Decanato de Posgrado

Trabajo Final para optar por el título de

MAESTRÍA EN GERENCIA Y PRODUCTIVIDAD

Titulo:

Desarrollo de un sistema de Reconocimiento Facial para ser instalado en los Colegios de Educación Básica radicados en la Zona Metropolitana del Gran Santo Domingo.

(Caso: Colegio Fernando Arturo de Meriño, CAFAM)

Postulante:

Ing. Riquelmy Calcaño Hernández

ID: A00103851

Asesor(a):

Prof. Graciela Mirtha Morales Pacheco

Santo Domingo, Distrito Nacional
República Dominica
2021

TEMA

Desarrollo de un sistema de Reconocimiento facial para ser instalado en los Colegios de educación Básica radicados en la Zona Metropolitana del Gran Santo Domingo.

(Caso: Colegio Fernando Arturo de Meriño, CAFAM)

Resumen

En esta presentación de tesis sobre la investigación acerca de la creación de un sistema de reconocimiento facial biométrico dactilar para el Colegio Cafam, orientado específicamente al control de entrada y salida de los alumnos, padres y/o tutores, personal docentes y administrativos de dichas Institución. Este proyecto pretende crear una solución que permita mejorar la gestión y el control de los familiares autorizados a retirar los estudiantes, a través de la autenticación por medio de reconocimiento fácil desde un lector o dispositivo de captura facial y se validará enviando un mensaje por medio de una pantalla conectada remotamente indicando el nombre del estudiante. Entregando al estudiante a los familiares autorizados; realizando nueva vez la autenticación por imagen digital para dar de alta en el sistema biométrico, quedando registrado la hora de llegada y salida del estudiante. Con todos los registros del flujo por cada día permitirá tener un control detallado, no solo de quien accede a las instalaciones, sino también llevar estadísticas para mejorar el desenvolvimiento dentro del plantel. Cada padre, familiar o persona autorizada deberá de antemano estar registrado mediante huellas dactilares, vinculado a cada estudiante, el grado y aula que cursa donde el sistema enviará un mensaje de aviso del estudiante en la pantalla. Del mismo modo, el estudiante será entregado al personal autorizado registrándose a través de un lector de huella dactilares y estará dado de salida al estudiante. Este proyecto de seguridad educativa mostrara a los padres confiabilidad y seguridad al instante del que el niño ingrese al colegio, en vista de que el sistema ofrece un alto grado de seguridad, control de acceso al momento de acceder a la institución.

DEDICATORIA

Dedico con todo mi corazón mi proyecto de tesis a mi querida esposa y familiares, pues sin ellos no habría logrado este sueño. Sus bendiciones a diario a lo largo de mi vida me han protegido y he sido guiado por el camino del bien. Por eso les otorgo el proyecto gracias a su paciencia y amor.

AGRADECIMIENTO

Agradezco a Dios por la fuerza que me ha dado en el transcurso de la maestría y de forma especial a mi querida esposa Jennifer Arredondo por su cariño, comprensión y apoyo absoluto, a mis padres por siempre haberme brindando la confianza, mis hermanos que siempre estuvieron brindándome apoyo incondicional, como además a mis compañeros de trabajo por su ayuda incondicional.

Quiero agradecer a mis asesores de tesis Prof. Graciela Mirtha Morales Pacheco y Fidias Mejía por sus conocimientos que me sirvieron de gran ayuda. Gracias por todo el apoyo, considero que ustedes fueron mi mejor elección.

Quiero agradecer de forma especial al Profesor Alexander Almonte, por su motivación y consejos durante mi crecimiento profesional.

ÍNDICE GENERAL

LISTA DE LABLAS

LISTA DE FIGURA

INTRODUCCIÓN

Los sistemas faciales son herramientas concernientes a los más recientes avances tecnológicos actuales de autentificación que existe en el mundo hoy en día, siendo el reconocimiento facial uno de los más confiables y fáciles de utilizar en las empresas e instituciones.

El objetivo general de este estudio fue identificar la situación actual del Colegio Cafam y a partir de ella, desarrollar recomendaciones que permitan a las instituciones establecer una estructura organizativa funcional acorde con las mejores prácticas establecidas por el sistema de inteligencia facial.

La ausencia de un sistema de reconocimiento facial en los colegios de educación básica en el gran santo domingo constituye un gran riesgo a la seguridad y confiabilidad de los niños que se encuentra ubicado en la zona metropolitana.

Debido a la inseguridad que impera últimamente a nivel general, gracias a Dios nuestro país no ha llegado todavía la situación de los ataques armado como se ha dado en instituciones básica situado en otros países, sin embargo han habido caso de niños (as) que han sido secuestrados de parejas que se encuentran separadas, tanto el hombre como la mujer han aprovechado la situación para ingresar al colegio en una hora específica para retirar al niño (as) ,en razón de que la custodia está en poder del otro miembro de la pareja. Se han dado la misma situación de esa naturaleza, de que se han introducido personas ajenas a los colegios con fines de negocios o de hacer cualquier otra mala acción que esto pueda implicar un riesgo para los estudiantes.

Se considera que, si hubiese un sistema de reconocimiento facial en los colegios, fuera más seguro el ambiente de estudio de los niños de educación básica.

El desarrollo de un sistema tecnológico mejora la calidad de vida de los usuarios al brindar soluciones que apoyan la ejecución de las actividades, resultando en un consumo energético, más cómodo, optimizando al mismo tiempo aplicaciones, servicios seguros y fáciles de utilizar.

Una de las características más importantes de la automatización de un sistema de reconocimiento facial, es la seguridad, debido a que este es un factor muy importante para brindar cierto tipo de confianza y comodidad, incluida la satisfacción del usuario al ingresar a la instalación y brindar una sensación de seguridad cuando el niño(a) está adentro del colegio. Para un reconocimiento facial seguro, el personal deberá estar autenticado en el sistema.

CAPÍTULO 1: Sistema Facial, presenta la historia y el desarrollo del sistema facial. El concepto básico, se evoca de la siguiente manera; tratando de representar el tipo de sistema de vigilancia, análisis y el número máximo de enfoques en los que se desarrollaron. Los métodos de investigación y las representaciones del conocimiento se presentan de manera general.

EL CAPÍTULO II: Diagnóstico Del Sistema, describe el modelo de elaboración de un diseño. También demuestra el funcionamiento de las encuestas y entrevistas realizadas y la estructura general.

EN EL CAPITULO III: Patrón biométrico, se presenta el proceso de codificación del modelo de conocimiento en las herramientas de desarrollo seleccionadas: Elaboración de propuesta, presentación a los directivos y APMAES de las entidades educativas. La implementación de cada uno de

los elementos. Finalmente, se presenta un breve análisis de la implementación de propuesta y presentaciones los directivos.

CAPÍTULO: 1

TEORÍAS Y CONCEPTOS SOBRE LOS SISTEMAS DE VIGILANCIA EN LAS INSTALACIONES EDUCATIVAS DEL GRAN SANTO DOMINGO.

1.1- Historia de los sistemas de vigilancia de reconocimiento facial de patrones biométrico.

En la década de los 60 el matemático estadounidense Woodrow Wilson Bledsoe logró desarrollar un sistema que clasificaba rostros a partir de fotografías. Registrando las coordenadas de los ojos en la nariz, la línea del cabello o la boca se valió de un dispositivo conocido como tableta Grant, una de las primeras tabletas graficas que existieron. Estas métricas se incorporaban a una base de datos y así el dispositivo era capaz de devolver la imagen que más se pareciera. En los siguientes años, su precisión fue evolucionando, pero no fue hasta la llegada de los 90 cuando se dieron los primeros pasos hacia el reconocimiento automático y especialmente en esta última década cuando la inteligencia artificial y el aprendizaje automático proporcionaron un salto exponencial a sus capacidades, tanto en fotografías como en videos en tiempo real.

El reconocimiento facial ha evolucionado en los últimos avances tecnológicos a la par de los dispositivos móviles de última generación, ya que varias de sus aplicaciones requieren de los servicios de identidad facial.

Actualmente el sistema facial está presente en el desbloqueo de muchos dispositivos móviles, tanto que pueden reconocernos a través del rostro; pero su uso más polémico es el que realizan las fuerzas de seguridad, ya que hoy en día existe un poder sin precedentes capaz de seguir el rastro de cualquier ciudadano.

Los sistemas de reconocimiento facial han logrado introducirse poco a poco en la sociedad, sin embargo cada vez son más las voces que alertan y cuestionan su uso en términos de ética y privacidad. El mercado de la

vigilancia facial es enorme y su objetivo no se centra solo en las fuerzas de seguridad, sino también en las empresas que consumen esta tecnología.

No es difícil saber que, tiempo atrás, el ser humano identificó un individuo gracias a cualquier rasgo que este muestre, por ejemplo: un corte sobre la piel, su color, su estatura, su voz, etc., y que, en su momento, estas características serían suficientes para reconocer una persona, con tan solo verlas.

Con el pasar de los años, identificar a una persona requiere mayores exigencias; por lo que, han ido apareciendo nuevas técnicas para identificar personas como, por ejemplo: usuario y claves de acceso, número de identificación personal (NIP), tarjeta de identificación por radio frecuencia (RFID), pasaporte, licencia de conducir, entre otros. Pero estas técnicas utilizan atributos que se pueden extraviar, olvidar, manipular o ser robados, creando percances económicos y problemas de seguridad. Es así como empieza la necesidad de crear otros sistemas muchos más confiables para la identificación de personas. En este sentido, digitalizar las características morfológicas del ser humano sería la solución (uso de la biometría).

Entre los tipos de sistemas biométricos (huella, iris, mano, firma, voz, rostro), el reconocimiento facial es el que más ha evolucionado, y poco a poco deja de verse solo en ciencia ficción, siendo aplicados en la vida real. Este sistema es muy usado para identificar personas y crear métodos de seguridad y protección sofisticados.

1.2- Características y tipología de las Tecnologías Biométricas.

Reconocimiento de voz

Las aplicaciones de reconocimiento de voz utilizan sistemas de inteligencia artificial (especialmente redes neuronales) para aprender el reconocimiento de voz. El algoritmo debe medir y estimar la similitud entre muestras para devolver un resultado o una lista de posibles candidatos. Factores como el ruido ambiental dificultan la identificación, por lo que siempre debe considerar el margen de error.

Reconocer el lenguaje natural de algunas personas sigue siendo difícil, pero esta tecnología tiene la ventaja de que el receptor es solo un micrófono, por lo que no es necesaria ninguna inversión adicional.

El uso de este método es más común en sistemas de respuesta de voz y centros de llamadas que en el control del acceso físico, redes y equipos de TI.

Reconocimiento de escritura de teclado

Esta técnica se basa en el hecho de que existe una mecanografía personal y persistente. Mide la fuerza del golpe, la duración del golpe y el tiempo transcurrido entre presionar una tecla y presionar otra.

La principal ventaja de esta técnica es que la inversión necesaria para el sensor es prácticamente nula. Los teclados de ordenador están presentes en muchos aspectos de nuestra vida diaria y también son muy bien recibidos por las personas que los utilizan a diario. De esta manera, los costos de implementación están centrados en el software.

Reconocimiento de la forma de andar

Este método se basa en la forma en que las personas caminan. Este comportamiento se registra y analiza para crear un modelo biométrico único derivado del comportamiento descrito anteriormente.

Esta tecnología aún se encuentra en desarrollo y aún no ha alcanzado el nivel de desempeño requerido para implementarla de la misma manera que otras tecnologías biométricas.

Usos y aplicaciones

La biometría, utilizada como formato de autenticación propietario o en combinación con otras métricas (tarjetas inteligentes, claves de cifrado, firmas digitales, etc.), está configurada para propagarse a otros aspectos cada vez mayores de nuestra vida diaria. Esta guía se centra en aspectos relacionados con la ciberseguridad.

Control de accesos físicos y lógicos

Uno de los usos más habituales de la biometría son las aplicaciones de control de acceso, tanto físicas (como el acceso a edificios o espacios confinados) como lógicamente (a sistemas informáticos, programas o dispositivos, teléfonos móviles, tabletas, etc.).

Actualmente, la huella dactilar es la principal solución para este uso en España por su gran madurez, precio competitivo y facilidad de uso.

Sin embargo, este tipo de aplicación ofrece reconocimiento facial en lugar de huellas dactilares.

En algunos casos, se utiliza una combinación de tecnologías para controlar el acceso a áreas altamente seguras. Los ejemplos incluyen el uso de una contraseña o una tarjeta de identificación con una huella digital o el uso de una combinación de dos técnicas biométricas conocidas como biometría modal. Por lo tanto, puede combinar los dos factores distintivos. Uno es quién eres y qué eres (biometría) y el otro es lo que sabes o tienes (contraseñas, tarjetas, etc.).

Control de presencia

El método tradicional utilizado para registrar el tiempo diario que un empleado entra y sale de cada trabajo se basa a menudo en el uso de un PIN o tarjeta personal.

Una de las principales desventajas de estos métodos es que son propensos al fraude porque no requieren verificación adicional, como compartir un PIN personal o una tarjeta con un colega.

Los datos biométricos no se pueden compartir entre los empleados, por lo que el uso de datos biométricos es una forma eficaz de mitigar este riesgo.

Las huellas dactilares se utilizan comúnmente en este tipo de aplicación, pero existen algunas técnicas menos comunes en el mercado, como las formas de las manos.

Lucha contra el fraude

El uso de estas tecnologías para realizar operaciones bancarias es muy popular, ya que se consideran preferibles al uso de métodos tradicionales al proporcionar un mayor nivel de seguridad.

Sin embargo, su uso para prevenir el fraude no se limita al sector privado. El gobierno ha implementado un sistema biométrico para prevenir este delito, con el objetivo de evitar el gasto ocasional de fondos públicos.

Aumento de la seguridad en el control de accesos

Sin duda, uno de los beneficios más importantes para las empresas al utilizar la tecnología biométrica es la autenticación de sus empleados. Esto le permite identificarse, es decir, sus características. Los datos biométricos solo están vinculados a usuarios legítimos.

Un individuo puede culpar a un tercero por obtener acceso a un área restringida o por participar en una actividad fraudulenta al robar credenciales o identidades. Además, estas credenciales se pueden compartir voluntariamente entre los empleados.

La implementación de un sistema biométrico mejora la seguridad al reducir la probabilidad de que personas no autorizadas tengan acceso a áreas o aplicaciones restringidas.

Mejora de imagen corporativa

La implementación de tecnología biométrica hace que las operaciones comerciales sean más eficientes y seguras, y reduce el fraude interno. Entonces, además de todos los beneficios anteriores, la opinión general de la empresa ha mejorado enormemente. Del mismo modo, las organizaciones se conectan con la innovación, invierten en investigación y desarrollo y trabajan en tecnología de vanguardia.

Métodos De Autentificación

El desarrollo de métodos de autenticación multifactorial y códigos clave de token de teléfonos inteligentes.

La autenticación de múltiples factores, más antigua que la propia Web, es un método técnico de seguridad informática que requiere que usted proporcione múltiples formas de identificación o información para verificar la validez de la identificación de una transacción. Traduzca en línea o en línea para acceder a sus aplicaciones comerciales. El objetivo de la autenticación multifactorial es hacer que sea más difícil para un atacante explotar el

proceso de inicio de sesión para moverse libremente por la red personal o corporativa e irrumpir en equipos informáticos para obtener información de robo, información confidencial, etc.

En pocas palabras, la autenticación multifactorial requiere algo que solo cada usuario tiene (huella digital, huella de voz, llavero de token, código de seguridad o software en el teléfono) y otro que el usuario conoce. Combine con el elemento (como de costumbre). Diálogo de inicio de sesión con nombre de usuario / contraseña) para demostrar que son la persona legítima que afirman (Strom, 2016).

Tecnología RFID

Esta tecnología permite almacenar y recuperar datos sobre objetos que son identificados a través de ondas de radio. Entre las ventajas que este sistema presenta al código de barras, está la comodidad para su utilización, ya que no es necesario establecer un contacto visual entre el objeto identificado y el lector del código de barras. Por otra parte, este sistema permite registrar la información simultánea de varios productos. Está compuesto por diferentes elementos básicos; las etiquetas o tags son tarjetas autoadhesivas, compuestas por un chip y una antena que se incorporan al producto. El lector de esta capta los datos y mediante sus antenas envían la información digital codificada en ondas de radiofrecuencia y el sistema de conectividad que ofrece los servicios de almacenamiento de almacenamiento de información registrada en la base de datos. Las etiquetas pueden ser a su vez pasivas o activas; en el primer caso prescinden de alimentación eléctrica y funcionan a través de la señal que envía el lector al microchip; en el segundo caso posee una fuente de energía propia. Si bien las aplicaciones más habituales de RFID aportan al soporte de la gestión comercial, estas no

son las únicas, ya que dicha tecnología permite un sinnúmero de ellas, como el seguimiento de expedientes para una fácil localización.

Mediciones manuales

En la década de 1960, Wilson Bledsoe trabajó en un sistema donde se podía clasificar imágenes o fotografías de rostro de forma manual, utilizando una tableta RAND (dispositivo donde se podía ingresar coordenadas verticales y horizontales sobre una cuadrícula, usando un lápiz óptico que generaba pulsos electromagnéticos). Este sistema se utilizaba para registrar de forma manual los puntos o coordenada de características faciales (incluyendo ojos, nariz, línea de boca y cabello). Debido a estas métricas, se guardaban las imágenes en una base de datos, cuando se recibían de un usuario, el sistema sería capaz de recuperar imagen que más se asemejara a esta persona dentro de la base de datos.

Marcadores faciales

En los años 70, Goldstein, Harmon y Lesk mejorarían el sistema manual de reconocimiento facial, utilizando 21 marcadores específicos que incluían el espesor del labio y el color de pelo. Pero al igual que el anterior sistema, estas métricas aun debían ser registradas manualmente.

Eigenfaces

En el año 1980, Kirby y Sirovich empezarían a solucionar el problema de reconocimiento facial usando algebra lineal. Mediante el enfoque Eigenface, buscaban representar imágenes faciales de baja dimensión, Estos dos científicos demostraron que se podía tener un conjunto de

características fundamentales, realizando el análisis de las características de un grupo de imágenes faciales. Turk y Pentland en 1991 desarrollarían aún más el enfoque Eigenface, al descubrir cómo localizar rostros dentro de una imagen, siendo los primeros pasos para el reconocimiento automático de caras.

Programa Feret

En la década de 1990, con el propósito de impulsar el mercado de reconocimiento facial, el instituto Nacional de estándares y tecnología y la Agencia de Proyectos de Investigación DARPA de USA crearon el programa FERET (Tecnología de Reconocimiento Facial). Que implicaba la elaboración de una base de datos con imágenes de rostros para la innovación del reconocimiento facial.

Proveedores de reconocimiento facial

A inicios de la década de 2000, el instituto NIST inicia el programa FRVT (Pruebas de Reconocimiento Facial), partiendo de FERT; para evaluaciones gubernamentales mediante sistema de reconocimiento facial comerciales. Esto para cumplir con las leyes estadounidenses.

Medios sociales

Desde el año 2010, la página social Facebook implementa el reconocimiento facial para identificar la cara de una persona que aparezca en la actualización de fotos que realicen los usuarios. Esto tuvo gran controversia ya que generó temas controversiales sobre la privacidad.

Reconocimiento facial en aeropuerto

En 2019, los gobiernos de EE. UU. y Panamá lanzaron el programa piloto de reconocimiento fácil FaceFirt en el aeropuerto Tocumen, para controlar el contrabando y crimen organizado, lo cual fue un éxito.

Reconocimiento de la cara móvil

Desde 2014, el ARJIS (Sistema Automatizado de información de Justicia Regional), distribuye la plataforma móvil FaceFirt a las agencias asociadas. Esta es una red que intercambian datos para el cumplimiento de la ley a personas no identificadas y se consideraban sospechosos.

Termómetro infrarrojo facial

El inventor de termómetro fue (Roberts-Oste, s.f.), un termómetro infrarrojo facial, ideal para medir la temperatura, sin tener contacto físico capaz de medir hasta una cantidad de personas por minutos. Si la temperatura esta fuera de rango o si la persona se encuentra de malestar esta produce una alerta.

Reconocimiento fácil en teléfonos móviles

En el año de 2017, Apple lanzó su teléfono iPhone X que poseía una característica principal de reconocimiento facial para seguridad del dispositivo. El modelo se vendió rápidamente, dando a conocer que el reconocimiento facial sería el nuevo estándar para la seguridad.

Personas que aportaron al reconocimiento facial

Rouhiainen (2019, en su investigación titulada “Inteligencia Artificial para Empresas”, presentada al público en general, menciona aspectos muy importantes como los beneficios y desafíos de la Inteligencia Artificial para empresas en las cuales destacan las mejoras en casi todos los procesos de negocio a través de la automatización, gran mejora en la eficiencia, decisiones de negocio más rápidas y precisas gracias al big data, productos y servicios mejores a través de la innovación y de una atención al cliente mejor y más personalizada. Menciona que la Inteligencia Artificial está cambiando drásticamente el entorno empresarial y cómo funcionan las empresas.

A Bledsoe (1960) se le conoce como “Padre del reconocimiento facial”, debido a su gran aporte en el desarrollo de un sistema que podría clasificar fotos de rostros a mano.

Sirovich y Kirby(1990-200) iniciaron ampliando el algebra lineal al problema del reconocimiento facial. La implementación de una base de datos de imágenes. La base de datos fue actualizada en el 2003 para incluir versiones a color de alta calidad y resolución de 24 bit.

Facebook (2010) fue la primera red social en implementar el uso del sistema de reconocimiento facial en sus redes sociales

. En el 2014 se empieza a implementar el sistema de identificación en los teléfonos móviles inteligentes de alta gama, con distintos fines de

seguridad; y en el 2017 se implementó el uso en las distintas aplicaciones con fines fluidos (LIKE, TIK TOK y otros).

Honeywell (1969) inventó los sensores de movimiento utilizando las alarmas para encender las luces en presencia de cuando hay un movimiento de persona o cosas.

OpenFace

Es una herramienta de código abierto implementada en Python y Torch que utiliza redes neuronales profundas y se basa en la conferencia sobre Reconocimiento de Patrones y Visión, por Computadora (CVPR).

Kairos

Es una plataforma con sus propios servidores de código licenciado entre sus principales funciones cuenta con la detección de rostro, verificación facial, detección de rasgos faciales, agrupamiento de rostros, entre otras funcionalidades.

Kairos es una herramienta utilizada para el desarrollo de sistemas de reconocimiento facial, el cual requiere un suscripción mensual o personalizada para acceder a su API (Interfaz de programación de aplicaciones).

Dlib

Es una biblioteca de software desarrollado en C++, que es fácil de usar a través su interfaz para el desarrollo de aplicaciones o por sus siglas en inglés API, contiene componentes para utilizar en aplicaciones como robótica, procesamiento de imágenes, aprendizaje automático, minería de datos

Dlib para la detección de rasgos faciales utiliza los puntos de referencia (landmarks), estos puntos se encargan de marcar las regiones de un rostro. Nosotros utilizaremos Dlib para la detección de las partes más relevantes de un rostro de esta manera obtenerlos y usarlos para el modelo propuesto.

Torch

Es un marco científico de computación de código abierto que permite que una red neuronal se pueda ejecutar en una UCP (unidad central de procesos) o con CUDA (Arquitectura Unificada de Dispositivos de Cómputo)

OpenFace

Utiliza Torch para el entrenamiento de miles de imágenes que se encuentran en distintos conjuntos de datos, esta herramienta permite hacer un solo entrenamiento para los miles de imágenes que se tenga.

OpenCV

Es una biblioteca de código libre diseñado en C++ / C cuya función es la extracción y el procesamiento de datos a través de imágenes basado en el algoritmo de violaJones.Durante la investigación se utilizará esta herramienta para la alineación, recorte y escala de imágenes en el proceso del modelo propuesto.

CASIA-WebFace

Es un conjunto de datos utilizado para el reconocimiento, compuesta por 10,575 individuos con un total de 494,414 imágenes que son rastreadas desde internet de una forma aleatoria y se pueden usar sin restricciones. En la Tabla 2.1, podemos observar una lista de conjunto de datos más populares, cabe destacar que OpenFace utiliza dos conjuntos de datos, actualmente están en proceso en utilizar el conjunto de datos de MegaFace contando con más de cuatro millones de imágenes para poder mejorar el entrenamiento de la red neuronal.

FaceScrub

Es un conjunto de datos utilizado para el entrenamiento de imágenes de reconocimiento facial de OpenFace compuesta por 100,000 imágenes de 530 personas, estas imágenes fueron tomadas de Internet y se toman en torno a situaciones del mundo real.

1.3- Tipos de sistemas de vigilancia

Cámara infrarroja

Se utilizan en lugares de poca iluminación, permitiendo encender el infrarrojo de forma automática al momento que los objetos emiten una radiación de movimiento.

Cámara de interiores

Se utilizan en hogares y oficina, estas no necesitan poseer característica en cuanto a la luminosidad (nocturnas, infrarrojas, etc.), debido a que permanecen en lugares iluminados.

Cámaras Antirrobos

Este tipo de cámara por lo general graban y capturan imagen en vivo cuando alguien ingresa a un área no autorizada, por lo que debe tener un material resistente a golpes, lluvia, calor, entre otros.

Cámaras IP

Estas se conectan de forma directa a un dispositivo de red, para enviar o subir información a la nube; de igual forma, se puede observar la imagen que esté transmitiendo mediante un dispositivo configurado con la cámara y conectado al Internet.

Cámaras con movimiento y zoom

Se utilizan en los sistemas de cámaras (CCTV), donde una persona encargada se encuentra monitoreando las cámaras y esta les realiza movimiento o zoom.

Cámaras ocultas. También llamadas cámaras espías, en termino general se colocan dentro de algún objeto, como; detectores de humo, sensores de movimiento, espejos, tornillos, enchufes, audio, entre otros. De esta forma no se ven y pasan por desapercibido.

Mediciones y precisión

¿Los Sistema de reconocimiento facial son evaluados por tres criterios?

1. Falso positivo (también conocido como falsa aceptación): Describe cuando un sistema erróneamente hace una coincidencia incorrecta. El número debe ser lo más bajo posible.

2. Falso negativo (también conocido como falso rechazo).

3. Con un falso positivo, un usuario genuino no coincide con su perfil. Este número también debe ser bajo.

4. Verdadero positivo: Describe cuando un usuario registrado coincide correctamente con su perfil. Este número debe ser alto.

Estas tres medidas se presentan en porcentajes. Entonces, digamos que un sistema de entrada evalúa a 1000 personas por día. Si se permite la entrada de cinco personas no aprobadas, la tasa de falsos positivos es de cinco en 1000. Eso es una de cada 200 o un 0.5%.

Entonces, ¿qué porcentajes alcanzan los sistemas actuales? El Instituto Nacional de Estándares y Tecnología (NIST) regularmente prueba múltiples sistemas para buscar en una base de datos de 26.6 millones de fotos.

En su prueba de 2018, descubrió que solo el 0.2% de las búsquedas no coincidía con la imagen correcta, en comparación con una tasa de fallas del 4% en 2014. Se trata de una mejora de 20 veces en cuatro años.

El científico informático del NIST, Patrick Grother, dice: "Las ganancias de precisión provienen de la integración, o del reemplazo completo, de enfoques anteriores con aquellos basados en redes neuronales convolucionales profundas. Como tal, el reconocimiento facial ha experimentado una revolución industrial" (Glother).

La nueva confirmación de la evolución tecnológica proviene de la Tecnología Biométrica del Departamento de Seguridad Nacional en 2018. En su prueba, el Sistema de Identificación Facial en Vivo (LFIS) de Gemalto obtuvo una tasa de adquisición del 99.44% en menos de cinco segundos, en comparación con el promedio de 65%.

1.4- Análisis de factibilidad a nivel internacional y nacional.

En la investigación se puede identificar que este proyecto para ser instalado en los colegios del **Gran santo Domingo** resulta factible, debido a que mejoraría la inseguridad que impera últimamente a nivel general.

En el ámbito internacional, el sistema de reconocimiento facial ha tenido una gran repercusión con la evolución del sistema educativo. Los colegios de Estados Unidos, como otros, se han beneficiado de este, debido a que se han podido identificar personas sospechosas con intenciones de hacer cualquier fechoría que pueda implicar un riesgo mayor para los mismos estudiantes.

CAPÍTULO: 2

DIAGNÓSTICO SOBRE LA PERTINENCIA DEL SISTEMA DE RECONOCIMIENTO FÁCIL DE PATRONES BIOMÉTRICO.

2.1- Diagnóstico sobre la pertinencia de instalar un sistema de vigilancia de reconocimiento fácil de patrones biométrico.

Se espera que este proyecto ayude, en cierta forma, al Colegio Cafam a confrontar la inseguridad que impera en los colegios del gran Santo Domingo, pues busca implementar un sistema de reconocimiento facial biométrico que hará factible el acceso a los usuarios, dando una mejor inspección en la automatización de la entrada y salida del reciento.

A pesar de la inseguridad que impera últimamente a nivel general en los colegios de educación básica en el gran Santo Domingo, el Colegio Cafam no ha estado expuesto a los ataques armados como se ha dado en instituciones de otros países. Sin embargo, en ellos sí se han dado casos de niños (as) secuestrados por uno de los miembros de parejas separadas que, al no tener la custodia, ha provechado la situación para ingresar al colegio en una hora específica y sacar al niño (a). Se han dado otros casos de esa misma naturaleza, en los que han entrado personas ajenas a los colegios, con fines de negocios o de hacer cualquier otra mala acción que pueda implicar un riesgo para los mismos estudiantes.

Para nadie es un secreto que la seguridad en los colegios de educación básica en la República Dominicana es vulnerable. Los colegios pueden aprovechar los avances tecnológicos para implementar este mecanismo de sistema biométrico facial, ya que se estima una población de 150,000 estudiantes.

El sistema de seguridad por reconocimiento facial de patrón biométrico es fiable, fácil de usar y de un nivel de aceptación muy alto, es por eso por lo que se ha escogido como modo de acceso para el sistema de seguridad propuesto.

Las instituciones educativas están en constante evolución. Aunque muchas instituciones internacionales ya se benefician de los sistemas de reconocimiento facial, estos aún no se han incorporado de manera generalizada al campo de la educación dominicana. La implementación de este sistema biométrico en el Colegio Cafam podría suponer múltiples beneficios, ya que sería de gran ayuda para realizar y agilizar gestiones del día a día. Esto iría en apoyo general a la seguridad física del colegio que se encuentra vulnerable.

Tomando en cuenta los antecedentes suscitados dentro de los colegios de Estados Unidos y otros países, este diagnóstico ofrece un método para crear un sistema de reconocimiento facial biométrico que pueda ser utilizado en la educación básica del Colegio Cafam, con la ayuda de cámaras biométricas de alta definición, permitiendo el acceso a las instalaciones a los estudiantes, padres y/o tutores, personal académico y administrativo. Al mismo tiempo, este sistema de reconocimiento facial permitirá enviar alertas del individuo no identificado que haya querido ingresar al colegio, por esa razón se ha introducido la estrategia para ofrecer una solución a esta problemática.

Antes de utilizar el sistema biométrico, se debe completar el registro inicial con la persona que brinda el servicio. En otras palabras, la huella dactilar o el iris de cada usuario deben guiarse a través de la base de datos. Es un proceso similar al de la expedición de una tarjeta o carnet de identidad. A partir de este momento, existen dos maneras de utilizar el sistema biométrico. En primer lugar, se usa para identificar a la persona que se tiene en frente, es decir, saber quién es partiendo únicamente de las muestras biométricas que presenta; o para verificar la identidad de dicha persona, al comparar las muestras biométricas de esta con todos los patrones biométricos almacenados en la base de datos.

En el segundo caso, la verificación, es ligeramente diferente. La persona se identifica mediante un documento como una tarjeta o nombre de usuario o una cédula de identidad. A continuación, se toman sus muestras biométricas y estas se comparan sólo con el modelo biométrico faciales almacenado en la base de datos. Esta evaluación es en gran medida más rápida, ya que se compara con el inicio de una identificación, permitiendo reconocer si se trata o no de la misma persona.

Ningún método es mejor que otro, todo depende de la aplicación que se incorpore. Por ejemplo, desde que una persona llega a la casa tiene sus dedos solamente para entrar y poder acceder a ella en lugar de utilizar la llave; cuando llega al aeropuerto, antes se utilizaban boletos en los que estaba escritos el nombre y se necesitaba una identificación extra para poder abordar al avión y despegar, en la actualidad no se necesita más que utilizar la cara para poder volar. Como las identificaciones biométricas han cambiado la vida, los teléfonos celulares tiene la capacidad de leer la huella digital, las redes sociales, el Twitter, Facebook, Instagram y cada una de esta aplicación se requiere de un Password o a través del reconocimiento facial, sin la necesidad de recordar todos estos números.

2.2- Elaboración del diseño del diagnóstico

Para lograr que un sistema de seguridad de control de accesos cumpla con los objetivos requeridos y sea satisfactorio, se debe emplear la siguiente herramienta de seguridad, donde se certifica la necesidad del diseño de este prototipo para ser utilizado en la institución.

Los requisitos funcionales del módulo del sistema de control de acceso se enumeran se enumeran a continuación.

Paso1: Lector Biométrico de Huella

Los escáneres de huellas dactilares biométricos son dispositivos de entrada llamados "biometría" que escanean huellas dactilares para identificar usuarios específicos, lo que les permite analizar y comparar huellas dactilares.

Paso 2: Huellas

Puede ser que sean útiles a la hora de sostener objetos ásperos, pero si esta fuera su función principal, se tendrían huellas dactilares en toda la mano. Lo que está claro es que mejoran la sensibilidad táctil mediante la amplificación de pequeñas vibraciones, cada vez que los dedos rozan una superficie.

Paso 3: Procesamiento y comparación

La comparación de procesos constituye un mecanismo de identificación de procedimientos de trabajo específicos que podrían mejorarse a través de la imitación de ejemplos externos de excelencia que pueden establecerse como la mejor práctica de la industria. En ese sentido, implica la comparación de la propia empresa de servicios con empresas similares, con el propósito de lograr un auto mejoramiento mediante la adopción de estructuras o métodos que en otras partes se utilizan con éxito.

Paso 4: Base de datos

Es una colección organizada de información estructurada, o datos, típicamente almacenados electrónicamente en un sistema de computadora.

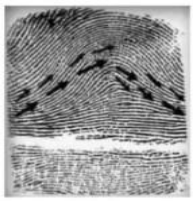
Tabla No: 1 Requerimientos funciones

D	Requerimiento	Descripción	Prioridad
COD001	Registro Usuario	Permite a los Administradores del sistema fácil biométrico registrar a los usuarios permitido a entrar y salir.	Alta
COD002	Modificar usuario	El encargado del sistema puede realizar modificaciones al este con los usuarios ya existentes.	Alta
COD003	Agregar Sesión	El encardado administrativo, tiene acceso a verificar las sesiones ingresa durante la semana.	Alta
COD004	Eliminar Sesión	El administrador del sistema facial puede eliminar la sección registrada en el sistema.	Alta
COD005	Visualizar usuarios registrados	Esto permite a los administradores del sistema ver a los usuarios registrado en la base de datos.	Alta
COD006	Agregar Dependencias	El administrador del sistema es responsable de agregar las dependencias registradas cuando el visitante ingresa a la institución.	Media
COD007	Eliminar Dependencias	Los administradores del sistema pueden eliminar dependencias previamente guardadas	Media
COD008	Salir plataforma	Esto permite que el administrador abandone la plataforma.	Media

2.3- Tipos fundamentales de huellas dactilares

Arco huella

La huella de los dedos tiene el debido detalle de ser únicos e irrepetibles con carente de delta.

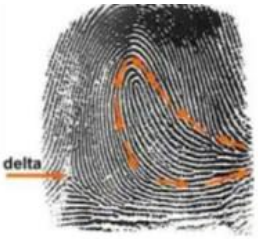


Presilla Interna

Se caracteriza por Dactilograma que vislumbre uno, dos o más deltas al del observador.

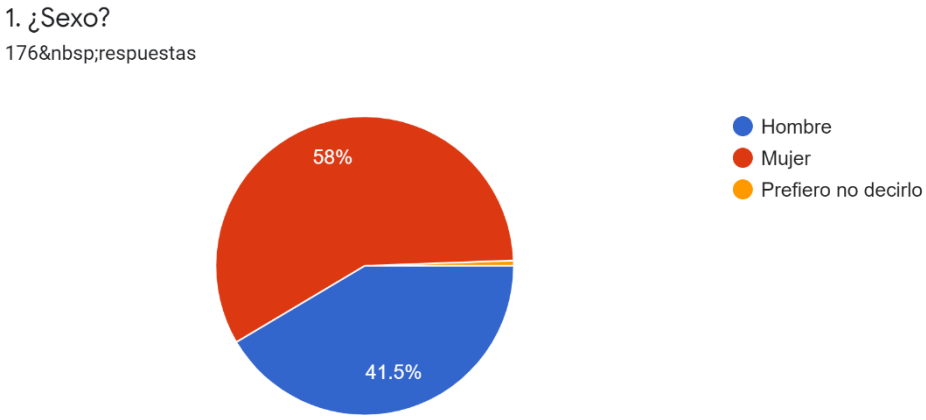
Presilla Externa

Se caracteriza por un Dactilograma que presenta uno o dos más deltas a la derecha del observador.

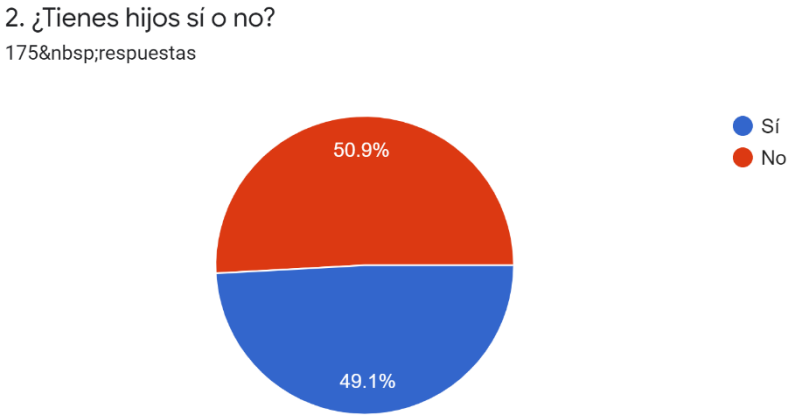


2.4- Implementación de la encuesta y entrevistas

De conformidad al proyecto de investigación se aplicó la encuesta a 176 personas ubicada en Santo Domingo.



El proceso de calificación fue liderado principalmente por las mujeres con 58%, el segundo gráfico se caracterizó por el 1,5% de los hombres y el tercer gráfico fue detectado en el 0,5% por un grupo de personas a las que no les gustó. Se distingue el género.

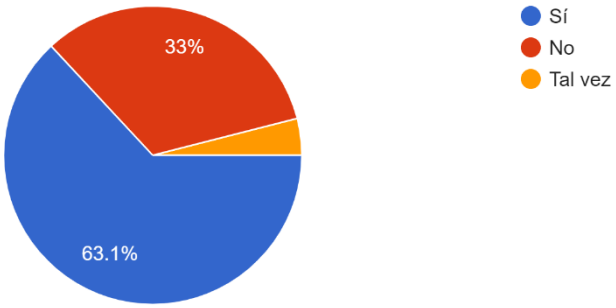


Se puede observar que el 50,90% de la muestra tienen hijos y el 9,1% restante no tiene hijos.

El 72% de los encuestados dijo que sabían cómo funcionan los sistemas de reconocimiento facial en la actualidad, mientras que el 17% dijo que sabían cómo funcionan los sistemas faciales y el resto 10,9% por falta de información, desconocen del su funcionamiento.

4. ¿Has utilizado el reconocimiento facial en algún dispositivo celular, tablets, otros?

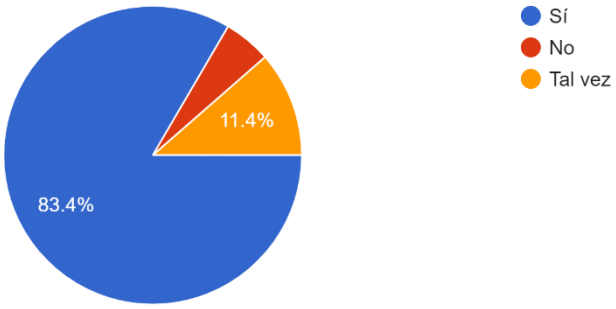
176 respuestas



De los encuestados, el 63,1% dijo que lo habían usado, mientras que el 33% dijo que nunca había usado un dispositivo de reconocimiento facial y el 3,9% dijo que tal vez, pudo haberlo usado.

5. ¿Esta ud. de acuerdo que se implemente un sistema de reconocimiento facial para ser utilizado en los colegios de educación básica, para identificar a los padres al momento de recoger a su hijo?

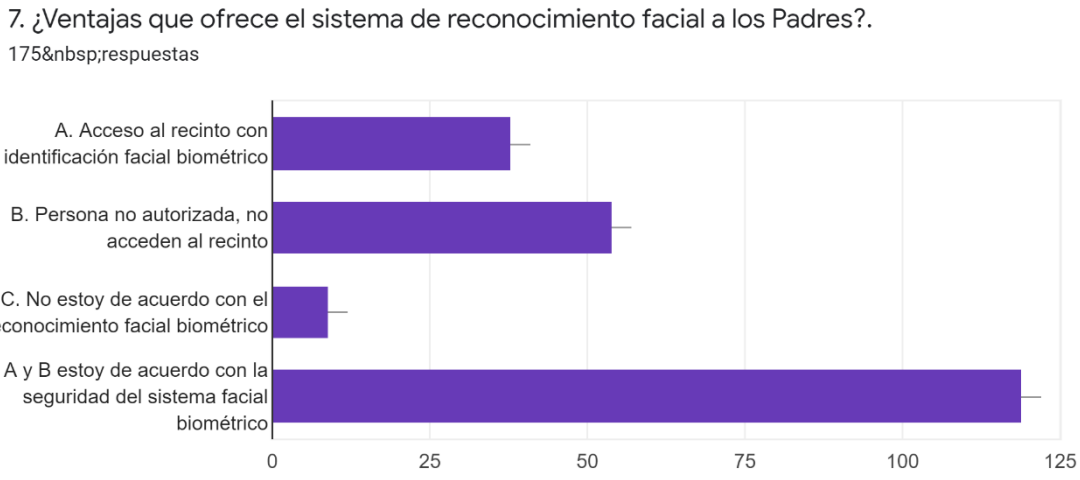
175 respuestas



El 83.4% de los encuestados dijo que le gustaría utilizarlo como medio de acceso para acceder a la institución, mientras el 11.4 % dijo que

no está de acuerdo con la implementación del sistema en Colegio y el 5.2% dijo que tal vez probablemente quisiera.

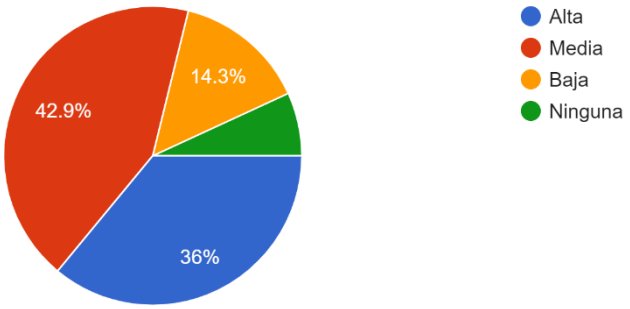
El 56,8% de los encuestados confirman que el sistema facial es seguro, mientras el 36,9% dijo que no es seguro y el 6,3% dijo que probablemente tal vez sea seguro cuando se llegue a implementar.



El 56,8% de los encuestados confirmó que el sistema facial es seguro, mientras el 36,9% dijo que no era seguro y el 6,3% dijo que probablemente tal vez sea seguro.

8. ¿Cuáles son sus expectativas de la implementación de este sistema facial en los colegios de educación básica en el Gran Santo Domingo?.

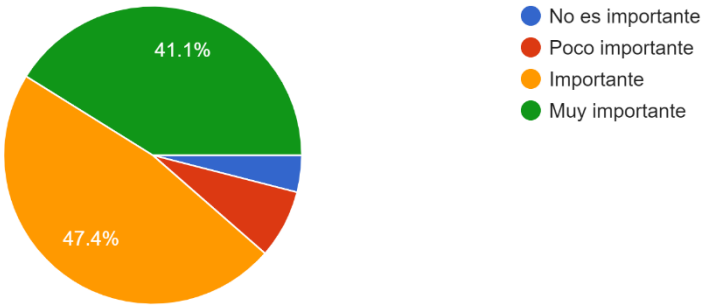
175 respuestas



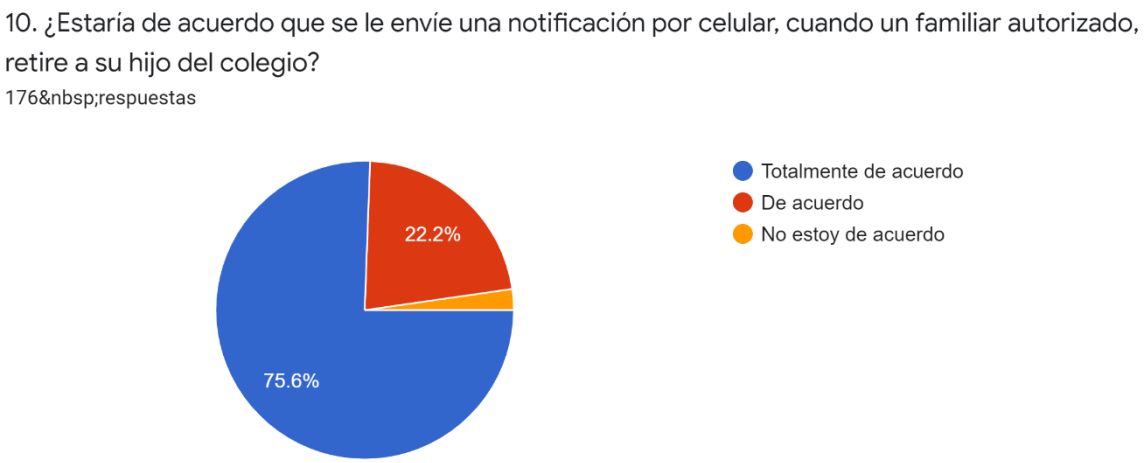
El 42.9% de los encuestados consideran que sus expectativas son medias, el 36% considera que su expectativa es alta, mientras que el 14.3% califico como baja la expectativa y el 6,8 restante eligió ninguna expectativa espera del sistema.

9. ¿Qué tan importante consideras este producto en la seguridad infantil en los colegios de educación básica?

175 respuestas



El 47.4% de los encuestados dijo que el sistema facial es importante su funcionamiento en la institución educativa, y el 41.1% lo consideró muy importante, mientras que el 6.4 cree que es poco importante y el 5.1% lo considera no importante.



El 75,6% de los encuestados están de acuerdo de que el sistema envíe notificación cuando su hijo sea retirado con familiar autorizado, mientras el 22,2% no está de acuerdo con el sistema de la notificación y el 2,2% no está de acuerdo.

Entrevista

De conformidad al proyecto de investigación se aplicó la entrevista a 16 personas ubicada en Santo Domingo.

1. **¿Qué es un sistema de reconocimiento facial biométrico?**

El reconocimiento facial es un método para identificar o verificar la identidad de una persona a través del rostro. De igual forma se pueden utilizar para identificar personas en fotos, videos o en tiempo real.

2. **¿Cómo funciona el sistema?**

El funcionamiento del sistema, esta familiarizados con la tecnología del reconocimiento facial Face ID utilizada para desbloquear el iPhone, mientras que otras similares la utilizan las empresas para identificar a los empleados.

3. **¿Quiénes usan el sistema de reconocimiento facial?**

Lo utilizan las empresas para optimizar proceso, Google, Amazon, Facebook, Android o Apple usan el reconocimiento facial para mejorar la seguridad y la experiencia del usuario, facilitando pagos móviles seguros y acelerando ciertos procesos.

4. ¿Ventajas del reconocimiento facial?

- Bajo riesgo de robo de información personal
- Ninguna acción de manipulación del usuario
- Efectivo con otros métodos biométricos
- No utilice factores externos para la identificación
- No necesita el uso de contraseña.
- Difícil de vulnerar el equipo

5. ¿Seguridad biométrica?

La seguridad biométrica se conoce como una aplicación biométrica para proteger y asegurar dispositivos, instalaciones o información corporativas o de usuario sensibles y es más avanzada que los métodos tradicionales como contraseñas, de acceso y tarjeta.

2.3- Sistematización de los hallazgos

Después de haber realizado la encuesta, se puede decir que la causa de un sistema de reconocimiento facial se debe a la falta de un sistema de control de acceso biométrico instado en los Colegios del Gran Santo Domingo.

Además de que hay un alto porcentaje de algunos padres que indican que estarían de acuerdo con la implementación de un sistema de reconocimiento facial biométrico por las ventajas de seguridad que esta ofreces, al momento de que un padre o tutor retire su hijo del Colegio.

Se puede afirmar que la mayoría de las personas encuestados, alegan de que en los Colegios se actualicen con sistema tecnológico de seguridad, que mayor control en la entrada y salida de personas de la institución. Como también, las ventajas y beneficio que ofrecen a los padres, profesores y personal administrativa.

Se puede comprobar que la menoría de los encuestado afirma, que no estaría de acuerdo con la implementación de un sistema de reconocimiento facial biométrico en colegios de educación básica del gran santo domingo, debido a que el sistema facial no es seguro.

CAPITULO: 3

PROPONER EL DISEÑO DEL SISTEMA DE RECONOCIMIENTO FACIAL DE PATRONES BIOMÉTRICO

3.1- Sistema de Reconocimiento Facial de patrones biométrico

Un sistema biométrico es un método automático de identificación con el fin de identificar a un usuario en tiempo real. Su principal ventaja es realizar el reconocimiento de una persona por medio de sus rasgos o un patrón único que lo diferencia de los demás.

Para la realización de un sistema biométrico, es necesario distinguir el tipo de registro biométrico. En la Biometría, se distinguen dos tipos, la Biometría Estática y la Biometría Dinámica. Donde la Biometría Estática hace referencia a las características físicas, es decir se enfoca a los aspectos fisiológicos o morfológicos de una persona, como la huella dactilar, las características del iris, patrones en la retina, entre otras. Mientras que la Biometría Dinámica, se enfoca en las características conductuales de una persona, por ejemplo: dinámica de la firma, pulsaciones en el teclado, entre otras.

3.2- Elaboración de la propuesta del sistema

Podemos decir que este proyecto es factible, ya que mejoraría el sistema de seguridad estudiantil con la que cuenta actualmente el Colegio Cafam, proponiendo un mejor servicio en el sistema de vigilancia, en la entrada y salida del personal.

Factibilidad Operacional

Ante la propuesta de desarrollar un sistema de reconocimiento facial de biométrico para la detección de personas no autorizadas al ingresar al colegio se ha contado con el apoyo de los padres de los estudiantes para realizar una investigación que sea necesaria para el correcto desarrollo de este proyecto.

Desde el punto de vista operativo se considera que el desarrollo de este sistema traerá beneficio a todos los padres y personal administrativo del colegio, debido a que se realizaron encuestas a los padres, para saber el conocimiento que tienen acerca del sistema facial biométrico que contara la institución, y así validar el grado de aceptación del proyecto. Con los resultados obtenidos se ha concluido que el proyecto planteado es factible operacionalmente.

Factibilidad Técnica

Software

Para demostrar la simulación se necesitaron los siguientes componentes:

- Computadora
- Cámara Digital

Computadora

Este equipo es principal ya que si se quiere que el sistema funcione correctamente es necesario que la PC conste con características básicas, donde se pueda instalar de manera correcta el programa con el fin de llevar a cabo una buena presentación.

Para esto se utilizará una PC con las siguientes características:

Tabla No: 2 Descripción del equipo

Equipo	Sistema Operativo	Disco Duro	Memoria	Procesado
PC/ Dell	Windows 10 64bits	1TB	16GB	Icore7

Cámaras faciales

Las cámaras faciales son de suma importancia para el procesamiento de imagen, con la técnica del reconocimiento facial es necesario tener en cuenta factores como: resolución, pixeles, calidad de imagen etc.

Debido a las especificaciones técnicas que se necesitan para llevar a cabo este proyecto se optó de la mejor manera utilizar la Webcam Genius Facecam ya que esta dispone de los requerimientos antes mencionados.

Factibilidad Económica

Para el desarrollo de la simulación del tema propuesto utilizamos recursos de hardware, software, entre otros recursos que detallamos a continuación.

PRESUPUESTO

Para gestionar el proceso de entrega de estudiantes mediante el sistema facial Display Child.

- Deberá proporcional un Hardware con las características detallas más abajo.
- Para el mostrar el nombre del estudiante se requiera un Monitor o TV.
- Requerimientos de Hardware y Software para instalación de Software de gestión.

Tabla No: 03 Recomendaciones de almacenamiento del pc

Rubros	Recomendaciones
Procesador	Inter Core i7 / Xeon E3 0 AMD Atlon
Memoria Ram	16 Gb
Sonido	1tb
Sistema Operativo	Compatible con Windows / Linux
Motor de Base de Datos	SQL 2018

Modelos de lectora ofrecidos en esta propuesta

Cuadro No: 4 Detalles de los equipos faciales

cant	Cod producto	DETALLE DEL PRODICTO	Precio	Toral
1	DCh-SB	Software Display Child de SoftBox	47,750.00	147,750.00
1	ZK-TRAC100	Zk-Teco Lector de Huella de Pedestal a prueba de agua	18,900.00	38,900.00
1	S-HDMI-C4	Spliter HGMI 4 CH	2,700.00	5,700.00
3	CNV-RJ45-H	Convertidor RJ45 to HDMI	1,675.00	6,025.00

1	CAB-MT-MO	Cableado, Tuberia y Materiales de Intalación	15,550.00	55,550.00
1	MO-CONF	Instalación, parametrización, Entrenamiento & Soporte	12,000.00	68,700.00
				TOTAL, RD$ 322,625.00

Condiciones generales:

- El costo de Licenciamiento Display Child será un solo costo, cubriendo actualizaciones y nuevas versiones y todos los servicios del Software.

- Los Hardware donde estará instalado Software y los Monitores serán proporcionados por el cliente según las características identificadas anteriormente.

- Soporte en Sitio luego de instalación se consideró en Santo Domingo serán de cuatro (6) visitas anuales

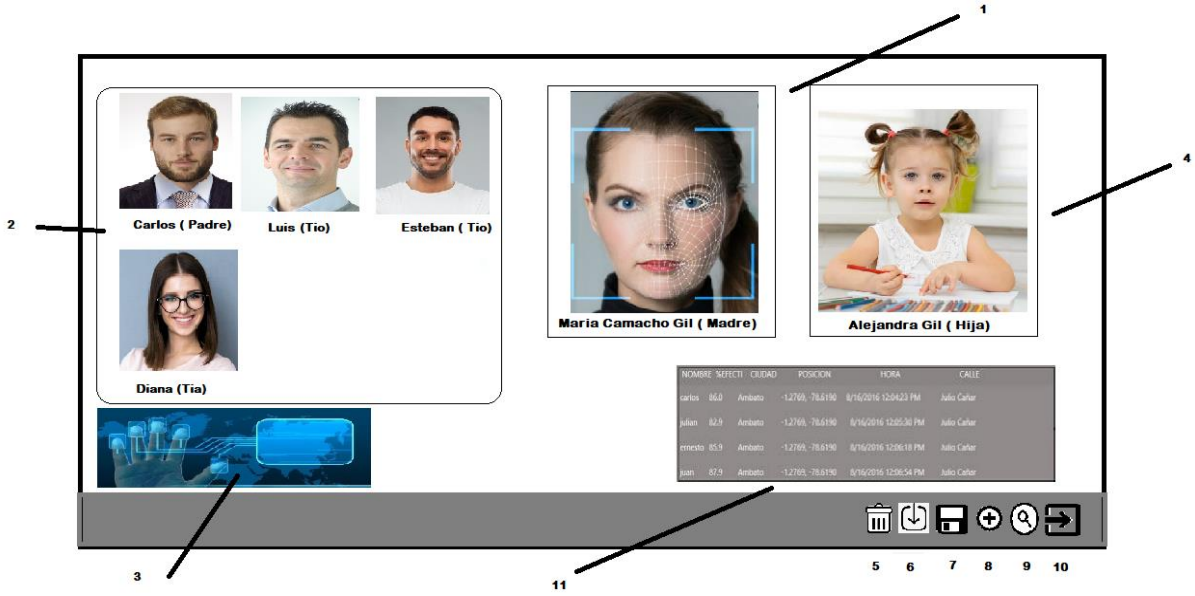
- Capacitaciones permanentes vía remota.

3.3- Presentación a los directivos y APMAES de las entidades educativas.

Presentación del sistema de reconocimiento facial biométrico.

Debido a los tiempos actuales que conocemos en donde cada vez es más indispensable tener controles para garantizar la seguridad de los niños (a) de la escuela, por este motivo el sistema ayudará aumentar la vigilancia controlando la entrada y salida del colegio por biometría facial y dactilares a personas registradas al sistema, que pueden llevar y traer a su hijo (a), avisando en tiempo real una notificación a los padres o tutores cuando sus hijos entren o salgan de la escuela.

Visión general del sistema



Menú del sistema administrativo

Figura No 1. Pantalla que visualiza la imagen vinculada al sistema, donde se muestra la persona registrada.

Figura No 2. Este segmento muestra una lista de personas que están autentificado en el sistema, como familiares autorizados.

Figura No 3. Segmento de interfaz gráfica que muestra las huellas dactilares en tiempo real en el sistema biométrico facial.

Figura No 4. Segmento de pantalla en la cual se muestra una captura del niño o niña identificada por el sistema.

Figura No 5. Botón para borrar la pantalla después de una búsqueda realizada.

Figura No 6. Botón que permite descargar imágenes manualmente desde el sistema.

Figura No 7. Botón que permite guardar manualmente la imagen en una ubicación específica del sistema.

Figura No 8. Botón que permite agregar nueva persona al sistema biométrico.

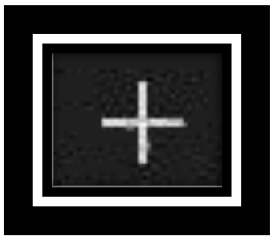


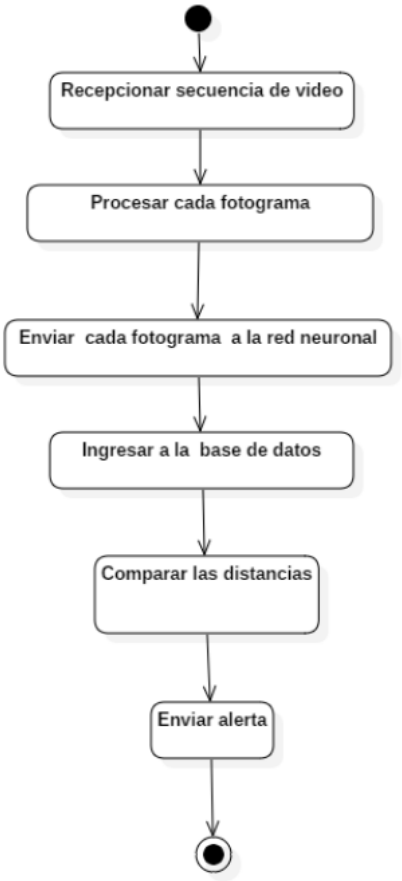
Figura No 9. El botón envía una señal al sistema para identificar a la persona que entran al colegio, similar a un botón físico.

Figura No 10. Botón para salir del sistema.

Figura No 11. En el segmento de interfaz gráfica, muestra los perfiles de información de las personas identificadas por fecha, hora entrada y salida, del sistema.

NOMBRE	%EFECTI	CIUDAD	POSICION	HORA	CALLE
carlos	86.0	Ambato	-1.2769, -78.6190	8/16/2016 12:04:23 PM	Julio Cañar
julian	82.9	Ambato	-1.2769, -78.6190	8/16/2016 12:05:30 PM	Julio Cañar
ernesto	85.9	Ambato	-1.2769, -78.6190	8/16/2016 12:06:18 PM	Julio Cañar
juan	87.9	Ambato	-1.2769, -78.6190	8/16/2016 12:06:54 PM	Julio Cañar

Figuera No.12 Muestra el diagrama de proceso.



CONCLUSIÓN

En el presente trabajo se ha presentado el desarrollo de un sistema de reconocimiento facial a partir del análisis de la información de profundidad del rostro facial.

La creación de un sistema para la seguridad escolar se plantea como una propuesta tecnológica novedosa que reemplazaría el proceso manual lo cual provoca pérdida de recursos y tiempo.

El sistema cuenta con una interfaz sencilla de administración que permite administrar la información de cada uno de los socios que pertenecen a la cooperativa.

En ese orden de ideas, este trabajo se enmarco en el diseño de un sistema de seguridad biométrica que funcione como medio de control de acceso y detección de intrusos, robos y secuestros facilitando la detección de personal no autorizado dentro del organismo de seguridad del Colegio. Todo esto, mediado por el Sistema de reconocimiento fácil.

A partir de allí y en correspondencia con los objetivos planteados, se identificaron las áreas críticas que representan un riesgo de seguridad en el Colegio; como resultado se referenciaron los pasillos y aulas de niños de educación básica como puntos débiles dentro del sistema de seguridad y que representan un riesgo alto en el Colegio.

Hoy en día, la mayoría de los países del mundo utilizan esta tecnología como un sistema de identificación conveniente y seguro. Existen varios métodos de identificación, como el escaneo de huellas dactilares, el iris del ojo, la fiebre facial o la voz. Determine el mejor método de reconocimiento humano.

Los sistemas de reconocimiento facial han revolucionado los medios tradicionales de control, puesta a punto y acceso a los vehículos, logrando mayores niveles de precisión y un mejor uso de los recursos económicos en las operaciones.

Los sistemas faciales resultan ser tecnología avanzada de Campaz destinada a mejorar, orientar, revolucionar y mejorar la calidad de servicio de una empresa de una forma casi imposible de irrumpir en los sistemas de seguridad antes mencionados.

La inteligencia artificial en su desarrollo se está diversificando en campos especializados. Las áreas más importantes incluyen el procesamiento del lenguaje natural, la robótica, la visión por computadora, los juegos y los sistemas de base de conocimientos. Posteriormente, el sistema evolucionó hasta convertirse en un sistema experto, que actualmente es una de las tendencias más importantes en el desarrollo de la inteligencia artificial. Algunos autores lo consideran un dominio independiente del sistema de base de conocimientos.

Este desarrollo hace más que sentar un precedente práctico. Se sentaron las bases teóricas para apoyar nuevas experiencias prácticas. La mayoría de los autores coinciden en algunas características a considerar a la hora de definir un sistema experto. Estos se incluyen en la definición del sistema experto propuesto en este estudio. Un sistema basado en el conocimiento que toma decisiones o inferencias efectivas a través de modelos aproximados de estrategias de resolución de problemas utilizados por expertos humanos en un campo en particular.

Determinar qué es esencial para desarrollar un sistema experto es otra contribución de la experiencia de desarrollo inicial. Estos factores son campos de aplicación, métodos de desarrollo, métodos de representación y mecanismos de resolución de problemas.

Se ha determinado que la influencia del Machine Learning en la eficiencia del Comercio Internacional es positiva ya que se tiene como sustento el hallazgo del coeficiente de correlación de Spearman que fue de 0.478. Además, basándonos en los resultados de las encuestas, las empresas peruanas de Comercio Internacional se muestran, casi en su totalidad, muy positivos respecto al Machine Learning y su influencia. También, creen que pueden beneficiarse de esta herramienta, quieren capacitarse para conocer más sobre el ML y sus usos, afirman un potencial uso del ML en todas las áreas de las empresas y ven un futuro positivo para su adopción en las empresas de Comercio Internacional.

Se ha demostrado que la influencia de la Robótica con IA en la eficiencia del Comercio Internacional es positiva, tomando en cuenta el hallazgo del coeficiente de correlación de Spearman que fue de 0.508. También, analizando los resultados de las encuestas, las empresas peruanas de Comercio Internacional muestran, casi en su totalidad, una postura muy positiva hacia la Robótica con IA y su influencia en el Comercio Internacional. La mayoría utilizaría un producto de la Robótica con IA y afirma que la eficiencia de su empresa mejoraría, les gustaría capacitarse para conocer más sobre la herramienta, afirman que es beneficiosa para el futuro del Comercio Internacional y ven con positivismo su implementación en las empresas de Comercio Internacional.

Se ha determinado que la influencia de los Asistentes Virtuales en la eficiencia del Comercio Internacional es positiva, considerando el hallazgo del coeficiente de correlación de Spearman que fue de 0.469 el cual es

significativo al 0.05. Además, basándonos en los resultados de las encuestas, las empresas peruanas de Comercio Internacional indican, casi la totalidad, una postura bastante positiva hacia los Asistentes Virtuales y su influencia en la eficiencia del Comercio Internacional, además, si utilizarían un producto de los Asistentes Virtuales, afirman quieren capacitarse para conocer más sobre la herramienta, afirman un potencial uso en varias áreas de las empresas y ven con positivismo su futura implementación en las empresas de Comercio Internacional.

RECOMENDACIONES

Para utilizar este sistema biométrico, lo recomendable es que tenga un escenario que posee buena iluminación agradable, para que la aplicación de reconocimiento pueda tener un mayor enfoque hacia la persona.

Se requiere un monitor o televisor para mostrar el nombre del estudiante y el padre.

Requiere hardware y software de alta capacidad para instalar el software de gestión.

Dado que los sistemas biométricos pueden detectar a muchas personas al mismo tiempo, recomendamos utilizar un sistema de procesamiento rápido que pueda procesar la información de la base de datos para una comparación eficiente.

Las cámaras deben tener ciertas características, como la resolución de la imagen, en términos de calidad para la detección de individual no identificado.

Para mayor seguridad, la información debe almacenarse en un sistema seguro.

BIBLIOGRAFÍA

ANGULO USATEGUI, J. (1986). Visión Artificial por Computador. Madrid: Thomson Paraninfo S.A.

BRANCH, J., & Olague, G. (2001). La visión por computador: Una aproximación al estado del arte.Revista Dyna.

CÁCERES, T. J. (2002). La visión artificial y las operaciones morfológicas en imágenes binarias. Alcalá, España.

CALLE, A. S. (2005). Aplicaciones de la visión artificial y la biometría informática. Madrid: Dykinson.

CAMBRIDGE, A. L. (1994). The Database of Faces. Obtenido de AT&T Laboratories Cambridge: http://face-rec.org/databases/.

FEIGENBAUM, E. A. (1984). The fifth generation: artificial intelligence and Japan's computer challenge to the world. New York: New American Library.

FREUND, Y., & SCHAPIRE, R. E. (1997). A decision-theoretic generalization of on-line learning. Journal of Computer and System Sciences.

GÁMEZ JIMÉNEZ, (2009) Carmen Virginia, Diseño y desarrollo de un sistema de reconocimiento de caras.

GÓMEZ VERDEJO, V., ORTEGA-MORAL, M., ARENAS-GARCÍA, J., & FIGUEIRASVIDAL, A. R. (2006). Boosting by weighting critical and erroneous samples.

HESELTINE, T., Pears, N., & AUSTIN, J. (2002). Evaluation of image preprocessing techniques for eigenface-based face recognition. In Second International Conference on Image and Graphics.

JAIN, A., Bolle, R., & PANKANTI, S. (2006). Biometrics: personal identification in networked society. New York: Springer Science & Business Media.

JAIN, A., Flynn, P., & Ross, A. A. (2007). Handbook of biometric. New York:

Ken-Ichi, M., MASATSUGU, K., & HIDENORI, S. (1978). Design of local parallel pattern processor for image processing. Proceedings of the National Computer Conference.

Plegrí, J. (2019). Inteligencia Artificial y Robótica: La búsqueda de la perfección de la producción. Recuperado de https://blog.universal-robots.com/es/inteligencia-artificial-yrobotica

Quierotec (2018). 6 características de la Inteligencia Artificial. Recuperado de https://www.quierotec.com/inteligencia-artificial-caracteristicas/

Ros, I. (2018). Amazon mejora su eficiencia gracias a los robots Kiva. Recuperado de https://www.muycanal.com/2018/10/20/amazon-eficiencia-robots-kiva

Quierotec (2018). 6 características de la Inteligencia Artificial. Recuperado de https://www.quierotec.com/inteligencia-artificial-caracteristicas/

Saavedra, B. (2018). Empresas peruanas de exportación de servicios son premiadas por Promperú. Recuperado de https://infomercado.pe/empresas-peruanas-de-exportacion-deservicios-son-premiadas-por-promperu/.

ANEXO

Anexo.1

UNAPEC
ESCUELA DE GRADUADOS

SOLICITUD Y AUTORIZACIÓN EMPRESARIAL PARA REALIZACIÓN DE TRABAJO FINAL

Yo, **Riquelmy Calcaño Hernández**, cédula **223-0093064-5**, matrícula de la Universidad APEC **2019-1428**, estudiante de término del programa de **Gerencia y Productividad Sistema de Reconocimiento Fácil**, cursando la asignatura de trabajo final, solicita la autorización de (nombre de la empresa) para realizar mi trabajo final sobre (nombre o título de la investigación) y acceder a las informaciones que precisaré para este fin.

Este trabajo tiene por objetivo aportar en **la seguridad del Colegio Cafam.**

(Firma)

Yo, **Sr. Martires Peñas Reyes** (nombre de quien autoriza) **Director de Seguridad**, (cargo que ocupa), cédula 001-1202303-1, autoriza a realizar el trabajo final arriba señalado y que el mismo podrá:

Utilizar [x] el nombre de la empresa [ ] Utilizar un pseudónimo

[x] Ser expuesto ante compañeros, profesores y personal de la Universidad APEC

[x] Incluido dentro del acervo de la Biblioteca de UNAPEC

[x] Aplicado en el área correspondiente dentro de la empresa si responde a las necesidades diagnosticadas.

UNIVERSIDAD APEC DIRECCIÓN DE SEGURIDAD Santo Domingo, R.D.

(Firma y sello)