AUTENTICACIÓN MULTIFACTOR CON EL USO DE UN SENSOR KINECT

MULTIFACTOR AUTHENTICATION USING A KINECT SENSOR

Fatima Moumtadi
Ph. D. en Televisión
Universidad Nacional Autónoma de México
México D.F., México
fatima@fi-b.unam.mx

Luis Alfonso García-Vázquez
M.I. Telecomunicaciones
Universidad Nacional Autónoma de México
México D.F., México
loualph@gmail.com

Resumen– **En este trabajo se desarrolló un sistema de autenticación multifactor empleando el sensor Kinect y equipo de cómputo. Se utilizó programación en lenguaje C# con el ambiente de desarrollo y las herramientas que provee el fabricante para el sistema operativo Windows. Se eligió una combinación de métodos de autenticación con el fin de reducir la capacidad que tiene un usuario no autorizado de ser elegible para tener acceso a un determinado sistema o lugar. Se seleccionaron cinco métodos para conseguir la autenticación multifactor, cubriendo las tres categorías de métodos de autenticación: Llaves de información, Llaves físicas y Llaves biométricas, basadas respectivamente en algo que la persona sabe, algo que la persona posee y algo que la persona es. Se consiguió un sistema de autenticación confiable, robusto y sencillo de usar, privilegiando la confiabilidad y disminuyendo la complejidad de cada uno de los métodos individuales. Se demostró que es posible desarrollar un sistema de autenticación multifactor con un sensor Kinect.**

Palabras clave– **Autenticación, Kinect, multifactor.**

Abstract– **In this paper a multifactor authentication system by using Kinect sensor and computer equipment was developed. It was used the C# language for coding with the development environment and tools provided by the manufacturer for Windows operating system, to choose a combination of authentication methods to reduce the ability of a non-authorized user to be eligible to access a certain place or system. Five methods were chosen to obtain the multifactor authentication, covering the three categories of authentication methods: Information keys, physical keys and biometric keys, based respectively in something the person knows, something the person has and something the person is. A reliable, robust and easy to use authentication system was achieved, favoring the reliability and reducing the complexity of each of the individual methods. It proved to be possible to develop a multifactor authentication system with Kinect sensor.**

Keywords– **Authentication, Kinect, multifactor**

1. INTRODUCCIÓN

Las tecnologías de la información y la comunicación cada vez tienen más importancia en la vida cotidiana, ya que las computadoras se han vuelto de uso común. Debido a la cantidad y tipo de nuevos usos, existe una creciente necesidad de garantizar su correcto funcionamiento así como su operación adecuada. Por otro lado, existen malos usos de los equipos de cómputo y es necesario contar con sistemas que garanticen su seguridad [1].

La autenticación es un elemento esencial de un modelo de seguridad. Es importante distinguir entre la autenticación y la autorización, que es otro elemento importante en un plan de seguridad. La autenticación comprueba la identidad de un usuario, mientras que la autorización verifica que el usuario tenga los permisos correctos y derechos para acceder a determinado lugar o recurso. Existen tres categorías de métodos distintos de autenticación: Llaves de información, Llaves físicas y Llaves biométricas, y se basan respectivamente en algo que la persona sabe, algo que la persona posee y algo que la persona es [1], [2]. Cada método de autenticación tiene sus desventajas, sin embargo es posible utilizar autenticación multifactor que incluya dos o más métodos de autenticación con el fin de incrementar la solidez de la autenticación [3].

El avance en la tecnología ha permitido el desarrollo de nuevos tipos de sensores y también ha disminuido su costo, lo que ha abierto la posibilidad al desarrollo de diversos sistemas de autenticación. Entre los nuevos dispositivos disponi-

bles se encuentra el sensor Kinect, que permite controlar juegos de video sin manos, así como el control mediante interfaces naturales de usuario para interaccionar con un sistema sin necesidad de mandos o dispositivos de entrada físicos. El sensor Kinect, introducido en el 2010, permite el desarrollo de nuevos sistemas de autenticación con varios métodos, debido a su capacidad de seguir los movimientos del cuerpo humano, medir distancias y reconocimiento de voz entre otras capacidades [4]. Esto permite el desarrollo de sistemas de seguridad en los que se sigue la postura del cuerpo humano, se reconoce la voz y se envían notificaciones como confirmaciones. El sensor Kinect cuenta con una cámara a color, un sensor de profundidad infrarrojo, así como un emisor infrarrojo, un motor de inclinación, un LED y un arreglo de micrófonos [5]. Una de las ventajas de utilizar el sensor Kinect para sistemas de autenticación es que se tiene gran flexibilidad en las formas de ingreso de información, facilitando así la diversidad de métodos y tipos de sistemas de autenticación posibles.

Se han realizado diversos estudios sobre el uso del sensor Kinect para fines relacionados con la seguridad y la detección de los movimientos del cuerpo humano.

Los autores Jiří Přinosil, Kamil Říha, Fu Dongmei [6] en su artículo hablan sobre una solución para evitar que una persona no autorizada pase a través de una puerta segura, utilizando la detección del número de personas que pasan por la puerta mientras esta permanece abierta. Por otro lado los autores Sean McSheehy y Erik Cowley [7] discuten en su trabajo sobre cómo podría detectar un robot a intrusos potenciales. También vinculado con el uso del sensor Kinect para aplicaciones que requieren la detección de movimiento del cuerpo humano, los autores Martínez-Zarzuela et al. [8] revisan el mundo en torno al sensor Kinect y establecen las directrices para desarrollar aplicaciones basadas en el seguimiento de movimientos con este dispositivo.

En relación con la utilización del sensor Kinect para aplicaciones de autenticación con el uso de contraseñas, los autores Mohd Afizi Mohd Shukran y Mohd Suhaili Bin Ariffin [9] plantean la creación de un gesto de mano patrón que actúe como contraseña, incluso con las variaciones en la orientación de la mano, la escala o la articulación. En la misma línea, el autor Liang Li [10] explora la autenticación de usuarios basada en gestos capturados por el sensor Kinect. También utilizando los gestos, los autores Wu et al. [11] investigan las ganancias en desempeño y robustez para la autenticación de usuarios, basada en gestos utilizando varios sensores Kinect.

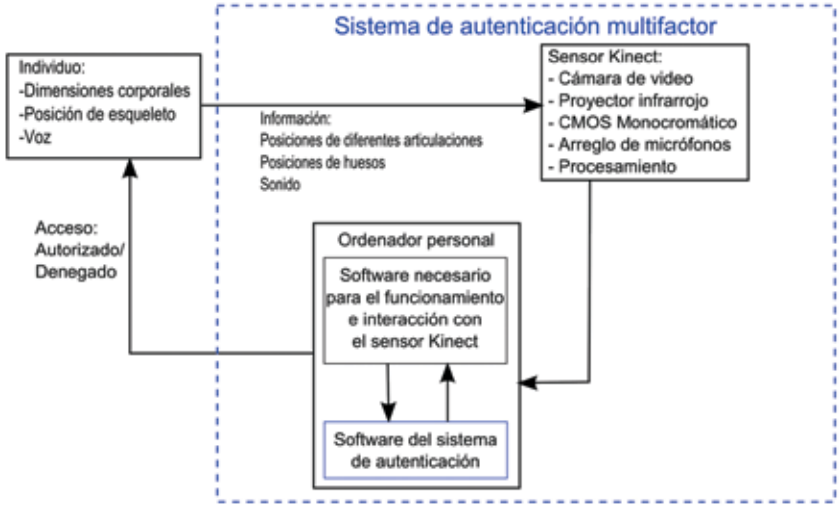
En autenticación biométrica, el autor S. Joseph Fluckiger [12] explora en su artículo la capacidad de reconocer la presencia de un humano y estimar sus dimensiones, al utilizar una cámara, efectuando una autenticación biométrica y usando el sensor Kinect. Los autores Araujo et al. [13] consideran la viabilidad de utilizar el sensor Kinect para obtener puntos de las posiciones del esqueleto de sujetos en movimiento y usarlos para identificación biométrica para considerar la contribución de diferentes combinaciones de partes del cuerpo al proceso de identificación. Otro caso biométrico es el del artículo de los autores Wu et al. [14] en el cual se propone el uso del Kinect, pero en lugar de acomodar a un amplio número de usuarios se explota la unicidad de cada usuario en términos de gestos. Para identificar personas de forma discreta y a distancia de forma biométrica, los autores Dikovski et al. [15] construyen y evalúan conjuntos de características y partes del cuerpo en el proceso de reconocimiento de personas a partir de su forma de caminar, utilizando los datos esqueléticos obtenidos con el sensor Kinect. Los autores Hayashi et al. [16] en su artículo introducen un sistema de identificación que utiliza las diferencias individuales en longitudes de segmentos del cuerpo y patrones de gestos de movimientos de manos, es decir, utiliza llave biométrica y llave de información.

El sistema de autenticación desarrollado en este trabajo, se llevó a cabo desde una nueva perspectiva y enfoque; se cubrieron los tres tipos de métodos de autenticación, donde cada uno de los métodos seleccionados es sencillo y complementario a los demás, para lograr una autenticación multifactor.

2. DESARROLLO

El diseño del sistema se esquematiza en el diagrama en la Fig. 1

Fig. 1. ESQUEMA GENERAL DEL SISTEMA DE AUTENTICACIÓN



Fuente: autores.

El *software* del sistema de autenticación interpreta los diferentes parámetros y valida el acceso al sistema o lo niega. Con ayuda del sensor Kinect Modelo 1414 es posible obtener palabras pronunciadas por el individuo, utilizando los micrófonos incorporados, mediciones de su esqueleto y las posiciones de sus diferentes articulaciones.

2.1 Selección de métodos de autenticación

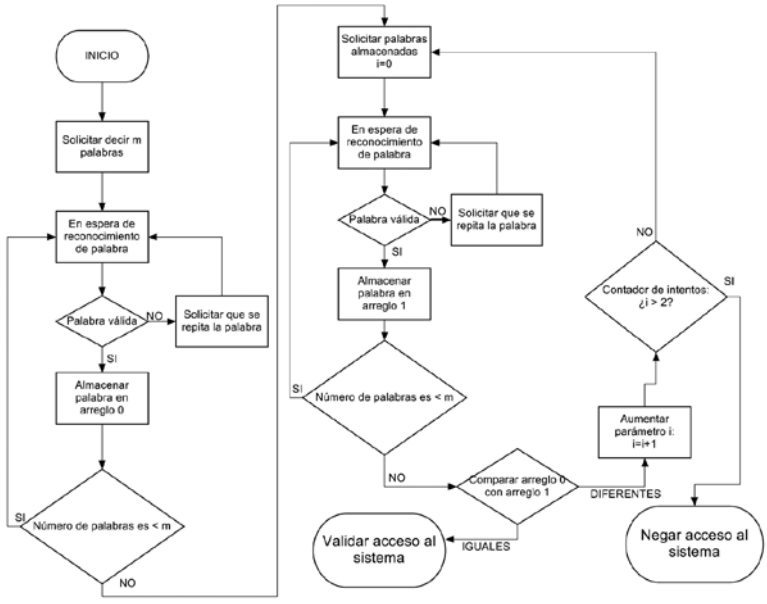
Debido a los parámetros que se pueden obtener con el sensor Kinect así como a sus rangos de operación y limitaciones, se seleccionaron cinco métodos de autenticación: 1) Método de ingreso de palabras utilizando el reconocimiento del habla. 2) Método de introducción de contraseña utilizando la posición de alguna parte del cuerpo humano. 3) Método de introducción de contraseña utilizando la postura del cuerpo humano. 4) Método de medición de longitudes del esqueleto y 5) Método con llave física utilizando una tarjeta impresa con información necesaria para validar acceso.

2.1.1 Método de ingreso de palabras utilizando el reconocimiento del habla

Este método usa un tipo de autenticación con llave de información o contraseña. El objetivo de este método es permitir el ingreso de palabras como información que será utilizada para la autenticación de un individuo. Una cadena de caracteres forma una palabra. En este caso los elementos que forman la contraseña son palabras en lugar de caracteres, de modo que una contraseña está representada por una cadena de palabras en lugar de una cadena de caracteres. Se seleccionó un subconjunto de palabras del total existente en el lenguaje español con el fin de cumplir con dos objetivos: 1) Añadir seguridad al no permitir que cualquier palabra del español sea considerada como un ingreso válido y 2) Evitar que el sistema de reconocimiento confunda dos o más palabras que sean homófonas, es decir, que tengan la misma pronunciación. Para conseguir el segundo objetivo se definieron palabras que tuvieran pronunciación diferente entre sí. El primer objetivo permitió incorporar el método con llave física, utilizando una tarjeta impresa con información necesaria para validar el acceso, que consiste en que el usuario necesitará portar una llave física, una tarjeta con una lista de las palabras válidas que representan los ingresos posibles para el sistema, así como información relevante para los demás métodos de autenticación que serán empleados.

En la Fig. 2 se encuentra un diagrama del algoritmo para este método. Los arreglos 0 y 1 son arreglos de palabras mientras que i es el contador de intentos y m el número de palabras necesarias para la autenticación.

Fig. 2. DIAGRAMA DE ALGORITMO PARA EL MÉTODO DE INGRESO DE PALABRAS UTILIZANDO EL RECONOCIMIENTO DEL HABLA



Fuente: autores.

2.1.2 Método de introducción de contraseña utilizando la postura del cuerpo humano

Este utiliza un método de autenticación con llave de información. El kit de desarrollo de *software* de Kinect soporta seguimiento del esqueleto humano, y es posible detectar el movimiento del esqueleto humano que se encuentre frente al sensor.

Las posibilidades de autenticación a través de la introducción de claves utilizando la postura del cuerpo humano son muchas. Sin embargo, para cumplir con los objetivos de ser un sistema simple pero efectivo se decidió utilizar un algoritmo que fuera sencillo, pero que pudiera garantizar que aportara una barrera importante de seguridad. El objetivo principal de este método es evitar que las personas que no conozcan el sistema puedan ingresar información al sistema para la autenticación. En un escenario hipotético la persona podría hacer movimientos aleatorios en frente del sensor con la esperanza de obtener acceso al sistema, pero este método está diseñado para impedirlo. Entonces, el problema principal de este método fue elegir posiciones del cuerpo humano tales que no fueran naturales pero que tampoco fueran complicadas o difíciles de mantener. Esto es importante porque si se trata de una posición común o natural, una persona ajena al sistema podría sortear esta barrera haciendo movimientos aleatorios o permaneciendo en una posición natural. Al mismo tiempo fue importante que no fueran posiciones complicadas por comodidad y simplicidad en su ejecución.

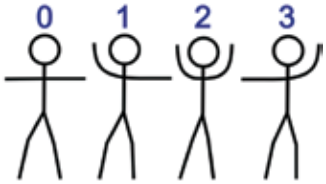
La solución propuesta tomó en cuenta dos aspectos: 1) Las posiciones posibles o válidas y 2) El tiempo que deben ser mantenidas para ser consideradas como una entrada o ingreso de información al sistema.

Para el primer aspecto se consideró que a mayor complejidad en las posiciones mayor seguridad, pero también mayor dificultad en la ejecución. Se eligió que las posiciones del cuerpo humano se limitarían a las posiciones de los brazos, tanto por simplicidad como por razones de aplicabilidad al mayor número de personas. Si una persona por alguna razón no puede estar de pie, el algoritmo de autenticación sigue siendo válido y se puede emplear ya que solo considera las posiciones de los brazos.

El siguiente paso fue elegir la cantidad y tipo de posiciones válidas. Se desarrolló un algoritmo que requiriera que el individuo conociera cierta información para poder ejecutar las posiciones de forma apropiada. La información que requiere co-

nocer el individuo en este caso es que ambos brazos deben estar estirados. Cualquier posición de los brazos en la cual estos no estén ambos estirados simultáneamente, no es considerada como válida por el sistema y no se puede continuar con el proceso de autenticación, de modo que el individuo no conseguirá acceso al sistema. Se eligieron cuatro posiciones válidas, que se muestran en la Fig. 3.

Fig. 3. LAS CUATRO POSICIONES VÁLIDAS



Fuente: autores.

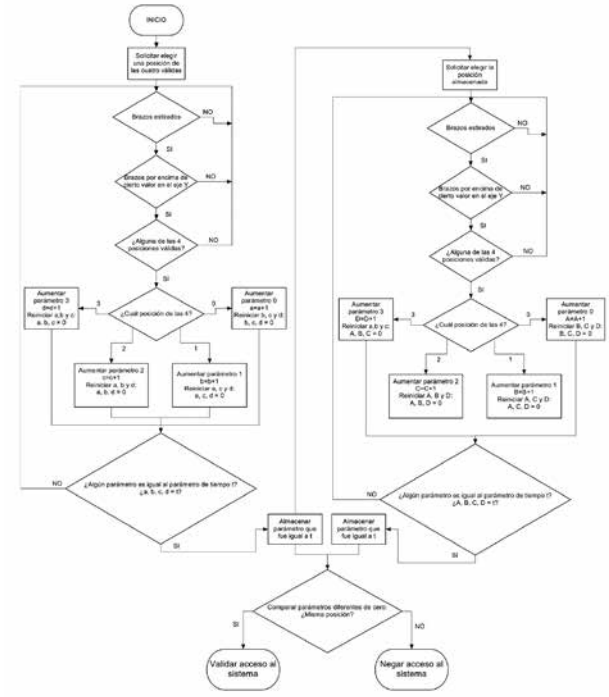
Las cuatro posiciones requieren que el individuo mantenga estirados ambos brazos. Las posiciones son las siguientes: (0) Ambos brazos a los lados u horizontales (1) Brazo derecho arriba o vertical y brazo izquierdo a un lado u horizontal (2) Ambos brazos arriba o verticales y (3) Brazo izquierdo arriba o vertical y brazo derecho a un lado u horizontal.

De modo que es necesario mantener alguna de las posiciones válidas durante cierto tiempo para poder continuar con el proceso de autenticación. El tiempo que debe ser mantenida cualquiera de las posiciones para ser considerada como una entrada o ingreso válido de información al sistema es controlado por un parámetro dependiente de los cuadros por segundo que son enviados de la información de las posiciones del esqueleto y fue ajustado en la fase final de desarrollo.

El algoritmo funciona de la siguiente forma: Si el individuo tiene ambos brazos estirados, el sistema libera un candado. Si el individuo tiene ambos brazos por encima de cierta altura, con respecto a sus hombros, el sistema libera un segundo candado. Si el individuo se encuentra en alguna de las cuatro posiciones válidas, el sistema libera un tercer candado.

En la Fig. 4 se muestra el diagrama que representa la forma de operar del algoritmo para este método. El parámetro de tiempo *t* está relacionado con el número de cuadros del flujo de esqueleto y permite controlar el tiempo que es necesario mantener la posición para considerarla un ingreso de información.

Fig. 4. DIAGRAMA DE ALGORITMO PARA EL MÉTODO DE INTRODUCCIÓN DE CONTRASEÑA UTILIZANDO LA POSTURA DEL CUERPO HUMANO



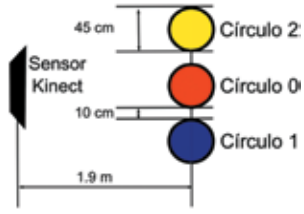
Fuente: autores.

2.1.3 *Método de introducción de contraseña utilizando la posición de alguna parte del cuerpo humano*

Este método utiliza un tipo de autenticación con llave de información o contraseña y fue incluida debido a que no agrega dificultad de uso al sistema, pero constituye una barrera más y toma ventaja de la información que obtiene el sensor. Es similar al método de introducción de claves utilizando la postura del cuerpo humano, pero solo toma en cuenta la posición del individuo respecto al sensor, en este caso se seleccionó la posición de la cabeza. En este método se puede elegir una de las tres posiciones posibles, indicadas en el piso con círculos marcados. Las posiciones son: círculo 0, círculo 1 y círculo 2. Los círculos marcados en el piso tienen un diámetro de 45 cm y están separados entre sí por 10 cm.

En la Fig. 5 se muestra un diagrama a escala de la vista desde arriba de la distribución de los diferentes elementos necesarios para este método.

Fig. 5. DISTRIBUCIÓN DE LOS ELEMENTOS PARA EL MÉTODO DE INTRODUCCIÓN DE CONTRASEÑA UTILIZANDO LA POSICIÓN DE LA CABEZA

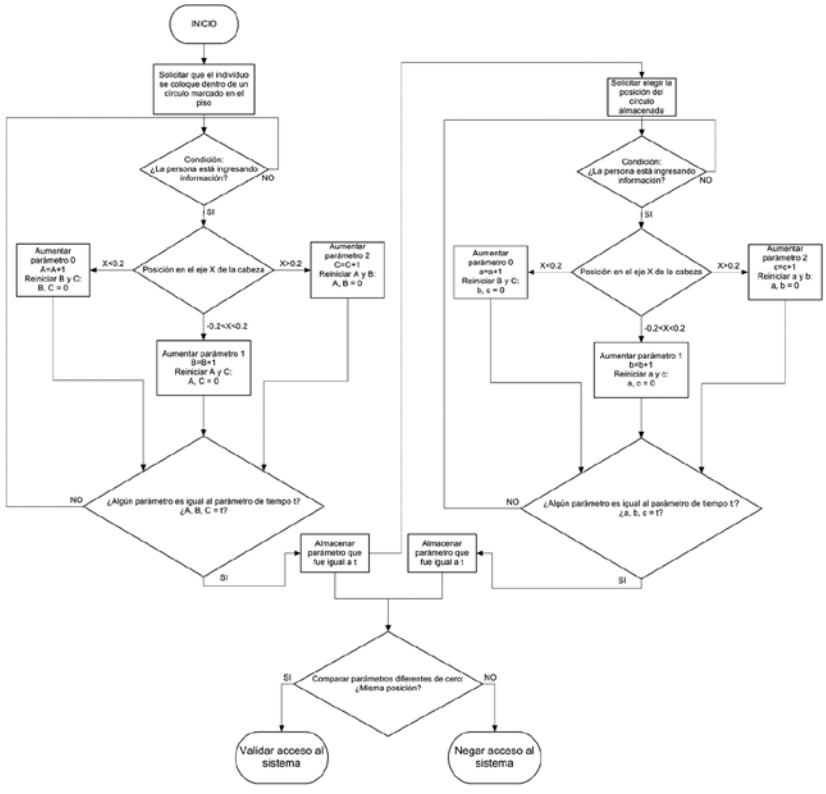


Fuente: autores.

Debido a que se indica al usuario las posiciones a través de unos círculos marcados en el piso, en este método es importante que la persona permanezca derecha y se coloque dentro de alguno de los círculos.

En la Fig. 6 se indica que es necesario conocer si la persona está ingresando información, para incrementar el parámetro correspondiente. En la implementación final del sistema se utiliza la detección de la posición válida de los brazos para asegurar que la persona está intentando ingresar información.

Fig. 6. DIAGRAMA DEL ALGORITMO PARA EL MÉTODO DE INTRODUCCIÓN DE CONTRASEÑA UTILIZANDO LA POSICIÓN DE ALGUNA PARTE DEL CUERPO HUMANO



Fuente: autores.

Esto es necesario porque si la persona se encuentra en frente del sensor, pero no desea indicar un círculo marcado en el piso en particular, el algoritmo debe ignorar las mediciones que se realicen en ese momento. Este criterio se utiliza también en el método de medición de longitudes del esqueleto, para garantizar que la persona se encuentra en la misma posición mientras se realiza la medición de la longitud utilizada en la autenticación.

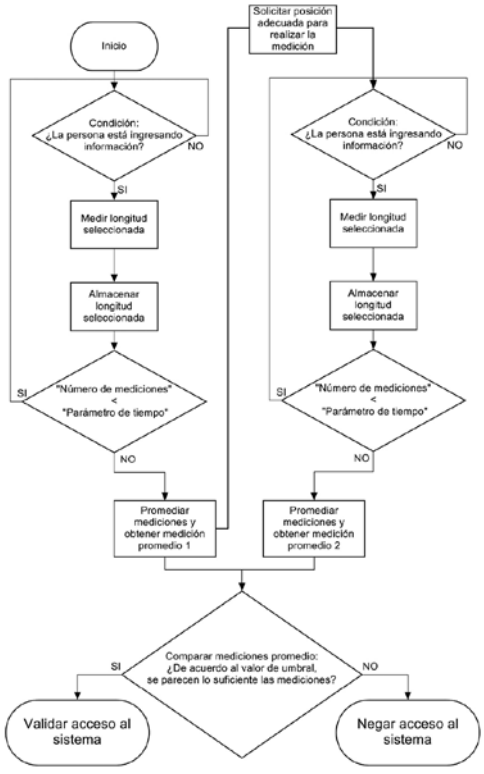
2.1.4 Método de medición de longitudes del esqueleto

Este método utiliza un tipo de autenticación biométrica con la información de las dimensiones del cuerpo humano obtenida a través del sensor Kinect. El primer aspecto importante por considerar es el sensor Kinect, en particular sus limitaciones para tomar mediciones de longitudes del cuerpo humano. En pruebas iniciales para verificar el funcionamiento adecuado del sensor, se encontró que tomar una sola medición no es suficiente, ya que las fluctuaciones en las mediciones impiden distinguir a una persona de otra con una sola medición. Con el fin de mejorar la medición de la longitud se toman tantas mediciones como sea posible durante el intervalo de tiempo definido por el parámetro de tiempo y se promedian. En la Fig. 7 se muestra el diagrama que representa la forma de operar del algoritmo para el método de medición de longitudes del esqueleto. El parámetro de tiempo limita el número de mediciones posibles, ya que el flujo de esqueleto tiene un número de cuadros por segundo máximo. Las mediciones se efectúan únicamente mientras la persona se encuentra en alguna de las posiciones válidas de brazos.

2.1.5 Método con llave física utilizando una tarjeta impresa con información necesaria para validar acceso

Este utiliza un tipo de autenticación con llave física, que consiste en una tarjeta impresa con información necesaria para validar el acceso. El usuario necesita portar esta llave física, una tarjeta con una lista de las palabras que representen los ingresos posibles para el sistema así como información relevante para los demás métodos de autenticación empleados, para validar su acceso al sistema. En la Fig. 8 se muestra la tarjeta con la información adicional necesaria para la autenticación.

Fig. 7. DIAGRAMA DEL ALGORITMO PARA EL MÉTODO DE MEDICIÓN DE LONGITUDES DEL ESQUELETO



Fuente: autores.

Fig. 8. TARJETA CON INFORMACIÓN NECESARIA PARA LA AUTENTICACIÓN

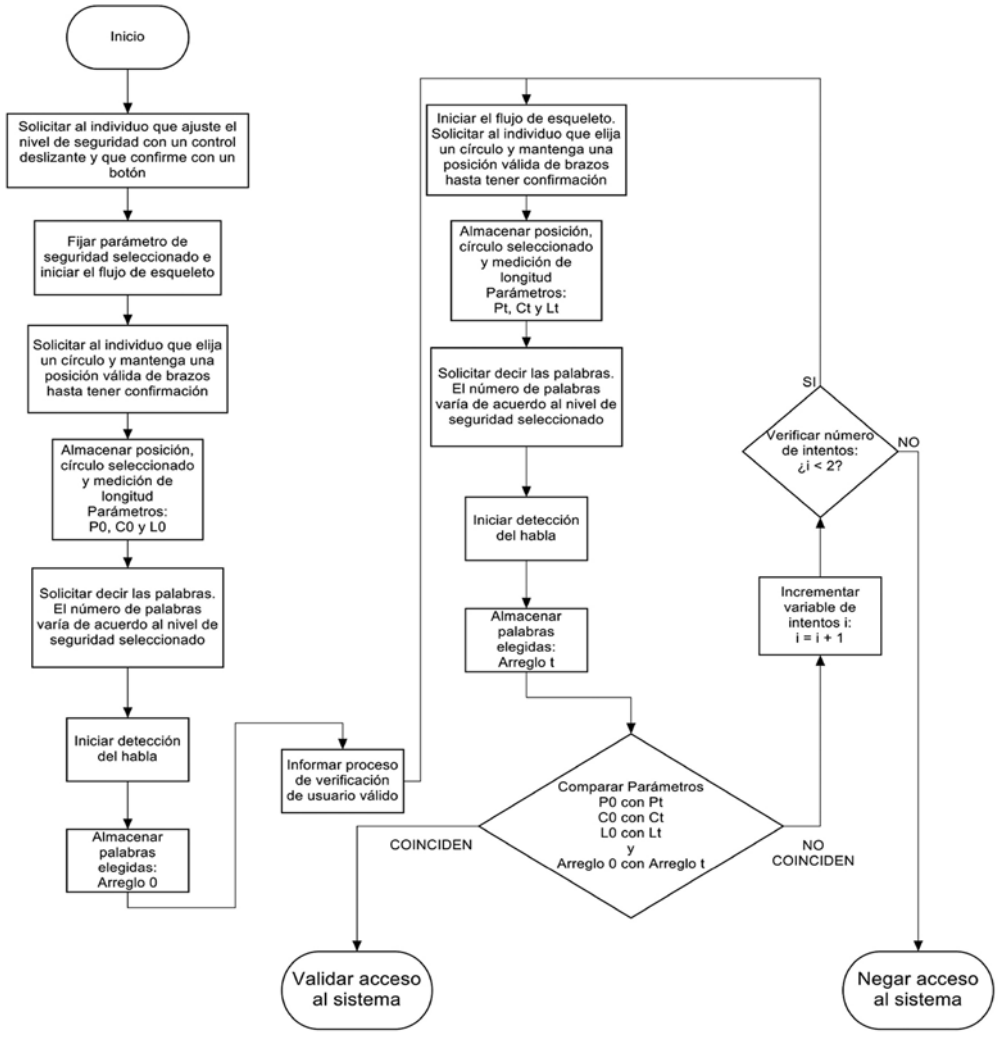
Fuente: autores.

2.2 Integración y operación del sistema

El diagrama de la aplicación que integra los métodos de autenticación seleccionados, tomando en cuenta la interfaz de usuario y que corresponde al *software* del sistema de autenticación que interpreta los diferentes parámetros y valida el acceso al sistema o lo niega se encuentra en la Fig. 9. Las notificaciones se muestran en la pantalla del equipo de cómputo. Se permitió variar el nivel de seguridad ajustando el número de palabras necesarias para realizar la autenticación con el método 1 entre tres, cuatro y cinco.

Por último, fue necesario el ajuste a través de la determinación de los diferentes parámetros, así como definir la cantidad de palabras válidas y las partes del esqueleto que serían consideradas para efectuar las mediciones biométricas.

Fig. 9. DIAGRAMA DE LA FORMA DE OPERAR DE LA APLICACIÓN QUE INTEGRA LOS MÉTODOS DE AUTENTICACIÓN SELECCIONADAS

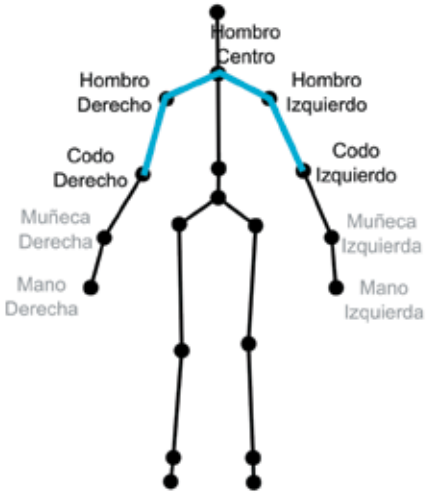


Fuente: autores.

3. RESULTADOS

Para el método de autenticación por medio de la medición de una longitud, se consideró la suma de las siguientes distancias: distancia de hombro derecho a centro de hombros, distancia de centro de hombros a hombro izquierdo, distancia de codo izquierdo a hombro izquierdo y distancia de codo derecho a hombro derecho. El diagrama de esta longitud se encuentra en la Fig. 10.

Fig. 10. FORMA DE MEDIR LA LONGITUD PARA EL MÉTODO BIOMÉTRICO



Fuente: autores.

Este valor de longitud se obtiene para cada cuadro del flujo esquelético y se promedia con todos los obtenidos durante el periodo de reconocimiento de la posición de brazos. Las manos y muñecas se excluyeron de la medición de longitud porque los valores de la localización de las posiciones de las manos fluctúan demasiado.

Se determinó que la diferencia mínima en longitud, que permitiera distinguir entre dos personas diferentes, fuera tal que disminuyera la probabilidad de falso rechazo, estableciendo un umbral de 9 cm para la comparación de promedios de longitudes. Se hicieron pruebas considerando la estatura del individuo, pero las variaciones en las mediciones son muy grandes. Si la persona trae algún sombrero o zapatos muy altos, la medición de estatura cambia. Debido a que la medición de longitud se lleva a cabo mientras se detecta la posición de brazos, la comparación entre las mediciones de longitud se realiza entre dos mediciones tomadas con la misma posición de brazos y en el mismo círculo. El método biométrico desarrollado en este sistema permite diferenciar a personas que sean lo suficientemente diferentes en sus distancias entre articulaciones, pero como método único para distinguir entre dos personas cualesquiera no es suficiente.

El sistema de autenticación fue ajustado para que funcionara adecuadamente. El método que impide una autenticación más confiable es el biométrico, ya que distinguir entre personas de dimensiones similares, con el sensor Kinect e infraestructura actual y utilizando el método de medición de longitud propuesta, tiene gran dificultad. En la Tabla I se muestra una comparación cualitativa de los métodos seleccionados.

TABLA I
COMPARACIÓN CUALITATIVA DE LOS MÉTODOS

Método / Característica	Medición longitud (Método 4)	Posición círculo (Método 2)	Voz habla (Método 1)	Posición brazos (Método 3)	Tarjeta física (Método 5)
Confiabilidad	No	Sí	Sí	Sí	Sí
Facilidad de uso	Sí	Sí	Sí	Sí	Sí
Costo adicional	No	No	No	No	No
Factor sorpresa	Sí	Sí	Sí	Sí	Sí
Requiere tiempo adicional	No	No	Sí	No	No
Alto número de configuraciones posibles	No aplica	No	Sí	No	Complementaria
Interferencias	Precisión y exactitud de medición	No atender instrucciones	Ruido, pronunciación, eco	No atender instrucciones	Daño, extravío
Requerimiento de espacio adicional	No	No	No	No	No
Posibilidad de mejoría en el futuro	Sí	Sí	Sí	Sí	Sí
Posibilidad de reconocimientos falsos	Sí	No	Sí	No	No aplica
Afectación o interferencia con los demás métodos	No	No	No	No	No
Ventaja principal / Aporte	Autenticación biométrica	Facilidad de uso	Número de configuraciones posibles	Conocimiento / Factor sorpresa	Llave física

Fuente: autores.

Si se aumenta la tolerancia en la comparación de promedios de longitudes, se incrementa la probabilidad de falsa aceptación. Aunque los demás métodos contribuyen para aumentar la robustez de la autenticación, esto disminuye la efectividad del sistema. Si por el contrario, se disminuye la tolerancia en la comparación de promedios de longitudes, se incrementa la probabilidad de falso rechazo, lo cual conduce a un mayor descontento de los usuarios del sistema.

El umbral para la posición de la cabeza se obtuvo al definir el diámetro que tienen que tener los círculos marcados en el suelo para que una persona pueda caber dentro y las diferentes distancias requeridas. Por simplicidad de implementación se eligieron tres círculos, ya que de esta forma se admite un mayor rango de error en la posición de las marcas de los círculos en el piso. Además, el aporte en el nivel de seguridad tanto del método de posiciones de los brazos como del de la elección del círculo, es adicional y su principal fortaleza es la facilidad de uso y su novedad. La seguridad, desde el punto de vista de la cantidad de configuraciones posibles, la aporta el método de reconocimiento del habla. Por facilidad de uso es conveniente limitar la cantidad de ingresos válidos tanto en el método de posición de brazos como en el de selección de círculo, y aumentar el número de palabras válidas del método de reconocimiento del habla así como el número de palabras requeridas para la autenticación. En la Tabla II se muestran los diferentes números de configuraciones posibles para los métodos 1, 2 y 3.

TABLA II

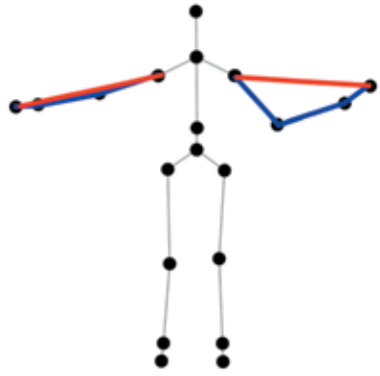
NÚMERO DE CONFIGURACIONES POSIBLES

	Configuraciones posibles		
Número de ingresos	Posición círculo (Método 2)	Voz habla (Método 1)	Posición brazos (Método 3)
1	3	150	4
2	9	22,500	16
3	27	3,375,000	64
4	81	506,250,000	256
5	243	75,937,500,000	1,024

Fuente: autores.

Para seleccionar las posiciones de brazos válidas, se tuvo un compromiso entre facilidad de ejecutarlas y la posibilidad de reconocimientos falsos. Para que no fueran difíciles de realizar, al mismo tiempo que se evitaran reconocimientos falsos, se ajustaron los parámetros experimentalmente. Las posiciones se eligieron de forma que implicaran un conocimiento previo sobre cómo realizarlas, además de requerir mantenerlas durante cierto tiempo. El conocimiento necesario para su ejecución correcta consiste en que ambos brazos deben estar estirados, de lo contrario el sistema no permite el ingreso de información y de esta forma niega el acceso al sistema. Para determinar si un brazo se encuentra estirado se compararon dos longitudes, si la diferencia es mayor a 3 cm se considera que el brazo no se encuentra estirado. Si la diferencia es menor a 3 cm se considera que el brazo se encuentra estirado. Este valor se determinó experimentalmente.

Fig. 11. LA LONGITUD MOSTRADA EN COLOR AZUL ES COMPARADA CON LA MOSTRADA EN ROJO



Fuente: autores.

El universo de palabras se seleccionó evitando palabras que tuvieran la misma pronunciación en el idioma. También se comprobó que a mayor número de palabras válidas, mayor dificultad para el reconocimiento y de que se confundan unas con otras. Lo mismo ocurre al elegir palabras cuya pronunciación sea similar. Experimentalmente se encontró que alrededor de 250 palabras son reconocidas de forma exitosa si son seleccionadas cuidadosamente para evitar palabras con pronunciación similar. Esto se hizo mencionando cada una de las 250 palabras, y cuando se requirió más de un intento para ser reconocidas o fueron reconocidas incorrectamente se cambiaron y se repitió el proceso. Al llegar a 300 palabras ocurren reconocimientos equivocados de palabras aunque se seleccionen con cuidado. Debido a esto, se seleccionó una lista de 150 palabras válidas, dejando un margen de tolerancia mayor para poder

seleccionar las palabras con más libertad. En la Tabla III se muestra la relación entre el número de palabras válidas y la dificultad para su reconocimiento.

A partir de esta limitación, se seleccionó el número de palabras para los diferentes niveles de seguridad. En la Tabla IV se encuentra el número de configuraciones posibles de acuerdo con el nivel de seguridad seleccionado así como el aporte de cada uno de los métodos.

A diferencia de las contraseñas en las que se trata de cadenas de caracteres, en las contraseñas de cadenas de palabras del sistema propuesto, las palabras son seleccionadas por el usuario de un modo que es difícil encontrar patrones en su selección. Con la indicación única de que no se repitan las palabras, es suficiente para que el usuario elija una contraseña fuerte.

Entre los parámetros ajustados se encuentra el parámetro de tiempo que controla el número de cuadros del flujo que serán considerados. Si se disminuye este parámetro se hace más rápido el proceso de autenticación, ya que el número de cuadros del flujo del esqueleto necesarios para considerar una posición de brazos o de la elección del círculo, es menor. Sin embargo, al disminuir este valor se corre el riesgo de obtener falsos reconocimientos de posición. Además de que, al disminuir el parámetro de tiempo, es menor el número de mediciones de la longitud seleccionada, de forma que se tiene un mayor error en el cálculo del promedio de la medición de longitud. Aumentar este valor hace que sea incómodo mantener la posición por tanto tiempo, además de aumentar el tiempo requerido para realizar la autenticación. Se eligió un parámetro de tiempo correspondiente a ≈2.4 segundos o 73 mediciones de longitud. También se realizó una medición del tiempo aproximado que se requiere para llevar a cabo la autenticación de acuerdo con los diferentes procesos involucrados. En la Tabla V se encuentra el tiempo requerido para realizar la autenticación de acuerdo con el nivel de seguridad seleccionado.

TABLA III

NÚMERO DE PALABRAS VÁLIDAS Y LA DIFICULTAD PARA SU RECONOCIMIENTO

Número de palabras válidas	Dificultad para el reconocimiento	Número de configuraciones posibles para 1 palabra	Número de configuraciones posibles para 2 palabras
250	Mayor	250	62,500
200	Menor	200	40,000
150	No	150	22,500

Fuente: autores.

TABLA IV

CONFIGURACIONES POSIBLES DE ACUERDO CON EL NIVEL DE SEGURIDAD SELECCIONADO

Método	Nivel de seguridad Bajo (3 palabras)	Nivel de seguridad Medio (4 palabras)	Nivel de seguridad Alto (5 palabras)
Brazos	4	4	4
Círculo	3	3	3
Voz	3,375,000	506,250,000	75,937,500,000
Conjunto	40,500,000	6,075,000,000	911,250,000,000

Fuente: autores.

TABLA V

TIEMPO REQUERIDO PARA REALIZAR LA AUTENTICACIÓN

Proceso	Tiempo requerido (s) (Seguridad baja)	Tiempo requerido (s) (Seguridad media)	Tiempo requerido (s) (Seguridad alta)
Brazos, círculo y biométrico	≈3	≈3	≈3
Configurar voz	≈6	≈6	≈6
Reconocimiento de voz	≈4	≈6	≈8
Total	≈13	≈15	≈17

Fuente: autores.

Un elemento importante para este sistema es la tarjeta. La tarjeta incluye información fundamental para realizar la autenticación, de forma que es necesario portarla. Esta tarjeta incluye información sobre cómo atender las indicaciones en pantalla, un diagrama con las posiciones de brazos y de círculos con el número que las identifica, indica que los círculos son un lugar así como que hay que permanecer erguido, nota que los brazos tienen que estar estirados, así como la lista de 150 palabras válidas para el sistema.

De forma que el tiempo requerido para realizar la autenticación de una persona con este sistema va de los 13 a los 17 segundos, si esta se lleva a cabo de forma exitosa. En caso de que se requiera la repetición de palabras será necesario agregar por cada palabra aproximadamente 2 segundos.

4. CONCLUSIONES

Se consiguió desarrollar un sistema de autenticación multifactor robusto, fácil de manejar y económico, a través de las posiciones del cuerpo humano y el reconocimiento de voz, utilizando un sensor Kinect y programación en lenguaje C#, tomando ventaja de las interfaces de programación de aplicaciones.

Se logró un proceso de autenticación simple pero sólido, aprovechando los atributos físicos del individuo y la universalidad de los movimientos permitidos por sus articulaciones, se requirió la presencia física del individuo e información de la tarjeta.

Se desarrolló un sistema novedoso, con la posibilidad de ser mejorado mediante *software* y sin la necesidad de actualizar el *hardware*. Al tratarse de una interface que no requiere contacto físico para ingresar la información, evita contaminarse de virus así como su modificación o daño. El número de cuadros por segundo máximo permitido por el sensor limita al sistema, existiendo un compromiso entre el tiempo requerido y la precisión de los datos que se puede obtener.

Al ajustar cada uno de los métodos se consiguió un sistema de autenticación con 40,500,000 configuraciones posibles que toma ≈13 segundos en el nivel mínimo de seguridad y con 911,250,000,000 configuraciones posibles requiriendo de ≈17 segundos para el nivel de seguridad alto.

Algunas de sus ventajas se deben a que se trata de un sistema de autenticación nuevo, con un gran potencial de mejoría para compensar por el posible conocimiento de su funcionamiento. Con el avance de la tecnología será posible obtener mejores mediciones, disminuir los requerimientos de espacio, permitir la detección de movimientos más sutiles, aumentar el número de cuadros por segundo máximo y reducir el tiempo requerido para la autenticación, entre otras mejorías. Las limitaciones no solamente están relacionadas con el *hardware* y las capacidades técnicas del sensor. También es posible mejorar, agregar, quitar, o combinar de forma diferente los métodos de autenticación.

Utilizando el sistema desarrollado se puede soportar tantos usuarios como número de configuraciones posibles, ya que el almacenamiento en un equipo de cómputo moderno, en el que se basa, cuenta con suficiente capacidad para almacenar gran cantidad de datos, a diferencia de algunos de los sistemas de autenticación disponibles actualmente en el mercado.

El potencial de desarrollo a futuro para este tipo de sistemas de autenticación multifactor utilizando un sensor Kinect es enorme.

REFERENCIAS

[1] E. A. Fisch and G. B. White, *Secure computers and networks. Analysis, design and implementation*. CRC Press, 1999, pp. 1-4, 53-67.

[2] M. Burnett, *Perfect passwords: Selection, protection, authentication*, Rockland: Syngress Publishing, 2006, pp. 76, 131, 133, 134.

[3] J. Killmeyer, *Information security architecture. An integrated approach to security in the organization*, Auerbach: CRC Press, 2006, pp. 101, 114-116.

[4] D. Catuhe, *Programming with the Kinect for Windows Software Development Kit.* Redmond, Washington: Pearson Education, 2012, pp. 3-5, 27, 32.

[5] J. Abhijit, *Kinect for Windows SDK Programming Guide*, Mumbai: Packt Publishing, 2012, pp. 7-18, 19, 21, 37-39, 47-53.

[6] J. Přinosil, K. Říha, and F. Dongmei, "Kinect Based Automated Access Control Systems," Department of Telecommunications, Brno University of Technology. Department of Automation, University of Science and Technology, Beijing Latest Trends in Information Technology. Nov. 2012.

[7] S. McSheehy, and E. Cowley, *Home Security Prototype Device*, University of Massachusetts Lowell. May. 2012.

[8] M. Martínez-Zarzuela, F.J. Díaz-Pernas, A. Tejero de Pablos, F. Perozo-Rondón, M. Antón-Rodríguez, and D. González-Ortega, "Monitorización del cuerpo humano en 3D mediante tecnología Kinect," SAAEI, 747-752. 2011.

[9] M. Afizi, M. Shukran, M. Suhaili, and B. Ariffin, "Kinect-based Gesture Password Recognition," Faculty of Science and Defence Technology, Universiti Pertahanan Nasional Malaysia, *Australian Journal of Basic and Applied Sciences*, vol. 6 no. 8, pp. 492-499, 2012.

[10] L. Li, "Gesture-based User Authentication with Kinect," Boston University, Department of Electrical and Computer Engineering, *Technical Report* No. ECE-2013-2. April 7, 2013.

[11] J. Wu, K. Janus, and I. Prakash, "The Value of Multiple Viewpoints in Gesture-Based User Authentication," *in Computer Vision and Pattern Recognition Workshops* (CVPRW), 2014 IEEE Conference on. IEEE, 2014.

[12] S. J. Fluckiger, *Security with Visual Understanding: Kinect Human Recognition Capabilities Applied in a Home Security System*, The University of Texas at Austin. May. 2012.

[13] Araujo, M. Ricardo, G. Graña, and V. Andersson, "Towards skeleton biometric identification using the microsoft kinect sensor," Proceedings of the 28th Annual ACM Symposium on Applied Computing. ACM, 2013.

[14] J. Wu, K. Janus, and I. Prakash, "Dynamic time warping for gesture-based user identification and authentication with Kinect," *Acoustics, Speech and Signal Processing* (ICASSP), 2013 IEEE International Conference on. IEEE, 2013.

[15] B. Dikovski, G. Madjarov, and D. Gjorgjevikj, "Evaluation of different feature sets for gait recognition using skeletal data from Kinect," *Information and Communication Technology, Electronics and Microelectronics* (MIPRO), 2014 37th International Convention on. IEEE, 2014.

[16] E. Hayashi, M. Maas, and J. I. Hong, "Wave to me: user identification using body lengths and natural gestures," Proceedings of the 32nd annual ACM Conference on Human Factors in Computing Systems. ACM, 2014.