Procesamiento de rostros a favor de la seguridad informática

Jovanny Israel Zepeda Roque

11/11/2014

1. Resumen:

Con la evolución del conocimiento informático la seguridad de la información se ha convertido en algo tan critico y fundamental que hoy en día es impredecible, sin embargo los algoritmos hasta el momento diseñados no son suficientes ya que los hackers siguen bombardeando nuestras aplicaciones para infiltrarse y robar información de muchos usuarios de cualquier tipo, sea este de tipo social o bien de tipo mas personal, por lo tanto nuestra obligación recae en crear nuevos mecanismos para evitar la falsificación de datos y para ello desarrollamos nuevos mecanismos tales como el análisis del rostro humano vivo.

2. Introducción:

Hablar de la seguridad es algo bastante común hoy en día ya que sin ella la vida no seria como la conocemos, simplemente seria un caos total y probablemente la esperanza de vida seria bastante corta a comparación de la que tenemos hoy en día, sin embargo esta seguridad que se menciona todo mundo la conoce y tiene presente ya que es bastante común el ver una estación de policía o comerciales con números públicos para presentar denuncias sobre abusos o maltratos o algo que no sea lo correcto, pero esta es la seguridad simple la que nosotros podemos ver, es algo que todos entienden y comprenden como funciona pero no es el único método de seguridad ya que este es solo física y actúa en el mundo real pero que pasa cuando nosotros dejamos el mundo real y disfrutamos de las cosas que todos nuestros antecesores han logrado crear a través de la historia, cuando usamos una aplicación, nos conectamos a una red social, realizamos una transferencia bancaria o cualquier otra cosa que se nos pueda ocurrir a nivel aplicación o a nivel web, aquí no todos saben que pasa realmente de hecho muchos no tienen ni la mas mínima idea del proceso tan complicado que se ha tenido que llevar para poder lograr que algo sea totalmente seguro y que aun así no siempre es lo suficientemente seguro por que alguien mas puede llegar a interceptarlo, es hay donde pese a la poca valoración o total ignorancia que dan los usuarios mortales hacia un sistema de seguridad nosotros tenemos que actuar, ya que todos los días es común tener que enfrentarnos a problemas de seguridad tan fuertes que no son pensables para los usuarios y es que en definitiva no es lo mismo un ataque físico a un informático, simplemente aquellos que hacen un ataque informático son personas muy capaces e inteligentes que bombardean todos los mecanismos de seguridad hasta encontrar una falla en ellos y aprovecharse de ellos por eso aquí en esta rama se deben estar inventando cosas nuevas a cada momento, de aquí nace la razón de este articulo se trata de explicar de forma sencilla como los usuarios pueden hacer todo lo que conocen de forma segura y además la explicación de un método adicional que ya esta siendo utilizado para algunos procesos pero que se puede seguir evolucionando conforme evoluciona la historia informática, con ello nos referimos a la visión computacional que ya tiene tiempo con nosotros pero que no se conoce para que sirve, pero he de aclarar que todos nosotros la usamos a cada momento para nuestras actividades cotidianas y no nos damos cuentas por ejemplo al tomar fotografías y detectar las sonrisas, detección de rostros que cualquier móvil trae en la actualidad, o bien en otro ámbito que es conocido seria cuan-

do alguien no deseado entra a algún lugar y en seguida responde seguridad para sacarlo, todo ello es la visión computacional que se ha ido desarrollando y no se va a detener por que es el futuro con ello se crea una seguridad muy avanzada por ejemplo la detección de rostros que es la que nos enfocaremos en el resto del documento y que es importante por que con ella es posible evitar la falsificación de datos ya que es mas fácil obtener una contraseña y un usuario que un rostro humano y aun mas difícil si se aplican los nuevos algoritmos para detectar si es rostro vivo o una fotografía y aun mas si los datos viajan a través de una conexión totalmente segura por el servidor tal y como lo hacen el sistema ssl, vpn o ssh (metodos de seguridad que evitan la lectura de los datos por alguien mas a parte del usuario y el servidor al que enviamos los datos), ahora que se definió toda la parte introductoria y se tiene una idea mayor sobre este ámbito de seguridad hablaremos sobre en que consistirá el proyecto al que nos enfocaremos la primer parte sera el inicio de la aplicación y la detección de rostro de la persona al hacer esto se conectara con el servidor y buscara en la base de datos para comprobar que el rostro esta identificado, si es así se abrirá el portal para ingresar el usuario y la contraseña que corresponden al rostro, si estos son pasados correctamente se tendrá acceso a al aplicación, así probaremos si es un método bueno o no debido a que hay probabilidades que sea tardado por los cálculos a realizar.

3. Antecedente:

La biométrica facial nació aproximadamente en los anos 60 cuando se creo el primer sistema semiautomático para la detecciióón de diversas partes del cuerpo tales como los ojos, orejas, nariz y la boca, sin embargo este sistema úúnicamente era capaz de realzar las detecciones sobre imáágenes de algún individuo las cuales posteriormente buscaba dentro de una base de información bastante densa, posteriormente en los anos 70 surgió un nuevo cambio a este proceso ya que con la ayuda de los investigadores Goldstein, Harmon y Lesk quienes implementaron un méétodo totalmente innovador para esta rama de investigación, este método consistía en agregar 21 marcadores con diferentes cambios de forma, textura, color u otros rasgos los cuales servían para poder obtener mayor precisión al momento de analizar un rostro humano, sin embargo esto no fue suficiente debido a que el método tenia que ser computado de forma manual, al paso de los anos Kirby y Sirobich aplicaron un método aun mas distinta la cual consistía en técnicas de álgebra linea

que fue bastante buena debido a que con no mas de 100 cálculos se obtenía el rostro idenficado siempre y cuando este estuviese bien alineado y perfilado, todo esto fue para los anos 1988, En 1991 Turk y Pentland dieron uso a las técnicas Eigenfaces el cual dio acceso a obtener el reconocimiento facial de un rostro en tiempo real lo cual de hecho fue bastante bueno debido a que a partir de este punto el interés a al creación de sistemas que permitiesen realizar este tipo de cosas creció considerablemente, fue así como en el ano 2001 se realizo el proceso mas importante en la historia de la evolución de este caso ya que en los juegos de la NFL se implemento dentro de cámaras de vigilancia el cual comparaba con imágenes digitales almacenadas en bases de datos, una vez realizado esto y obtener excelentes resultados el uso de la identificación facial se implemento en múltiples lugares como un medio de seguridad amplio debido a la gran capacidad de respuesta que obtuvo mucho mayor a la de un humano .

4. Metodos:

Ahora bien se se conoce acerca de la historia de este proceso y como funciona hablaremos sobre el método que se aplica en el algoritmo utilizado el cual por desgracia a falta de tiempo aun se encuentra incompleto pero ha dado resultados agradables. en primer instancia al ejecutarse el programa de detección activa la cámara web del ordenador, en este momento el algoritmo empieza a trabajar ya que en primer instancia por medio de la función cvtColor la cual dentro del programa tiene la función de pasar la imagen a escala de grises para que la información sea mucho mas ligera y así sea mas fácil detectar los detalles finalmente se realiza el proceso de detección de rostros por medio de la función detectMultiScale la cual como se menciono detecta las caras en la imagen momentánea, en seguida hacemos un ciclo de las caras obtenidas por la función anterior (parámetro de referencia), el ciclo nos servirá para tener las coordenadas de los rostros que posteriormente con otra función predefinida de OpenCV marca un rectángulo en esa sección, cabe mencionar que este rectángulo debe de recibir el punto x, y y posteriormente el punto x + ancho y punto y + alto, de esa manera el rectángulo se ajusta a lo acorde, sin embargo a la flexibilidad del código puedes modificar estos puntos para obtener resultados diferentes lo cual esta implementado en el programa realizado para mayor facilidad al momento de realizar un recorte de la imagen, ya con ello la desde la imagen se puede obtener un nuevo

histograma pero con los resultados específicos de esa sección y no de toda la imagen, el fin de ello es guardar los datos en la base de datos y con este simple método realizar un proceso inverso para realizar la detección, sin embargo es necesario mencionar que para que esto funcione se debe de efectuar un previo entrenamiento al proceso ya que de lo contrario la base de datos o bien no tendrá información o no tendrá casi información para realizar la búsqueda por lo que puede tener un rendimiento de identificación muy pobre, ahora bien si la comparación tiene un cierto porcentaje de similitud el sistema queda abierto para realizar procesos de cualquier índole.

5. Resultados:

Los resultados hasta el momento no son los esperados ya que no llega hasta el punto final debido a que no fue posible seguir desarrollando el programa por cuestiones de tiempo, sin embargo es posible seguir realizando el desarrollo futuro ya que la verdadera finalidad de realizar esto es el aprendizaje, manejo y entendimiento de este tipo de herramientas muy útiles para medios de seguridad como se había especificado en previas introducciones, ahora si bien el programa no es capaz de realizar mas funciones de las requeridas por lo menos es capaz de realizar una búsqueda de rostros y recortes de imágenes a tal punto que queda alineado a carde al centro del rostro tomando como referencia los puntos mas importantes de la persona frente a la videocámara como es la nariz, los ojos, la boca y un rango de piel necesarios para la elaboración del histograma mencionado en la ultima parte del proceso.

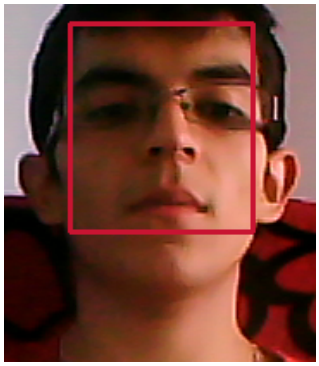

Figura 1: Tomada desde la aplicación.

6. Conclusión:

En teoría no hay nada que lamentar salvo a la falta de resultados del proceso fuera de ello es agradable el haber aprendido todo lo necesario para la realización de este tipo de proyectos, quizás no sea precisamente mi fuerte, pero es bastante interesante lo que se puede lograr no solo con la identificación facial, si no con todo lo que respecta a la visión computacional, considero firmemente que el futuro depende al cien por ciento de esta rama y seria aun mas agradable saber que las personas normales que usan la tecnología que ha costado bastante tiempo y esfuerzo de grandes personas lleguen a valorar correctamente todo lo que realizan por el bien de ellos y den un buen uso a todo aquello realizado, fuera de ello agradezco en lo personal a las personas que siguen trabajando duramente para obtener nuevas tecnologías para el uso humano.

7. Adjunto:

Es conveniente y necesario mencionar la importancia del usa de la documentación api de OpenCV ya que sin ella no hubiese llegado a entender como funciona OpenCV y c++ y también la documentación obtenida de latex para la elaboración del presente documento.

Referencias

[1] Link, *http://docs.opencv.org/modules/refman.html*

[2] Link, *http://ocw.um.es/gat/contenidos/ldaniel/ipu_docs/latex/tema6.html*

[3] Link, *http://www.biometria.gov.ar/metodos-biometricos/facial.aspx*

[4] Link, *http://www.seguridad.unam.mx/documento/?id=17*