores de aceleración que proporciona el acelerómetro triaxial están afectados por la fuerza de la gravedad, aun cuando el teléfono está en reposo [4]. Las variaciones en la orientación del teléfono generan cambios en las componentes gravitatorias de los ejes que forman al vector aceleración, resultando en la adición de señales de baja frecuencia, que pueden ser removidas usando un filtro paso alto. Se desarrolló una aplicación donde dichas señales se visualizan en tiempo real antes y después del proceso de filtrado (Figura 4). Las frecuencias importantes no superan los 10 Hz en la marcha humana y aproximadamente hasta la 7ma armónica hay contenido significativo de señal, que en promedio para un peatón no superaría los 6 Hz [8].

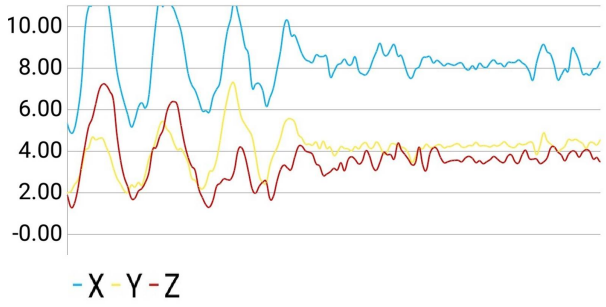


Figura 4: Señales temporales del acelerómetro triaxial, agitando el dispositivo.

En la etapa de pre-procesamiento (Figura 5) se prepara la señal para su caracterización en la autenticación del usuario. Los filtros empleados pertenecen a la librería de código abierto *KalebKE.FSensor* de Android Sensor Filter and Fusion.

La aceleración de gravedad debe ser removida, este procedimiento se considera la calibración del sensor. Esto se logró usando dos clases de la librería *Fsensor* siguiendo la recomendación de *Android Studio*, en la que un filtro pasabajo es aplicado a la señal para aislar la gravedad, valor que luego es substraído de la señal original. Los datos del

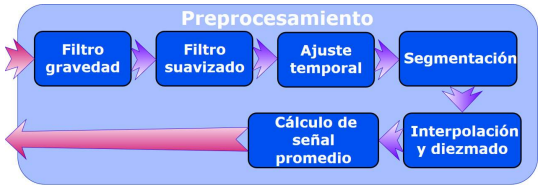


Figura 5: Etapas de pre-procesamiento.

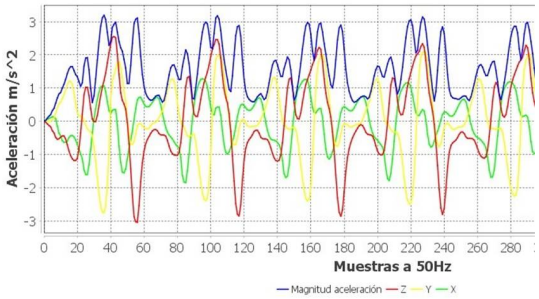


Figura 6: Señales de aceleración muestreadas en una ventana de 8 s, magnitud, X, Y y Z.

acelerómetro tienen ruido proveniente de varias fuentes (irregularidades en el piso sobre el cual se camina y procesos internos del teléfono) [7]. Dos filtros paso bajo en cascada, empleando la clase *LowPassFilter* fueron configurados para generar un efecto suavizador, eliminando componentes de alta frecuencia. En cuanto al ajuste temporal, la tasa de muestreo en dispositivos móviles celulares no es constante y depende del sistema operativo. Este *jitter* en el intervalo de tiempo entre muestras requiere ser corregido para contar con un conjunto de datos bajo una tasa de muestreo fija, por lo que una interpolación lineal fue empleada. A continuación se realiza una segmentación y extracción de ciclos. Se establece un tiempo finito para el registro del patrón del caminar de una persona, bajo una tasa de muestreo de 50 Hz, ello implica una gran cantidad de procesamiento por lo que se emplea una segmentación para la extracción de características y posterior clasificación [9, 10]. Con más de 20 ciclos es posible obtener una representación general del patrón de una persona. Por tal motivo, se estableció un tiempo de 40 s en cinco grupos de 8 s, en la cual la persona debe caminar. Estos grupos de muestras fueron organizados y almacenados en tablas de una base de datos por usuario. En la Figura 6 se aprecian las señales típicas obtenidas en esa ventana.

Las muestras tomadas en tiempo real se adquieren en ventanas de 6 s. El proceso consiste en recolectar los datos, efectuar el pre-procesamiento y ejecutar la autenticación para obtener una respuesta que permita tomar una decisión sobre quien porta el teléfono, repitiendo nuevamente todo el ciclo. La señal es cuasiperiódica, de manera que puede ser seccionada, y se obtiene cada uno de sus pseudociclos a los cuales le son extraídas características temporales/frecuenciales, para la autenticación (Figura 6). La señal Z presenta un pico de aceleración justo cuando se da un paso, evento que permitió desarrollar el algoritmo para la extracción de ciclos. Se elaboró un método "experimental" que consiste en desplazar una ventana con un ancho de 51 muestras desde el inicio hasta el final de la señal muestreada, y en cada desplazamiento verificar si la muestra que se encuentra en el medio de dicha ventana es la que posee mayor amplitud.

Para la extracción de características temporales/frecuenciales es necesario que cada ciclo obtenido posea la misma cantidad de muestras, por consiguiente se debe tomar un valor promedio y emplear algoritmos de interpolación y diezmado para modificar la frecuencia de muestreo. Para la interpolación se usó el método de los polinomios cúbicos de la librería *Commons Math* de Apache. Una vez que se obtiene la señal interpolada, se le extraen las muestras adecuadas para generar un nuevo vector diezmado en un algoritmo diseñado a tal efecto. Esta librería permite hacer el ajuste de curvas a través del cálculo de regresión polinomial. Se implementó un algoritmo que calcula la señal promedio determinando las medias de cada muestra.

Las aplicaciones desarrolladas generan una base de datos por cada usuario que registra un patrón de caminar en tablas individuales. Todos los datos son almacenados en la base de datos correspondiente al generarse el movimiento del individuo. El conjunto de algoritmos y técnicas de procesamiento mencionados fueron programados en dos aplicaciones para Android, que se incorporaron en una aplicación de prueba para la recolección de patrones de locomoción,

en función de la cual se desarrolló el algoritmo de autenticación. Estas aplicaciones registran a distintos usuarios en bases de datos SQlite, y permiten visualizar los patrones de caminar adquiridos (Figura 7).

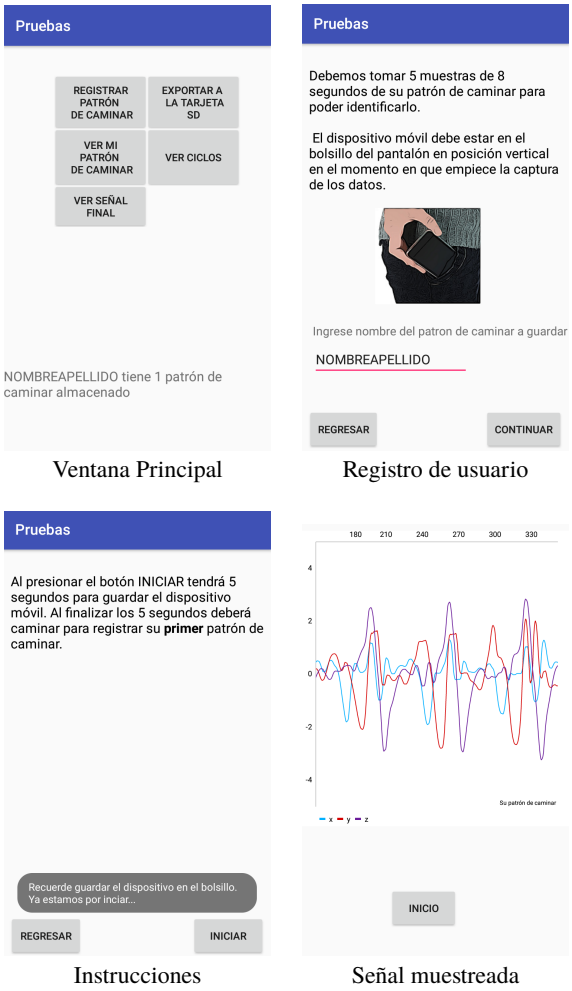


Figura 7: Vistas de la aplicación del módulo de adquisición programado.

En relación a la extracción de parámetros, cada ciclo es procesado y se extraen:

1. Características temporales, que son registradas en una matriz.
2. Vectores de cada uno de los índices de correlación temporal empleados
3. Índices de correlación espectral, empleando la FFT.

Algoritmos como *Sequential Forward Selection* (SFS) y *Sequential Floating Forward Selection* (SFFS) permiten determinar entre un conjunto de parámetros cuales son más discriminatorios [7, 11, 12]. Se seleccionaron los parámetros temporales para cada ciclo extraído de la señal en el eje Z y la señal de magnitud total, generando un vector con cada uno (Tabla 1). De cada matriz obtenida se calculan dos vectores que contienen el valor medio y la desviación estándar de cada parámetro temporal calculado.

Tabla 1: Parámetros temporales de las señales Z y magnitud de aceleración.

Parámetros de Z	Parámetros de magnitud
Valor RMS	Valor RMS
Energía	Energía
Longitud de forma de onda	Longitud de forma de onda
Desviación estándar	Desviación estándar
Media	Media
3^{er} momento (Skeness)	3^{er} momento (Skeness)
4^{to} momento (Kurtosis)	4^{to} momento (Kurtosis)
Aceleración máx.	Aceleración máx.
Aceleración mín.	Cantidad de muestras
Pico a pico	–

El cómputo de la correlación temporal se realiza mediante los índices de correlación de Pearson y Spearman entre cada ciclo con la señal promedio, y el algoritmo desarrollado almacena estos resultados en 4 vectores. Posteriormente se obtiene la media y la desviación de los índices contenidos en cada vector, con un total de 8 valores que sirven para la caracterización de la persona. Se computó el espectro de la señal promedio de cada patrón de caminar mediante la FFT. El cálculo se realiza con los métodos FFT de la librería Commons Math de Apache que aporta el método *FastFourierTransformer*. El espectro de un ciclo del patrón se compara con el de la señal de referencia del promedio usando las mismas técnicas de correlación aplicadas a los parámetros temporales.

En relación a la autenticación del usuario en base a los parámetros extraídos se desarrollaron dos métodos para hacer el proceso de autenticación del portador del móvil. El primer método, denominado *experimental*, se basa en la comparación de los valores estadísticos calculados, y el segundo en aplicar el algoritmo de machine learning, denominado K vecinos más cercanos (K-NN)

[13]. Para las validaciones de los métodos de autenticación se desarrolló una aplicación Java de escritorio llamada *MARCHEMOS*, empleando el IDE Netbeans, que permitió automatizar el análisis de los patrones. Se puede hacer elección de la base de datos a calcular y obtener los valores para una tabla específica, para conjunto de una base de datos o para varias bases de datos de un sujeto (Figura 8).

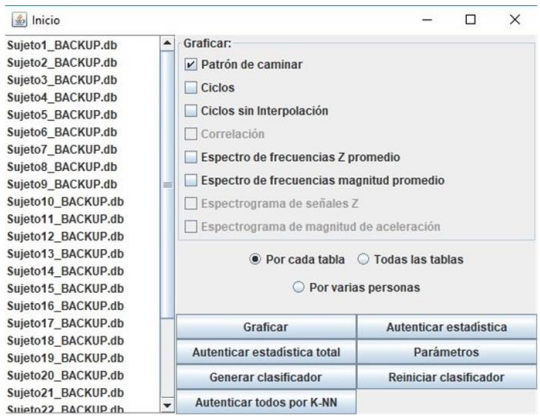


Figura 8: Aplicación *MARCHEMOS* desarrollada para el estudio y análisis de los patrones de locomoción.

Para la validación por el método experimental, con el propósito de comparar los patrones de cada una de las bases de datos obtenidas y constatar que cada persona posee una manera distintiva de caminar, se computó la correlación temporal de todos estos ciclos. Se estableció que la validación de las señales sería a 3 niveles: Correlación temporal, correlación espectral y comparación de parámetros (Figura 9). Para que una señal sea considerada como válida debe superar con éxito los criterios de los 3 niveles, devolviendo un valor de 1 con lo cual el sistema reconoce una autenticación correcta. Si la señal es descartada al no superar alguno de los niveles, se devuelve un valor de 0.

Figura 9: Método de validación experimental.

Alternativamente, se diseñó un método de validación basado en el algoritmo mencionado K-NN actuando como clasificador para llevar a cabo la autenticación del individuo. Un conjunto de bases de datos se usan para generar una matriz de características de referencia de individuos que representan usuarios no auténticos (impostores), mientras que una base de datos específica se emplea para generar una matriz de características que representan al patrón de caminar del usuario a identificar o auténtico. Otro conjunto de bases de datos representan los casos de prueba a los cuales se aplicará el clasificador. Para evitar que características con valores en una escala mayor influyan más que otras en la decisión, todos los valores son normalizados y estandarizados. El algoritmo fue probado usando la herramienta desarrollada *MARCHEMOS* empleando las bases de datos disponibles para formar el conjunto de referencia y prueba. El valor del parámetro k del fue seleccionado experimentalmente.

El objetivo es que las herramientas tengan por lo menos un 80 % de efectividad al momento de efectuar el proceso de autenticación, debido a que es un valor estadísticamente aceptable considerando todas las posibles variables que pueden afectar dicho proceso. Por otra parte, se considera que un evento es estadísticamente improbable si su probabilidad de ocurrencia es menor a 5 % [14].

Se desarrolló la aplicación final de seguridad con nombre *PasoSeguro*, programada en Java con el IDE Android Studio. Esta app es capaz de hacer la adquisición, autenticación y la toma de decisiones de seguridad en el momento que se detecte que un presunto impostor porta el dispositivo. El usuario debe registrar nombre, e-mail y número de teléfono alternativo para las notificaciones. Después se debe realizar la captura del patrón de caminar para tomarlo como referencia. Cada captura tiene una duración de 10 s en la que el sujeto debe caminar en línea recta (Figura 10).

Las pantallas principales de la app se observan en la Figura 11 y en la Figura 12 (navegación). Se diseñó la app con la capacidad para almacenar los patrones de caminar de dos usuarios diferentes, seleccionando uno de ambos para la autenticación

Posicionamiento del teléfono en el bolsillo

Adquisición de los datos, caminando

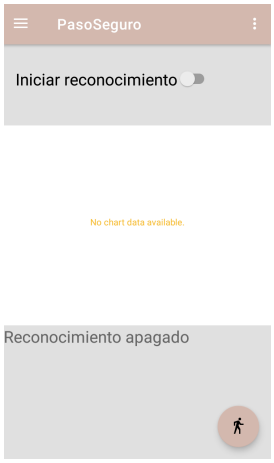
Figura 10: Proceso de captura de un patrón de marcha.

en tiempo real. Desde el *inicio* se puede acceder a las configuraciones de autenticación. Un usuario registrado con más de 5 patrones está habilitado para iniciar el proceso de autenticación en tiempo real. Una vez activado el proceso se ejecutan los algoritmos de autenticación desarrollados estableciendo como referencia todos los patrones de caminar disponibles. Este proceso se mantiene en ejecución hasta que el portador decida detenerlo.

Se recolecta una señal de 6 s, extrayendo los ciclos y realizar la autenticación. Si la autenticación se efectúa de manera correcta en un ciclo, el sistema devolverá un valor de 1, caso contrario, devolverá el valor 0. Luego de obtener los valores se vuelve a adquirir otra muestra de 6 s y así sucesivamente. Estos valores son almacenados en un vector que contiene máximo 100 muestras a la vez, eliminando los excedentes bajo un esquema FIFO. El porcentaje de validaciones correctas en el vector es representado gráficamente como se visualiza en la Figura 13.

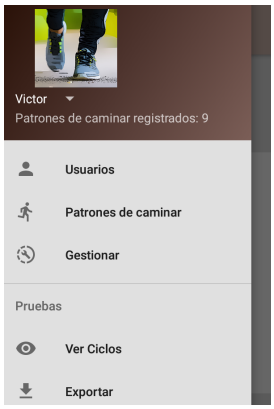
Si este valor se mantiene por debajo de un umbral, fijado según las pruebas, un contador registrará el tiempo transcurrido hasta que o bien el porcentaje de validaciones sobrepase el valor umbral y se reinicie el contador o se alcance el tiempo de reacción prefijado. Esto último desencadena la respuesta de seguridad programada (Alarma). El proceso de autenticación se resume en la Figura 14.

Como resultado de una autenticación que implique el posible hurto, el sistema de seguridad envía un mensaje de texto y un correo electrónico al número de teléfono y dirección de correo

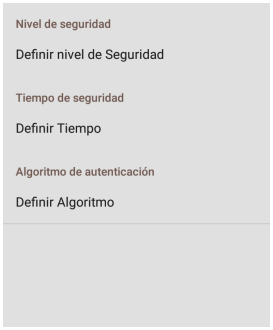


Inicio de la app

Registro de usuario



Panel de navegación



Configuraciones

Figura 11: Pantallas principales de la app *PasoSeguro*.

registrado. En el mensaje se notifica el uso no autorizado del dispositivo. El mensaje suministra la ubicación del portador mediante el GPS del teléfono. En la configuración se puede seleccionar uno de los algoritmos de autenticación desarrollados, además de elegir entre tres niveles de seguridad (bajo, medio y alto), lo cual modifica el valor de porcentaje umbral y parámetros de los algoritmos.

3. Análisis y discusión de resultados

En esta sección se analizan y discuten los resultados del empleo de la app con las herramientas desarrolladas en esta investigación, descritas en la sección 2 aplicada sobre varios sujetos de prueba. Los patrones de caminar obtenidos se grafican usando la app *MARCHEMOS*. En la Figura 15 se

Figura 12: Opciones del panel de navegación de la app *PasoSeguro*.

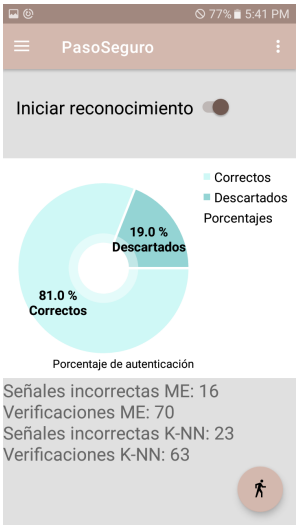


Figura 13: Porcentaje de verificaciones correctas respecto al total por método experimental.

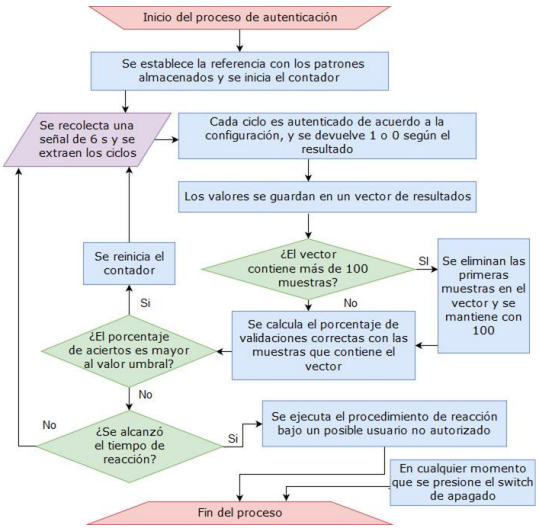


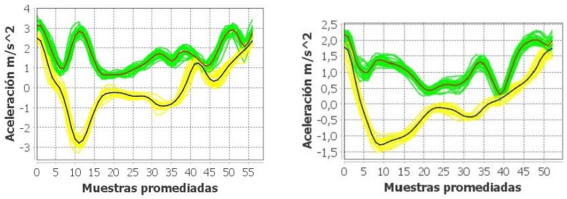
Figura 14: Diagrama de flujo del proceso de autenticación de la aplicación desarrollada.

muestran los patrones de caminar de las bases de datos de dos hombres y dos mujeres. Las señales del eje Z inician con un máximo positivo, pico que lo genera la pisada de la pierna donde se encuentra el móvil, seguidamente se observa que la señal cae a un pico negativo y fluctúa de forma característica para cada persona hasta el siguiente paso.

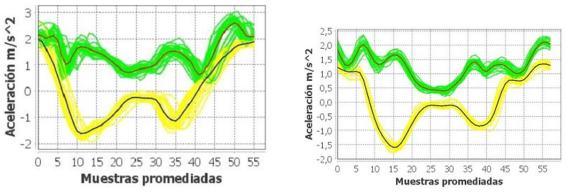
Comparando entre hombres y mujeres, en la caminata de un hombre se generan picos debido a la fuerza que se aplica al momento de la pisada. En contraste, para algunos casos de mujeres, los ciclos presentan diferencias notorias debido a lo suave de la pisada y hay casos donde se generan dos picos de aceleración con magnitudes similares cercanas (Figura 15 2do patrón femenino). La orientación de la pantalla del dispositivo dentro del bolsillo fue un factor importante. La pantalla del móvil se posicionó hacia afuera del pantalón. El efecto de las dos posibles orientaciones del móvil se ilustra en la Figura 16. El efecto del cambio es la inversión desplazada de la señal Z.

En otro orden, se observó que el estado anímico de un individuo afecta su biomecánica. Si una persona está nerviosa, tiende a apresurar el paso; por el contrario, cuando la persona se encuentra triste o cansada las zancadas se tornan más lentas e irregulares (Figura 17).

En relación al efecto del calzado y del terreno, se observó que un zapato alto (bota) repercute en la amortiguación de la zancada y por ende en la forma de onda. Para el caso de las mujeres fue evidente

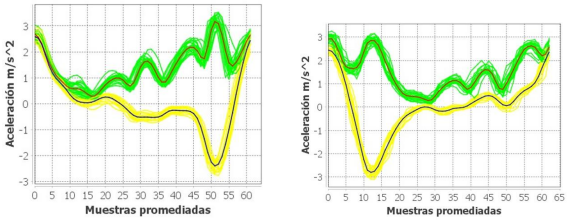


1er patrón masculino 2do patrón masculino



1er patrón femenino 2do patrón femenino

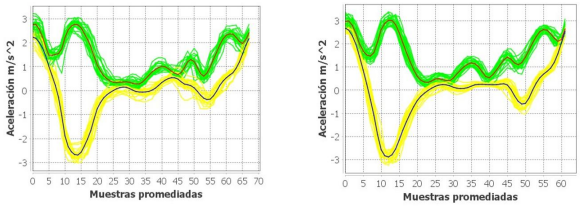
Figura 15: Patrones de caminar de señales Z y de magnitud.



Pantalla hacia adentro Pantalla hacia afuera

Figura 16: Efecto de la orientación del teléfono respecto al eje Z en la adquisición de datos.

Patrón adquirido a una persona

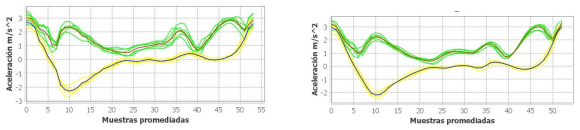


en estado de cansancio físico en estado neutral de actividad

Figura 17: Efecto del estado físico de la persona en la adquisición de datos.

que el uso de tacones modifica su forma de caminar. De igual manera el terreno influyó al momento de la captura de datos. Si la superficie es irregular se agrega ruido al patrón de la persona (Figura 18).

En la Figura 19 se exhiben dos patrones femeninos, de mujeres de 24 y 16 años de edad, con 1,69 y 1,60 m de altura respectivamente. Existe cierta similitud en sus señales promedio, aunque es apreciable que no son iguales. Es notable el parecido en el promedio de Z. Se observó que, en

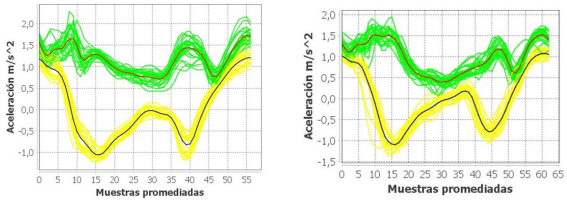


Caminando sobre asfalto Caminando sobre granito liso

Figura 18: Efecto del terreno en la adquisición de datos de la misma persona.

general, en el patrón de una persona tomado en un momento determinado la señal en Z presenta menos dispersión que la de magnitud, como se ve en las dos señales de la Figura 19.

Patrón femenino para la comparación



24 años y 1,69 m de altura 16 años y 1,60 m de altura

Figura 19: Similitud de dos patrones femeninos para la comparación de la señal Z y magnitud de aceleración.

Sin embargo, la señal de magnitud es más característica para una persona en particular, y más discriminatoria. Con respecto a la comparación entre bases de datos de un mismo sujeto, un individuo puede tener variaciones en su patrón en diferentes espacios temporales y situacionales, por lo que a algunos sujetos se les recolectó más de una base de datos. En algunos casos los valores de los ciclos extraídos distan de forma considerable entre bases de un solo individuo, como los que se muestra en la Figura 20, que fueron adquiridos de un sujeto de pruebas A. Aunque tienen un alto grado de similitud (ya que provienen de la misma persona), es evidente que presentan diferencias entre las señales Z.

En el dominio frecuencial se observan las diferencias entre los armónicos de cada señal promedio, resaltando la desigualdad de los tamaños de la componente continua de magnitud de aceleración (Figura 21). Esto puede ocurrir debido a factores como una pisada más fuerte, un calzado que presente menos amortiguación, el estado de ánimo de la persona o una forma de caminar

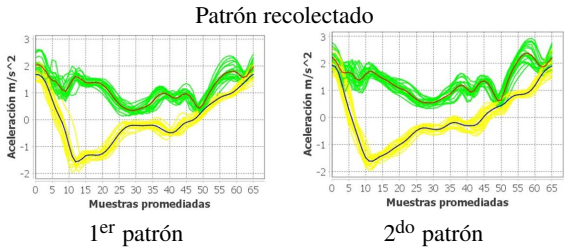


Figura 20: Comparación de dos patrones recolectados de un sujeto A en momentos diferentes.

anómala que presente diferencias marcadas entre un ciclo y otro (marcha festinante o la marcha espástica [15]).

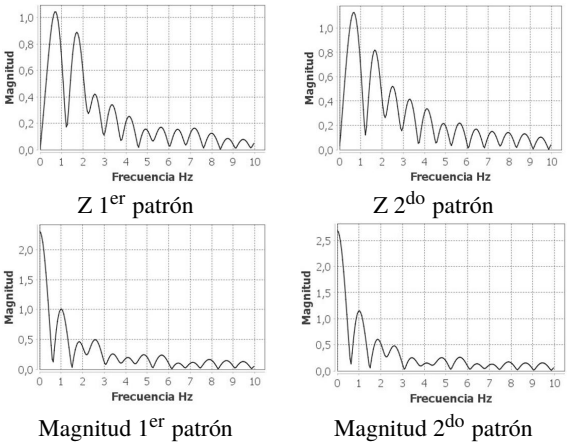


Figura 21: Espectros de las señales promedio de aceleración Z y de magnitud del sujeto A.

Por el contrario, hubo personas que mantuvieron su patrón más constante dentro de las bases obtenidas ya que entre una recolección y otra sus patrones no discreparon considerablemente. Un ejemplo es el caso de un sujeto de pruebas B que posee dos bases de datos (Figura 22). En cuanto al criterio de correlación espectral, se computa la FFT y los índices de correlación espectral. Se determinó que para los ciclos de una misma persona, el índice de Pearson de magnitud es mayor a 0,989, mientras que los tres restantes (Pearson Z, Spearman Z y magnitud) fluctúan más. Por ello, para emplear la correlación espectral como medida discriminatoria sólo se usó el índice Pearson de magnitud. Si éste es mayor a 0,989, la señal bajo estudio pasa a la última etapa de la autenticación, caso contrario es descartada.

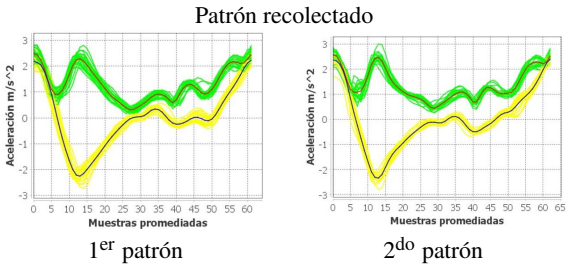


Figura 22: Comparación de dos patrones recolectados de un sujeto de pruebas B en momentos diferentes.

En la última etapa de la validación se comparan los parámetros temporales del ciclo de prueba y las referencias. Esto se realiza a través de un sistema de puntajes, donde la señal de prueba acumula puntos por cada parámetro que coincida con los de referencia, con un valor inicial de 0 puntos y según lo siguiente: Si un parámetro cae dentro del rango de la media más o menos tres desviaciones estándar, al acumulado se le suman 0,2 puntos, si el rango es de más o menos dos desviaciones se le suman 0,8 puntos y si el rango es de más o menos una desviación, se le suma 1 punto. Al comparar los primeros 4 parámetros de ambas señales: Valor RMS, energía, longitud y desviación estándar, estos se multiplican por 1,5 para darles más peso, ya que se consideran más discriminatorios [11]. El máximo acumulado posible es 26 puntos. Para que un ciclo sea válido debe acumular al menos 15,4 puntos, valor establecido por experimentación, como un balance entre la cantidad de falsos positivos y verdaderos negativos. Si la señal pasa estas tres etapas, se autentican el portador de manera correcta (dueño).

En relación a los resultados de la autenticación por el método experimental, a través del uso de la herramienta *MARCHEMOS*, se comprobó la eficacia del método, obteniendo resultados de cada nivel de seguridad al comparar cada base de datos de los sujetos de prueba con todas las demás, determinando los porcentajes de los ciclos autenticados correctamente y de los falsos positivos. Usando *MARCHEMOS* (Figura 23) se obtienen los resultados de autenticación: Seleccionando un sujeto de la lista y pulsando el botón *Autenticar estadística*, se autentica la base

de datos de del individuo contra todas las demás y sus propios valores, dando como resultado el porcentaje de ciclos autenticados correctamente y de falsos positivos para cada una de las etapas del método (Figura 24).

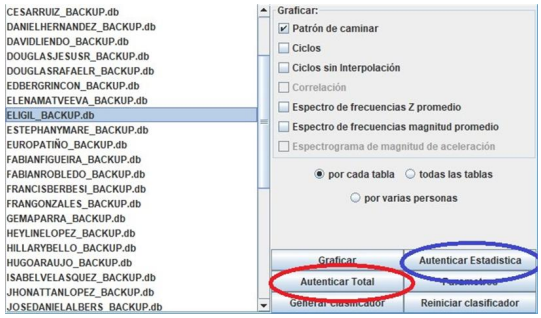


Figura 23: Aplicación *MARCHEMOS* para la autenticación por el método experimental.

```
Comparaciones Totales: 1854 , Mismo sujeto: 47 , Con otros sujetos: 1807
Verificaciones del mismo sujeto:
Por Correlación Temporal: 44 , Porcentaje: 93,62%
Por Correlación Temporal y Espectral: 42 , Porcentaje: 89,36%
Verificaciones Totales: 42 , Porcentaje: 89,36%
Falsos positivos en las verificaciones con otros sujetos:
Por Correlación Temporal : 130 , Porcentaje: 7,19%
Por Correlación Temporal y Espectral: 60 , Porcentaje: 3,32%
Falsos positivos totales : 16 , Porcentaje: 0,89%
```

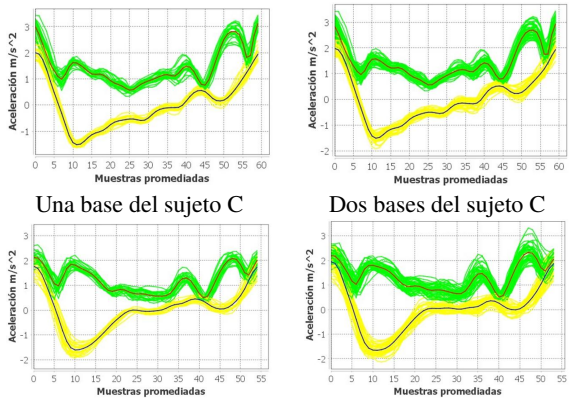
Figura 24: Resultados obtenidos de la autenticación de la base de datos de una sola persona.

Las validaciones correctas (verdaderos positivos) se calculan en base a la comparación de la referencia de una persona contra todos los ciclos de ese mismo sujeto, y cuando los resultados no son exitosos se les denota como falsos negativos: Ciclos correctos que no superan la validación y se catalogan por error como un presunto impostor. Los falsos positivos, por el contrario, se obtienen de la comparación entre una base específica contra todas las demás, por lo que este parámetro representa la cantidad de sujetos impostores que pueden ser autenticados erróneamente como verdaderos. El botón *Autenticar estadística total*, computa la autenticación entre todas las bases (Figura 25).

En la Figura 26 se ven los patrones de dos sujetos C y D con respecto a una y dos bases de datos. C mantiene la simetría entre los diferentes ciclos por lo que no hay cambios considerables en el patrón, pero D presenta ciclos con más dispersión. En la Tabla 2 para C y D se muestra el proceso

```
Número total de comparaciones de un mismo sujeto: 1854
Pasaron la primera fase: 1706  , segunda: 1687  , tercera: 1642
Número total de comparaciones sujeto impostor: 87138
Pasaron la primera fase: 4964  , segunda: 3407  , tercera: 1306
Sujetos de prueba: 48, Bases totales comparadas: 78
Desviación de las verificaciones: 9,97 Media: 88,18
Desviación de los falsos positivos: 1,78 Media: 1,50
Porcentaje promedio de verificaciones por Correlación Temporal: 91,29%
Porcentaje promedio de Verificaciones por Correlación Temporal y Espectral: 90,22%
Porcentaje promedio de Verificaciones Totales: 88,18%
Porcentaje promedio de Falsos positivos por Correlación Temporal : 5,69%
Porcentaje promedio de Falsos positivos por Correlación Temporal y Espectral: 3,90%
Porcentaje promedio de Falsos positivos totales : 1,50%
```

Figura 25: Resultados obtenidos de la autenticación de todas las bases.



Una base del sujeto C | Dos bases del sujeto C

Una base del sujeto D | Dos bases del sujeto D

Figura 26: Comparación entre los patrones recolectados de una y dos bases de datos, para los sujetos C y D.

Tabla 2: Porcentajes de la autenticación de los sujetos C y D, cuando se tienen una y dos bases de datos de referencia.

Número de bases de referencia	Sujeto	Validaciones correctas %	Falsos positivos %
1	C	89,36	1,09
2	C	97,87	1,15
1	D	59,27	0,92
2	D	78,72	3,05

de autenticación, fijando como referencia los datos extraídos de una y dos de sus bases por separado.

Las estadísticas de C sugieren que una sola base de referencia es capaz de obtener resultados adecuados. Se consideró también a un sujeto E al que se le extrajeron 8 bases de datos de locomoción. Se extrajo el patrón de la combinación de las 8 bases (Figura 27, con autenticación según la Figura 28).

Aún si los criterios se hacen respecto a 8 bases, la ocurrencia de falsos positivos se mantiene baja. En la Tabla 3 se muestran los resultados de la

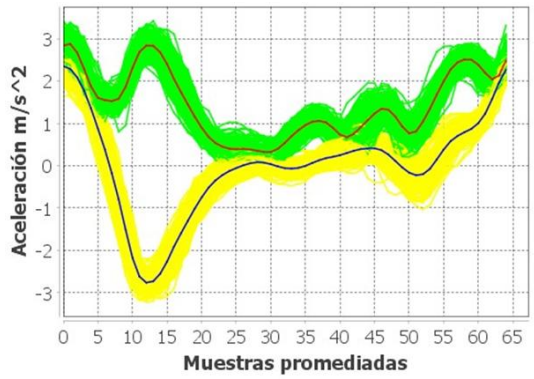


Figura 27: Patrón resultante del procesamiento de 8 bases de datos distintas de un solo individuo (sujeto E).

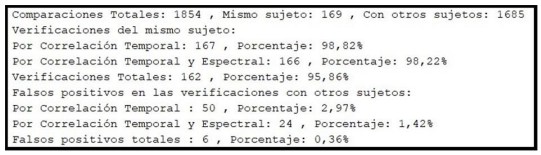


Figura 28: Resultado de la autenticación del patrón proveniente de 8 bases distintas de un solo individuo.

autenticación cuando se usan una, dos y tres bases para generar los criterios. Se realizó además la autenticación total de 48 sujetos (todos contra todos), incluyendo las bases extra. Se elaboraron los histogramas obtenidos para cada uno de los 48 sujetos, con el fin de conocer el tipo de distribución que presentan los resultados (Tabla 4).

Tabla 3: Porcentajes de la autenticación del sujeto E cuando se usan una, dos y tres bases distintas como referencia.

Número de bases de referencia	Validaciones correctas %	Falsos positivos %
1	55,62	0,12
2	68,05	0,25
3	92,90	0,50

En relación al estudio estadístico realizado cuando se aplica el método experimental de autenticación de un usuario, se empleó el método de prueba de hipótesis. Se usó la distribución t-student con prueba de dos colas, típico de

Tabla 4: Diferentes métodos de autenticación según una o varias bases de datos.

Método de autenticación	Criterio	Validaciones correctas %	Falsos positivos %
Comparando el uso de. criterios de decisión para una y múltiples bases de un sujeto	Una base de referencia	76,90	1,04
	Múltiples bases de referencia	88,18	1,50
Una sola base de datos como referencia	Correlación temporal	84,40	4,37
	Correlación espectral	88,89	9,00
	Parámetros temporales	86,51	9,05
Todas las bases disponibles por sujeto como referencia	Correlación temporal	91,29	5,69
	Correlación espectral	94,49	10,71
	Parámetros temporales	96,36	12,38

estas pruebas [14]. En este sentido los resultados de la autenticación del usuario por el método experimental fueron:

- Se tiene una confianza del 95 % de que el valor medio de efectividad del método experimental se encuentra entre 85,28 % y 91,08 %.
- Se tiene una confianza del 95 % de que el error medio del método experimental para autenticar falsos positivos se encuentra entre 0,98 % y 2,02 %.
- Se rechaza la hipótesis nula para los experimentos de la comparación entre los datos de un mismo sujeto, ya que los resultados sustentan la aseveración: el porcentaje de eficacia del método experimental para autenticar a una persona correctamente es de al menos un 80 %.
- Se rechaza la hipótesis nula para los experimentos de la comparación entre un sujeto y todos los demás, ya que los resultados sustentan la aseveración: el porcentaje de autenticación para un presunto sujeto impostor con el método experimental es a lo sumo 5 %.

A continuación se describen los resultados de autentificación empleando el método alternativo del algoritmo K-NN, programado en *MARCHE-MOS*, con las bases de datos recolectadas como sujetos de prueba. La herramienta computa falsos positivos, verdaderos negativos, falsos negativos y verdaderos positivos, empleados en las pruebas estadísticas. Ofrece la capacidad de efectuar la autenticación de algún usuario seleccionado de la lista contra los restantes, arrojando resultados parciales referentes al sujeto elegido, que será etiquetado como auténtico mientras que el resto como impostores. Luego de generado el modelo, el botón *Generar clasificador* cambia de nombre a *Autenticar sujeto* para que se efectúe la validación con el resto de bases de datos del listado, ciclo a ciclo. La opción *Autenticar todos por K-NN* consta de una autenticación al estilo "todos contra todos", en la que cada base de datos por separado de un sujeto de una lista de 70 bases sirve como auténtico y es comparado contra otra lista, conformada por los sujetos de la primera. Los resultados de esta opción (Figura 29), son los empleados en la posterior prueba estadística.

```
Comparaciones entre bases de un mismo sujeto: 39
Bases totales comparadas: 70
Porcentaje promedio de falsos positivos: 6,57%
Desviación de falsos positivos: 3,67
Porcentaje promedio de falsos negativos: 27,65%
Porcentaje promedio de verdaderos positivos: 72,35%
Desviación de verdaderos positivos: 17,89
Porcentaje promedio de verdaderos negativos: 93,43%
```

Figura 29: Resultados de la autenticación total por el método K-NN.

El algoritmo determina los K vecinos más cercanos y cataloga cada uno entre auténtico o impostor. Cada vecino que contribuye al contador de auténticos o de impostores genera un voto que es pesado por el inverso de la distancia. Esto asegura que vecinos más cercanos influyen más en la decisión final. La elección de emplear votos pesados para la toma de decisión del clasificador surge en función de la distribución de los parámetros temporales que son extraídos en las matrices de referencia. En la Figura 30 se observa una gráfica de dispersión de 2 de los 9 parámetros temporales. En color verde se ilustran los puntos de cada ciclo de la matriz referencial del sujeto auténtico mientras que en color rojo se muestran los puntos de cada ciclo de la matriz referencial de impostores.

Debido a la dispersión que presentan los puntos de un impostor se decidió que, para asumir un ciclo de caminar como auténtico, no solo basta con la sumatoria de votos, sino que esta debe ser superior a un valor umbral (denominado T_{knn}). Este valor umbral es seleccionado en función del valor del parámetro K.

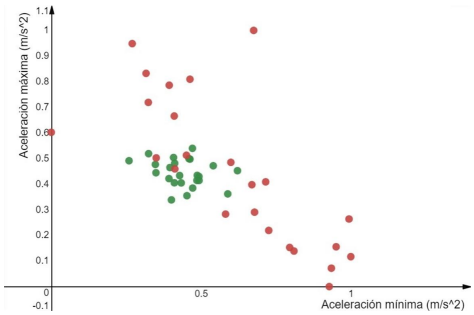


Figura 30: Diagrama de dispersión de la aceleración mínima versus aceleración máxima.

Se realizó el experimento para distintos valores de K y valores umbrales para determinar cuáles generaban los mejores resultados. Se observó que $K = 3$ presenta el mayor porcentaje de verdaderos positivos. Entre $K = 5$ y $K = 9$ ambos porcentajes se mantienen aproximadamente constantes, con el menor porcentaje de falsos positivos en $K = 9$. El valor de K a seleccionar debe ofrecer un bajo porcentaje de falsos positivos (dificultad para el rechazo de impostores) pero con un considerable porcentaje de verdaderos positivos. El valor de $K = 7$ presenta dichas condiciones, con el segundo menor porcentaje de falsos positivos (6,57 %) y un 72,35 % de verdaderos positivos. Estos porcentajes para un valor de $K = 7$ fueron logrados especificando un $T_{knn} = 8$. En cuanto a la capacidad de rechazo que ofrece el valor umbral resultó que para un valor de $T_{knn} = 8$ gran parte de los votos como auténticos para un usuario impostor se ubican por debajo del umbral, contrario a los votos de un usuario realmente auténtico, siendo así catalogado como impostor. En relación al estudio estadístico efectuado cuando se aplica el método K-NN de autenticación de un usuario, análogo en metodología al que se usó en el

método experimental, los resultados de la prueba de hipótesis aplicada a la autenticación K-NN del usuario por el método experimental son:

- Se tiene una confianza del 95 % de que el valor medio de efectividad de la autenticación por K-NN se encuentra entre 66,56 % y 78,14 %.
- Se tiene una confianza del 95 % de que el valor medio de error por K-NN para autenticar falsos positivos se encuentra entre 5,69 % y 7,45 %.
- Los estadísticos de prueba obtenidos no entran dentro de los rangos porcentuales que se establecieron previamente para medir la efectividad del método.

Una vez programados en el app *PasoSeguro* los algoritmos de autenticación (método experimental y K-NN) se realizaron pruebas sobre ese sistema. Para las pruebas previas se usaron 4 modelos de teléfonos inteligentes: Google phone Nexus 5, Doogee Xpro 5, Alcatel Cameox y Samsung Galaxy J3 Luna Pro, resultando éste último el seleccionado para probar el desempeño de la autenticación. Primero se evaluaron las validaciones correctas (verdaderos positivos). Para este fin, dos sujetos X y Y adquirieron 10 muestras de 10 s. Se realizó el experimento en dos escenarios, uno en piso de granito liso y otro en acera de calle. Se realizaron 3 pruebas para cada escenario y usuario. En la Figura 31 se muestran dos de los resultados obtenidos del sujeto X directamente de la aplicación y en la Tabla 5 se presentan los resultados logrados para cada escenario en ambos usuarios. Se observó que la autenticación K-NN presenta valores más altos que los obtenidos por el método experimental. Esto se debe a la gran cantidad de puntos que se utilizan en la comparación K-NN, con una referencia variada, aumentando la posibilidad de autenticación. Los valores obtenidos mejoran cuando el terreno es regular. Seguidamente, se presentan los resultados para 4 sujetos R1, R2, R3 y R4, realizándose la autenticación con las referencias de los sujetos X y Y, con dos pruebas por persona.

En la Figura 32 se muestran los resultados obtenidos para R1 y R2, usando como referencia

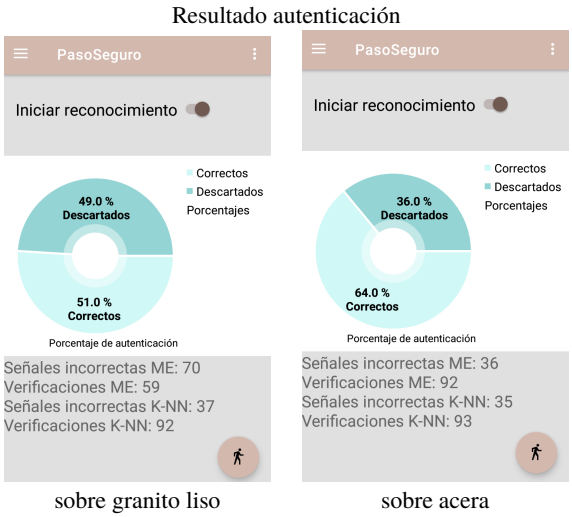


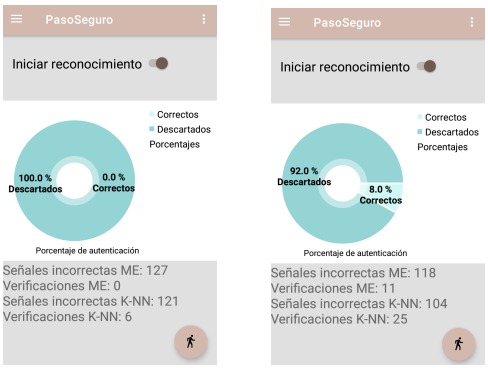
Figura 31: Resultados de la autenticación de la app *PasoSeguro* para el usuario X en dos terrenos diferentes.

Tabla 5: Resultados de las pruebas de verificación de la app *PasoSeguro*.

Usuario	Tipo de terreno	Prueba	Método experimental %	Método K-NN %
X	Granito liso	1	71,88	72,56
X	Granito liso	2	76,34	75,28
X	Granito liso	3	66,86	69,22
X	Acera de calle	1	45,74	71,32
X	Acera de calle	2	51,23	71,08
X	Acera de calle	3	40,54	66,34
Y	Granito liso	1	76,83	77,69
Y	Granito liso	2	70,34	73,27
Y	Granito liso	3	74,86	80,06
Y	Acera de calle	1	48,73	72,54
Y	Acera de calle	2	55,65	74,27
Y	Acera de calle	3	52,35	68,43

los patrones de X, en escenarios distintos. En la Tabla 6 se presentan los resultados obtenidos en el primer escenario con los 4 usuarios y en la Tabla 7 se muestran los de los cuatro sujetos en el segundo escenario. Los resultados del método experimental son más discriminatorios que los de K-NN, debido

a que es más probable que dos personas tengan valores similares en sus parámetros temporales a que las formas de onda de los patrones tengan un alto grado de correlación. Por ello la cantidad de falsos positivos del método experimental es mucho menor que la del K-NN.



usuario R1, acera de calle usuario R2, granito liso

Figura 32: Resultados de la autenticación de la app *PasoSeguro*, para R1 y R2 en prueba de la capacidad de rechazo, empleando la referencia del patrón de un sujeto X.

Tabla 6: Resultados de las pruebas respecto a la capacidad de rechazo de la app *PasoSeguro*, usando la referencia de dos sujetos X y Y, en el primer escenario (piso de granito liso).

Usuario	Prueba	Sujeto de referencia	Método experimental %	Método K-NN %
R1	1	X	8,53	19,38
R1	2	X	9,76	24,26
R1	1	Y	0,00	1,56
R1	2	Y	0,00	0,00
R2	1	X	1,49	4,72
R2	2	X	0,00	3,27
R2	1	Y	3,58	12,24
R2	2	Y	2,83	7,56
R3	1	X	0,00	2,73
R3	2	X	0,43	1,67
R3	1	Y	2,30	4,37
R3	2	Y	1,56	5,71
R4	1	X	0,00	3,65
R4	2	X	0,00	0,78
R4	1	Y	4,58	17,52
R4	2	Y	4,97	16,85

El algoritmo K-NN, aunque presenta una probabilidad de error mayor, aún puede ser empleado si tiene valores umbrales más altos.

Tabla 7: Resultados de las pruebas respecto a la capacidad de rechazo de la app *PasoSeguro*, usando la referencia de dos sujetos X y Y, en el segundo escenario (acera de calle).

Usuario	Prueba	Sujeto de referencia	Método experimental %	Método K-NN %
R1	1	X	3,61	17,43
R1	2	X	2,58	20,56
R1	1	Y	0,00	3,50
R1	2	Y	0,00	0,00
R2	1	X	0,00	3,40
R2	2	X	0,00	4,72
R2	1	Y	1,49	10,30
R2	2	Y	0,80	6,73
R3	1	X	0,00	1,53
R3	2	X	0,00	0,00
R3	1	Y	0,00	3,95
R3	2	Y	0,00	2,43
R4	1	X	0,00	0,00
R4	2	X	0,00	2,79
R4	1	Y	2,60	20,43
R4	2	Y	4,54	18,60

Los niveles umbrales se fijaron con los valores presentes en la Tabla 8. La autenticación por K-NN se muestra como la más indicada para estas situaciones.

Tabla 8: Valores umbrales para los distintos niveles de seguridad en ambos métodos de autenticación desarrollados.

Nivel de seguridad	Método experimental (%)	K-NN (%)
Bajo	20	30
Medio	30	45
Alto	40	60

En lo relativo a la reacción de seguridad posterior a la autenticación, la app genera una respuesta en función del nivel de seguridad (Tabla 8). Al finalizar el tiempo de seguridad y de no cumplirse el requerimiento de nivel umbral es enviado un e-mail de advertencia la dirección preestablecida, notificando de un presunto caso de hurto debido a que el portador del dispositivo no ha podido ser identificado, enviando las coordenadas geográficas capturadas por el GPS del móvil. El correo electrónico ofrece un enlace

a través del botón *Ubicar* en Google Maps y se ubica un puntero en la posición geográfica dada por las coordenadas obtenidas del GPS. Simultáneamente se envía un SMS al número de teléfono preestablecido, con información similar. Se evaluó el rendimiento computacional de la app final mediante la herramienta de software *Android Profiler,* en términos de ocupación de RAM, consumo de CPU y consumo de datos de red. Para esto se utilizó un teléfono Samsung Galaxy J3 Luna Pro de 1,5 GB de RAM y procesador de 1,4 GHz. Sin dar inicio a ningún proceso de registro o de autenticación la app llega a ocupar entre 40 y 60 MB de RAM, la cual no llega a representar un 10 %. El uso del CPU es constante en torno al 17 %, durante el lapso de tiempo que toma ingresar los datos de un usuario hasta que finaliza el registro del patrón. La RAM ocupada asciende hasta unos 79 MB para luego disminuir. Se midió el consumo de recursos también durante la autenticación. En esta etapa para el método experimenta el consumo de CPU es mínimo durante el lapso que dura el proceso, presentando picos que no sobrepasan un 10 % de consumo en cada nueva recolección de datos. La ocupación de RAM se mantuvo relativamente constante en 45 MB. Para el caso del uso del algoritmo K-NN, los resultados fueron similares.

4. Conclusiones

En relación al desarrollo del módulo de adquisición de datos se determinó que el mismo requirió no sólo de etapas de filtrado de ruido, sino también de la aplicación adicional de diezmado e interpolación para el ajuste del tamaño de las muestras. En cuanto a la construcción de una base de datos de patrones de locomoción de distintos sujetos, resultó conveniente seleccionar el motor de bases de datos SQLite de Android, por ser una opción que presentó flexibilidad durante la ejecución de las pruebas de almacenamiento y edición de datos. Parámetros temporales y estadísticos se pueden extraer de las señales de locomoción y cuáles resultaron ser los más discriminatorios para su empleo en la autenticación. Esto derivó en el desarrollo de dos métodos de reconocimiento: el método experimental y el algoritmo K-NN. La app programada fue capaz de adquirir y almacenar los datos del patrón de locomoción de un usuario y establecerlos como referencia para la autenticación en tiempo real, empleando los dos métodos desarrollados en el ambiente de software creado.

En relación al estudio estadístico realizado para estimar la confiabilidad se observó que el método experimental es más discriminatorio y presenta probabilidades de autenticar erróneamente a un usuario no autorizado menores a 5 %. El algoritmo K-NN mostró flexibilidad y capacidad de autenticación de verdaderos positivos, a costo del aumento del margen de error por falsos positivos. Se determinó la conveniencia de adquirir una variada cantidad de patrones de locomoción de un mismo individuo, para mejorar la efectividad de la autenticación. La evaluación de los distintos patrones de locomoción de sujetos de la base de datos permitió observar que los mismos se ven afectados por factores externos tales como el tipo de terreno o de calzado. A medida que estos factores no presenten una gran variación entre el momento en que se tomó el patrón de referencia del individuo y cuando se realizó el proceso de autenticación, los resultados obtenidos por la aplicación serán más precisos.

El desarrollo de los métodos de autenticación permitió observar que, a pesar de que los factores externos afectan los valores de las muestras, la forma de onda del patrón de locomoción generalmente conserva la distribución relativa entre muestras pudiendo aseverar que la correlación empleada como método de comparación entre señales es un criterio más robusto que el uso de los parámetros temporales. El estudio del espectro de los patrones de los sujetos de prueba dio paso al uso de los índices de correlación como una herramienta para ser implementada en la comparación de señales a nivel frecuencial. De los resultados de este tipo de correlación se puede afirmar que la marcha humana también presenta características con capacidades discriminatorias entre distintos patrones.

El protocolo de reacción incluyó los mensajes que alertan sobre un posible porte no autorizado del teléfono móvil permitiendo el conocimiento de

la ubicación geográfica aproximada del dispositivo vía GPS. Esta cualidad concede la posibilidad de recuperar el teléfono en un evento de pérdida.

En relación al desempeño computacional, la app requiere de una RAM mayor a 90 MB. Es conveniente un teléfono celular de gama media o alta con un mínimo de 1 GB de RAM para que la aplicación no afecte perjudicialmente el rendimiento del dispositivo. Para finalizar, puede señalarse que los casos de error en la autenticación son poco probables (menores a 5 % para autenticación por método experimental), determinándose que la autenticación a través de señales de locomoción es lo suficientemente distintiva y asertiva en cada sujeto, en la medida adecuada para justificar su empleo bajo los escenarios expuestos, otorgando viabilidad al prototipo de app objeto del estudio.

Reconocimiento

El presente Trabajo Especial de Grado fue reconocido con Mención Honorífica por la Escuela de Ingeniería de Telecomunicaciones de la Facultad de Ingeniería de la Universidad de Carabobo (Venezuela), quien declaró que los motivos para ello se deben al enfoque transdisciplinario aplicado al haber integrado en forma coherente e innovadora diversas áreas del conocimiento, que incluyeron la biomecánica, el procesamiento de señales, las técnicas de machine learning y la teoría de decisiones.

5. Referencias

[1] N. Boulgouris, D. Hatzinakos, and K. Plataniotis. Gait recognition: a challenging signal processing technology for biometric identification. *IEEE Signal Processing Magazine*, 22(6):78–90, Nov 2005.

[2] A. Kale, A. Roychowdhury, and R. Chellappa. Fusion of gait and face for human identification. In *2004 IEEE International Conference on Acoustics, Speech, and Signal Processing*, volume 5, pages V–901, May 2004.

[3] A. Kale, A. Sundaresan, A. Rajagopalan, N. Cuntoor, A. Roy-Chowdhury, V. Kruger, and R. Chellappa. Identification of humans using gait. *IEEE Transactions on Image Processing*, 13(9):1163–1173, Sep. 2004.

[4] A. Bayat, M. Pomplun, and D. Tran. A study on human activity recognition using accelerometer data from smartphones. *Procedia Computer Science*, 34:450–457, 2014.

[5] L. Cedeño, M. Fagúndez, R. Briceño-León, A. Camardiel, A. Chacón, M. Capriles, M. Tarre, J. Mayorca, C. Marín, A. Rebolledo, F. Esquerre, y P. Rondón. 1^{er} Informe del observatorio de delito organizado en Venezuela. Visibilizando lo que hay detrás de la criminalidad. Venezuela, 2015.

[6] N. Clarke and S. Furnell. Authentication of users on mobile telephones–a survey of attitudes and practices. *Computers & Security*, 7(24):519–527, 2005.

[7] T. Hoang, D. Choi, V. Vo, A. Nguyen, and T. Nguyen. A lightweight gait authentication on mobile phone regardless of installation error. In L. Janczewski, H. Wolfe, and S. Shenoi, editors, *Security and Privacy Protection in Information Processing Systems*, pages 83–101, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[8] D. Winter. *Biomechanics and motor control of human movement*. John Wiley & Sons, 4^a edition, 2009.

[9] G. Bajrami. Activity identification for gait recognition using mobile devices. Master's Thesis, Department of Computer Science and Media Technology, Gjøvik University College, 2011.

[10] M. Ehatisham-ul-Haq, M. Azam, J. Loo, K. Shuang, S. Islam, U. Naeem, and Y. Amin. Authentication of smartphone users based on activity recognition and mobile sensing. *Sensors*, 17(9):1–31, 2017.

[11] H. Thang, V. Viet, N. Dinh, and D. Choi. Gait identification using accelerometer on mobile phone. In *2012 International Conference on Control, Automation and Information Sciences (ICCAIS)*, pages 344–348, Nov 2012.

[12] J. Kwapisz, G. Weiss, and S. Moore. Activity recognition using cell phone accelerometers. *ACM SigKDD Explorations Newsletter*, 12(2):74–82, 2011.

[13] S. Imandoust and M. Bolandraftar. Application of k-nearest neighbor (knn) approach for predicting economic events: Theoretical background. *Int. Journal of Engineering Research and Applications*, 3(5):605–610, 2013.

[14] M. Triola. *Estadística*. Pearson Educación, 10^{ma} edition, 2004.

[15] A. Jain and A. Ross. Introduction to biometrics. In A. Jain, R. Bolle, and S. Pankanti, editors, *Biometrics: Personal Identification in Networked Society*, pages 1–42. Springer, 2008.