ALGORITMO DE GENERACIÓN DE LLAVES DE CIFRADO BASADO EN BIOMETRÍA FACIAL

Juan David Prieto Rodríguez[1]

Fecha de recibido: Julio 23 de 2015 | **Fecha de aprobado:** Septiembre 16 de 2015

Resumen

Actualmente, la tecnología ha evolucionado a tal punto que permite el acceso remoto a sistemas informáticos como plataformas, servicios digitales, redes de datos, servidores, etc. Todo ello a través de sistemas de autenticación que requieren credenciales de acceso. Sin embargo, a pesar de la robustez de los sistemas de autenticación, las contraseñas y llaves de acceso son cada vez más vulnerables, pues la técnica de los atacantes ya no va dirigida a destruir la seguridad de los sistemas, sino más bien a vulnerar la confidencialidad de las llaves. El presente artículo plasma la idea, los fundamentos técnicos y científicos, para el desarrollo de llaves de cifrado de datos basado en técnicas de biometría facial. Lo anterior, con el fin de aportar más seguridad a los sistemas de tecnología de la información, haciendo que las personas sean las portadoras de las contraseñas sin que las conozcan al mismo tiempo.

Palabras clave: biometría, cifrado, correlación, entropía, filtros.

[1] Juan David Prieto Rodríguez. Ingeniero Electrónico y de Telecomunicaciones. Aspirante al título de Especialista en Seguridad de la Información de la Universidad Piloto de Colombia y Docente Investigador en la Fundación para la Educación Superior San Mateo.

GENERATION ALGORITHM ENCRYPTION KEYS BASED ON FACIAL BIOMETRICS

Abstract
Nowadays, technology has evolved to the point that allows remote access to computer systems and platforms, digital services, data networking, servers, etc. All this through authentication systems that require login credentials. However, in spite of the robustness of authentication systems, passwords and access keys are increasingly more vulnerable as the technique of the attackers is no longer directed to destroy the security of systems, but rather to violate the confidentiality of the keys. This article presents the idea, the technical and scientific basis, for the development of data encryption keys based on facial biometrics techniques, in order to provide more security to the information technology systems, by making people the passwords' carrier without knowing them at the same time.

Keywords: biometrics, encryption, correlation, entropy, filters.

ALGORITMO DE GERAÇÃO DE SENHAS CRIPTOGRAFADAS BASEADO EM BIOMETRÍA FACIAL

Resumo
Atualmente a tecnologia tem evoluído a tal ponto que permite o acesso remoto a sistemas informáticos como plataformas, serviços digitais, redes de dados, servidores, etc. Tudo isso através de sistemas de autenticação que requerem credenciais de acesso. No entanto apesar da robustez dos sistemas de autenticação, as senhas e chaves de acesso são a cada vez mais vulneráveis, pois a técnica dos atacantes já não vai dirigida a destruir a segurança dos sistemas, senão mais bem a vulnerar a confidencialidade das senhas. O presente artigo cria a ideia, os fundamentos técnicos e científicos para o desenvolvimento de senhas criptografadas de dados baseado em técnicas de biometria facial, com o fim de contribuir com mais segurança aos sistemas de tecnologia da informação, fazendo que as pessoas sejam as portadoras das senhas sem que ao mesmo tempo as conheçam.

Palavras-chave: biometria, criptografia, correlação, entropia, filtros

INTRODUCCIÓN

Los sistemas de tecnología de la información en la actualidad requieren de más seguridad, pues software especializado y técnicas como la ingeniería social, permiten descubrir claves de acceso a estos sistemas logrando así atentar directamente contra la confidencialidad, integridad y disponibilidad de la información.

Las cifras de delitos informáticos a nivel mundial van en aumento de acuerdo al grado de tecnificación con el que cuenten las empresas y/o personas. Actualmente, el uso de internet es indispensable: el correo electrónico, transacciones bancarias, acceso a las sistemas informáticos de las empresas y consultas de las redes sociales; hace que el trabajo y diferentes aspectos de la vida se realicen de manera más fácil y rápida, dejando expuesto datos personales y contraseñas bancarias si no se tienen medidas de seguridad (Colprensa y Redacción El País, 2012).

Una comunicación segura a través de internet demanda un cifrado del canal de comunicación (Europa Press, 2012). Para ello, existen algoritmos y protocolos seguros que necesitan de llaves para cifrar la información, éstas generalmente las crea el ser humano con niveles bajos de entropía. Lo anterior permite que a través de técnicas como la ingeniería social, que basa su ataque en la manipulación de personas para que realicen actos o entreguen información de manera involuntaria (Imamoto, 2001), una persona sin escrúpulos acceda a la información que se quiere proteger.

Actualmente, se usan sistemas de biometría para control de acceso e identificación en sistemas de seguridad y aquellos que se han desarrollado sobre biometría facial están enfocados en el reconocimiento de criminales. Agencias de seguridad implementan cámaras en aeropuertos, edificios gubernamentales y estaciones de servicio público alrededor del mundo para detectar no solamente, actos delincuenciales sino también para identificarlos con total certeza desde terminales de monitoreo (Biscione, 2005).

Algunas características físicas y determinadas conductas de comportamiento humano son utilizadas como rasgos biométricos, pues poseen propiedades de universalidad, capacidad de distinción, constancia y capacidad de cuantificación, las cuales son variables que se deben tener en cuenta en el desarrollo de aplicaciones biométricas. El rostro humano cumple con cada una de las propiedades, por ejemplo: la forma de los ojos, la nariz y la boca junto con las distancias y ángulos de la cara, satisfacen los principios de distinción y capacidad de cuantificación; ahora bien, respecto a la universalidad, se puede afirmar que todas las personas tienen un rostro (Blázquez, 2013).

El presente trabajo expone la intención de desarrollar algoritmos de cifrado basado en técnicas de biometría facial con objeto de que los individuos porten su llave privada pero sin conocer como es ésta. El algoritmo propuesto se encuentra en una fase de implementación y está sujeto a la exploración de sus vulnerabilidades y la aplicación en los sistemas y tecnologías de la información y las comunicaciones.

MARCO TEÓRICO

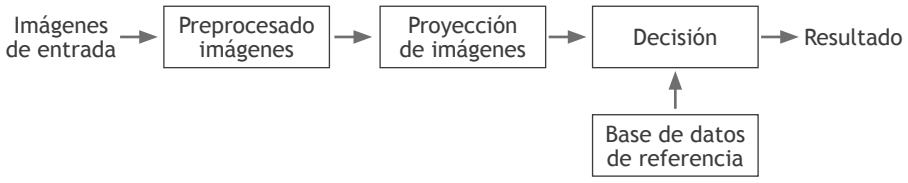
Técnicas de identificación de patrones biométricos faciales

Todo sistema que pretende hacer cualquier tipo de reconocimiento basado en patrones, está enmarcado por unas actividades en secuencia lógica:

1. Entrada de imágenes
2. Procesado de imágenes.
3. Proyección de las imágenes.
4. Sistema de decisión.
5. Base de referencia.
6. Resultado

A continuación se muestra en diagrama de bloque la secuencia de todo sistema de reconocimiento basado en patrones:

Figura 1. Diagrama de bloques de un sistema basado en patrones.



Fuente: Gimeno, R. (2010). *Estudio de Técnica de Reconocimiento Facial*

El reconocimiento facial automático nace en la década de los años 70 con la necesidad de encontrar rasgos singulares humanos adicionales a las huellas dactilares. Por tanto, las técnicas de aquella época consistían en la extracción manual de rasgos y análisis estadístico de las características en máquinas de procesamiento. Dentro de las características que definen los patrones biométricos del rostro humano se encuentran:

- **Técnicas basadas en rasgos locales:** en las cuales se utilizan las características que descubren la forma de la cara y en las que el cerebro humano reconoce los individuos. Estas son la forma de los ojos, nariz, boca, líneas o puntos que permitan medir distancias, áreas o ángulos (Moreno, 2004).

- **Técnicas holísticas:** se encuentran los métodos que describen la imagen que contiene el rostro de una persona, incluido el fondo, evitando así la etapa de segmentación, aunque el mayor espacio ocupado de la imagen debe ser el rostro (Moreno, 2004).

Detección de bordes utilizando técnicas basadas en el gradiente

Un borde en una imagen es considerado como una serie de puntos, los cuales tienen una intensidad determinada en una dirección que cambia drásticamente. Esto se debe a los cambios abruptos de la energía del pixel en las zonas que demarcan un objeto (División de Política y Seguimiento de la Tecnología del UIT-T, 2010). Teniendo en cuenta lo anterior, todo cambio brusco en una señal puede identificarse con una relación de razón de cambio, normalmente conocida como derivada.

En la identificación de cambios abruptos en la energía de un pixel para determinar el borde de algún patrón u objeto se implementa el cálculo de un vector gradiente, el cual permitirá identificar en un punto específico del espacio vectorial de la imagen la dirección en la cual cambiará la intensidad del pixel más rápido; este concepto es análogo al aplicado por físicos cuando desean identificar en qué punto la presión de un gas en un espacio determinado es más grande (Ramos, 2012).

El cálculo del gradiente en una imagen se expresa como la derivada parcial de la función de la imagen respecto a las dos variables dependientes:

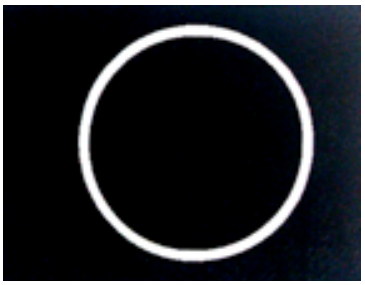
$$\nabla \mathrm{I}(x,y) = \begin{bmatrix} \frac{\partial I}{\partial x}(x,y) \\ \frac{\partial I}{\partial y}(x,y) \end{bmatrix} (1)$$

Para la identificación de la dirección y el punto en el cual la intensidad del pixel cambia se halla el valor del gradiente como se muestra en la ecuación 2:

$$|\nabla \mathrm{I}| = \sqrt{\left(\frac{\partial I}{\partial x}\right)^2 + \left(\frac{\partial I}{\partial y}\right)^2} \quad (2)$$

En términos matemáticos, con la implementación de las derivadas parciales encontramos los máximos y mínimos locales de una función evaluada en punto determinado, lo cual implica la implementación de filtros sobre las imágenes que converjan a espacios vectoriales específicos que permita la identificación de los bordes. La figura 2 muestra el resultado de aplicar la técnica del gradiente sobre una imagen que contiene un círculo.

Figura 2. Imagen con el gradiente hallado



Fuente: Cuevas, E., Pérez, M. y Zaldivar, D. (2010). *Procesamiento Digital de Imágenes con Matlab y Simulink*.

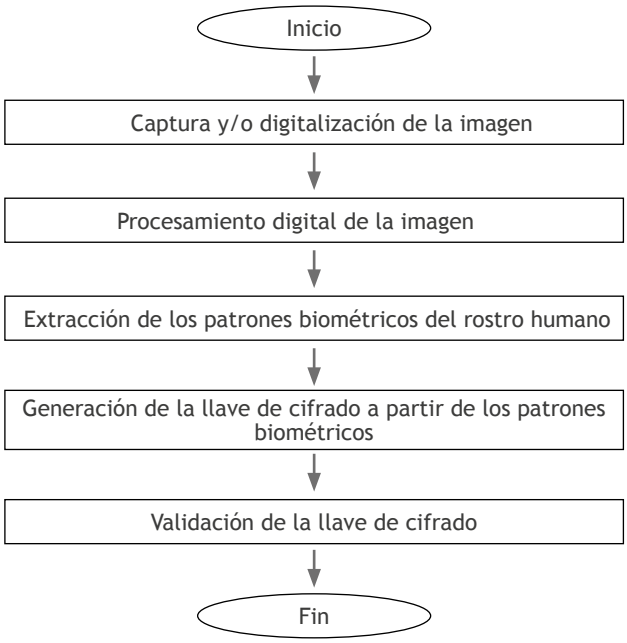
METODOLOGÍA

El rostro humano contiene patrones únicos, los cuales permiten distinguir visualmente la singularidad de cada individuo. Sin embargo, al diseñar un sistema de reconocimiento de patrones biométricos, se debe tener en cuenta que "el reconocimiento consiste en medir, almacenar y comparar características específicas de los individuos" (Moreno, 2004). Así lo afirma Ana Belén Moreno en su tesis doctoral: Reconocimiento facial automático mediante técnicas de visión tridimensional.

El algoritmo desarrollado para la extracción de los rasgos faciales hace uso de las técnicas basadas en rasgos locales y holísticas, con el fin de asegurar una relación entre la llave de cifrado generada y el sujeto de la imagen; esto desde la extracción de las formas de la cara (ojos, nariz, boca, cejas, etc.); por otro lado, se contempla desde la holística un aumento de la entropía de la imagen, contemplando variables adicionales al rostro humano, por ejemplo, brillo, texturas, etc.

El algoritmo planteado presenta hitos importantes en donde es necesario la implementación de diferentes algoritmos con el fin de extraer, procesar y entregar una llave de cifrado a partir de rasgos faciales del rostro humano. En la figura 3 se muestra los Hitos importantes que se tuvieron en cuenta para el desarrollo de algoritmo.

Figura 3. Proceso implementado para el diseño de algoritmo



Fuente: Elaboración propia

Captura y/o digitalización de la imagen

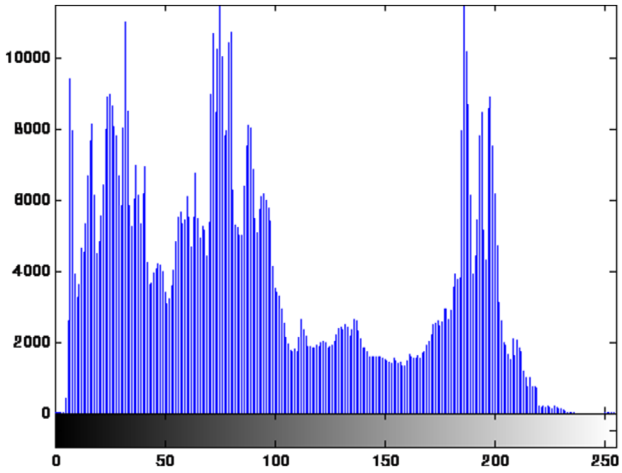
Dentro de las variables que se tienen en cuenta para definir que una imagen ofrezca una mejor resolución para extracción de patrones se encuentran: la iluminación, contraste y dinámica, todas evaluadas y analizadas en el plano "G" con la distribución de los pixeles en un histograma.

Siendo así, es deseable que las imágenes a analizar contengan una adecuada iluminación, lo cual garantiza una identificación de patrones con un alto grado de asertividad. A continuación se hace el análisis de iluminación de la imagen obtenida con la cámara del computador (figura 4 y 5) la cual contiene las siguientes especificaciones: HD Webcam impulsada por EXMOR™ para PC, resolución 1280 x 1024, 1.31 megapíxeles.

Figura 4. Imagen que contiene el rostro humano tomada con la cámara del PC

Fuente: Elaboración propia

Figura 5. Histograma correspondiente a la figura 4.



Fuente: Elaboración propia

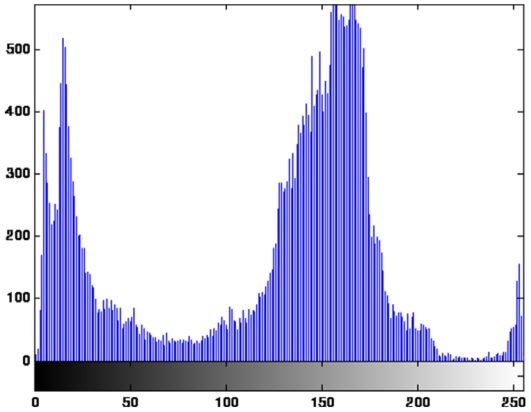
De acuerdo a los resultados arrojados por el histograma se observa que la mayoría de los pixeles se encuentran agrupados entre los valores opacos (0 - 100), por lo tanto, la imagen se encuentra con niveles de iluminación bajos. En cuanto al contraste se encuentra que es normal, pues se busca que existan pixeles distribuidos a lo largo de los posibles valores de intensidad definidos en la escala (es decir, 0 - 255) y respecto a la dinámica, se encuentra que es alta dado que el valor máximo del intervalo de la intensidad supera los 64 niveles.

A continuación se realiza el mismo análisis efectuado anteriormente con las imágenes producto de un estudio fotográfico (ver figuras 6 y 7)

Figura 6. Imagen que contiene el rostro humano procedente de un estudio fotográfico.

Fuente: Elaboración propia

Figura 7. Histograma figura 6.



Fuente: Elaboración propia

De acuerdo al histograma obtenido en la figura 7 se aprecia que la imagen cuenta con niveles adecuados de iluminación pues la mayor agrupación de intensidad de pixeles es superior al valor de 100; también cuenta con un contraste adecuado y una dinámica elevada, lo que indica que se puede realizar un reconocimiento de patrones biométricos.

Procesamiento Digital de la Imagen

Se seleccionó la implementación de los filtros Canny, dado que este método aplica una serie de filtros en direcciones y resoluciones diferentes con el fin de hacer una sumatoria al final del procesamiento para obtener un único resultado combinado, con el fin de minimizar los bordes falsos ocasionados por el ruido propio de la imagen o canal de comunicación si ésta se transmite; una mejor localización de bordes garantiza que el borde localizado sea únicamente un pixel; todo esto basándose en el criterio de la segunda derivada, donde se determina la concavidad de la función, es decir, para este caso en particular, se puede establecer la tendencia de la intensidad de los pixeles.

En procesamiento de imágenes el concepto de la segunda derivada se conoce como operador Laplaciano y es un filtro isotrópico que converge a la siguiente expresión matemática (Ecuación 3):

$$\nabla^2 I(x,y) = \frac{\partial^2 I(x,y)}{\partial x^2} + \frac{\partial^2 I(x,y)}{\partial y^2} \quad (3)$$

Dado que esta técnica se desea implementar para generar una llave de cifrado, es necesario que los filtros converjan en una función lineal, con el único fin de que la llave preserve esta propiedad y no quede expresada en funciones exponenciales, las cuales en pocos cálculos desbordarían la capacidad de procesamiento de los equipos; por tanto el filtro a utilizar como derivada debe ser lineal cumpliendo con las siguientes propiedades:

- Criterio de linealidad respecto a las abscisas (ver ecuación 4)
- Criterio de linealidad respecto a las ordenadas (ver ecuación 5)

$$\frac{\partial^2 I(x,y)}{\partial x^2} = I(x+1,y) - 2I(x,y) + I(x-1,y) \quad (4)$$

$$\frac{\partial^2 I(x,y)}{\partial y^2} = I(x,y+1) - 2I(x,y) + I(x,y-1) \quad (5)$$

Para llevar a cabo la implementación del criterio de la segunda derivada y el Laplaciano se usaron los filtros Canny, logrando así extraer los contornos de los patrones biométricos del rostro como se muestra en la figura 8, donde el resultado son los rasgos singulares del individuo de la figura 6.

Figura 8. Patrones biométricos identificados sobre estudio fotográfico (figura 6) implementado filtros Canny

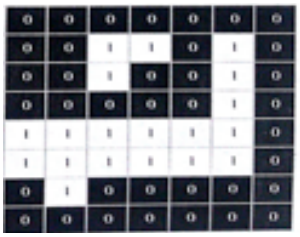
Fuente: Elaboración propia

Por tanto, cabe aclarar que para el desarrollo del algoritmo generador de la llave de cifrado se utilizarán los resultados obtenidos con el filtro Canny, junto con la técnica de adquisición de la imagen por estudio fotográfico, dado que resalta de mejor manera los contornos biométricos de la nariz, ojos, orejas, boca, forma geométrica de la cara y distintivos rasgos particulares del individuo.

Generación de la llave de cifrado a partir de los patrones biométricos

La imagen resultante luego de aplicar lo filtros Canny es una matriz binaria en donde el color negro es la representación de un cero lógico y el blanco por un uno, tal como se muestra en la figura 9.

Figura 9. Imagen binaria obtenida después del filtrado Canny en zona de patrones biométricos

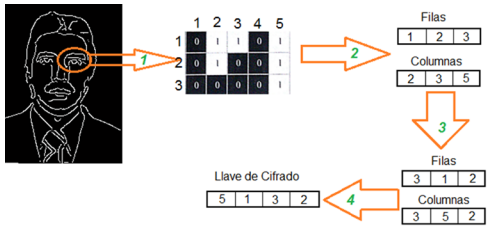


Fuente: Elaboración propia

De acuerdo a lo anterior, los bordes de los patrones biométricos de los rasgos locales y del contorno de las estructuras adicionales de la fotografía se referencian con un uno lógico, dato que es de interés dado que se asocia con la estructura singular del patrón biométrico.

De acuerdo a la premisa anteriormente contextualizada, el algoritmo que se propone (figura10) extrae la posición que un "uno" ocupa en la matriz, almacenando estos datos en un vector de tamaño variable de tal forma que sirve como un contenedor de valores posibles a usar en la llave de cifrado. La figura 10, muestra la secuencia de pasos de cómo el algoritmo extrae los datos sustentados desde la biometría facial.

Figura 10. Esquema de obtención de la llave de cifrado

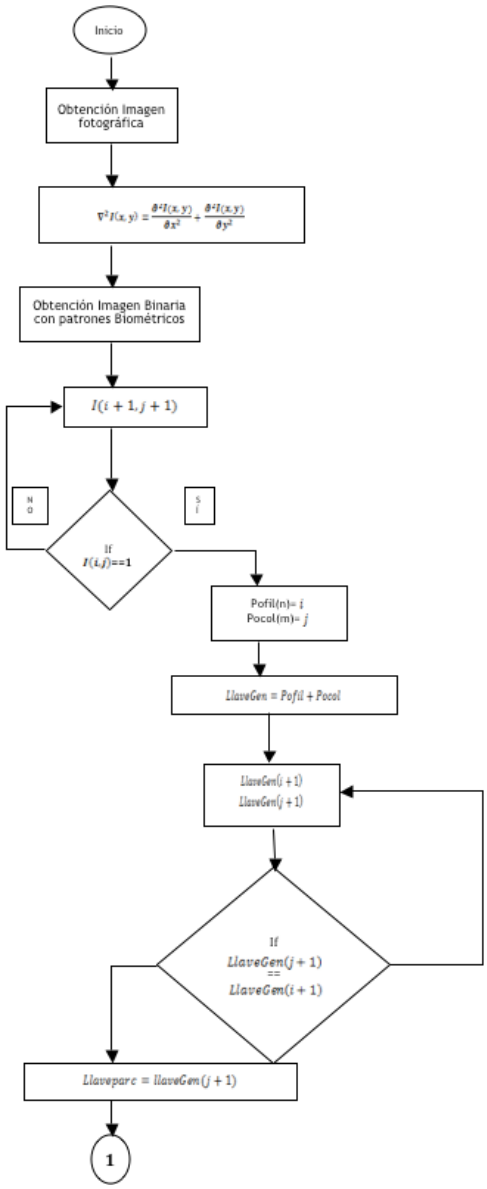


Fuente: Elaboración propia

Es de aclarar que el vector que contiene la llave de cifrado es de posición variable al igual que los vectores en donde se extraen los patrones biométricos. Esta propiedad se determinó dado que los rasgos singulares de un individuo cambian respecto uno a otro, haciendo imposible determinar un tamaño estándar. Se hicieron pruebas con 10 estudios fotográficos con rostros diferentes y el 100 % de los resultados obtenidos arrojo patrones biométricos diferentes, lo que implica un tamaño de vectores distintos.

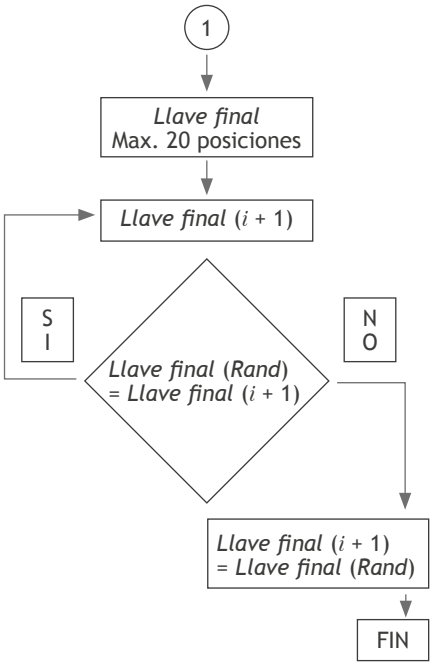
A continuación se muestra el algoritmo propuesto de manera completa y detallada en las figuras 11 y 12.

Figura 11. Algoritmo propuesto que genera la llave de cifrado



Fuente: Elaboración propia

Figura 12. Algoritmo propuesto que genera la llave de cifrado



Fuente: Elaboración propia

CARACTERÍSTICAS QUE TIENE LA LLAVE DE CIFRADO

El algoritmo que plantea este trabajo busca ofrecer una solución a los problemas propios de seguridad que tiene una llave de cifrado de información, haciendo que una persona sea la portadora de su llave sin que la conozca. Así pues, es pertinente estudiar y analizar las propiedades de esta llave, con el fin de establecer ciertas características con las que deba cumplir en el desarrollo de algoritmos similares enmarcados en el mismo contexto, el uso de fuentes naturalmente entrópicas como el rostro humano.

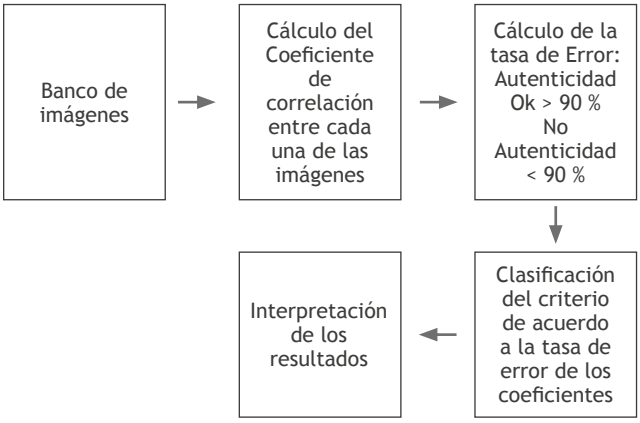
Uno de los principales inconvenientes de hacer uso de estos sistemas, en donde se utiliza alguna parte del cuerpo para proteger información, es precisamente relacionar al individuo con la misma como su legítimo dueño.

La correlación entre señales permite obtener una comparación ellas, entregando una relación de cuanto dista la una de la otra, en un intervalo comprendido entre 0 y 1, siendo 0 totalmente distantes y 1 totalmente similares.

La hipótesis que se quiere someter a prueba consiste en pensar si la correlación entre imágenes, que es una convolución en el dominio del tiempo, analiza los suficientes detalles del rostro humano que permitan garantizar el criterio de autenticidad.

Ahora bien, unos de los retos propuestos en este trabajo es el análisis de un banco de imágenes que contiene el rostro humano y poder asegurar que todos ellos tienen algo en común: el rostro del individuo con el que se generó la llave de cifrado. La figura 13 muestra el método propuesto para determinar el criterio de autenticidad.

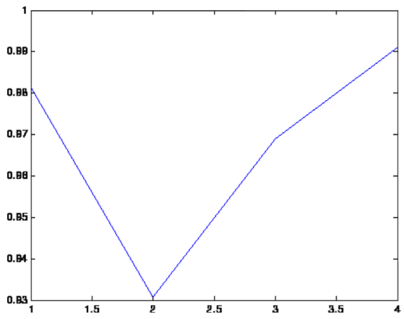
Figura 13. Método propuesto para determinar el criterio de autenticidad



Fuente: Elaboración propia

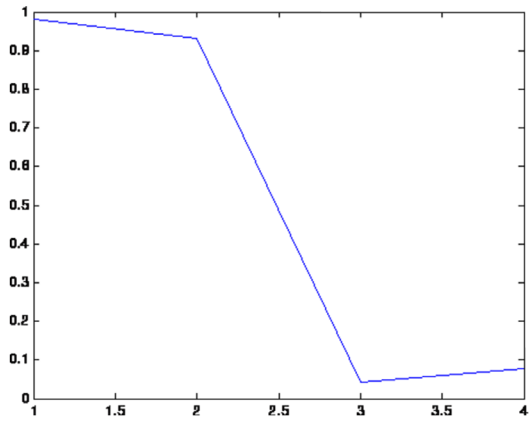
Se definió la escala de aceptación de coeficientes con un valor por encima de 0,90, dado que este dato indica un alto grado de similitud entre las imágenes sometidas a estudio. Las correlaciones que se encuentre por debajo de este umbral se descartan y automáticamente falla el criterio de autenticidad. Las figuras 14 y 15 muestran el comportamiento de las correlaciones realizadas a las imágenes del banco, donde se muestran correlaciones que verifican la autenticidad del individuo (figura 14) y donde se descarta (figura 15).

Figura 14. Comportamiento de las correlaciones exitosas en una prueba



Fuente: Elaboración propia

Figura 15. Comportamiento de las correlaciones fallidas en una prueba



Fuente: Elaboración propia

ANÁLISIS Y PRUEBAS REALIZADAS SOBRE LA LLAVE DE CIFRADO GENERADA A PARTIR DE PATRONES BIOMÉTRICOS FACIALES

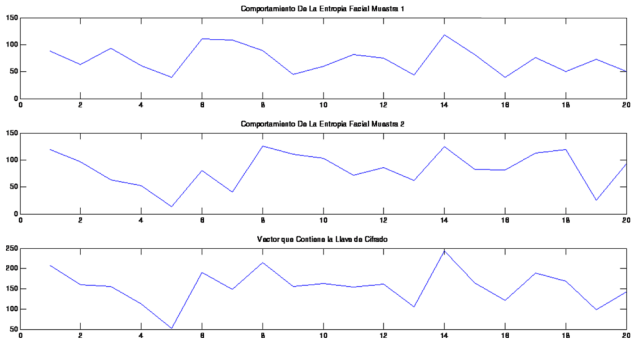
Los ataques por análisis de frecuencias y fuerza bruta son comunes al intentar vulnerar las llaves de cifrado. Siendo así, se expone el comportamiento que tiene en el dominio de la frecuencia la llave de cifrado generada a partir de la biometría facial humana. Sin embargo, realizar un análisis en el dominio de la frecuencia no es suficiente para determinar la seguridad de la llave, es importante el comportamiento de ésta a través del tiempo; técnicas como las transformadas de Fourier y coseno, permiten descomponer toda señal en el tiempo únicamente en diferentes componentes en frecuencias específicas, perdiendo así la capacidad de interpretación de algún fenómeno en el tiempo.

La transformada Wavelet (Ec. 6) es una herramienta matemática capaz de asociar un fenómeno en frecuencia en un tiempo determinado, característica que permite hacer un análisis en dos dimensiones del comportamiento de la llave de cifrado.

$$W_f(s_x,s_y;u,v) = \frac{1}{\sqrt{s_x s_y}} \iint f(x,y)\psi\left(\frac{x-u}{s_x};\frac{y-v}{s_y}\right)dxdy \qquad (6)$$

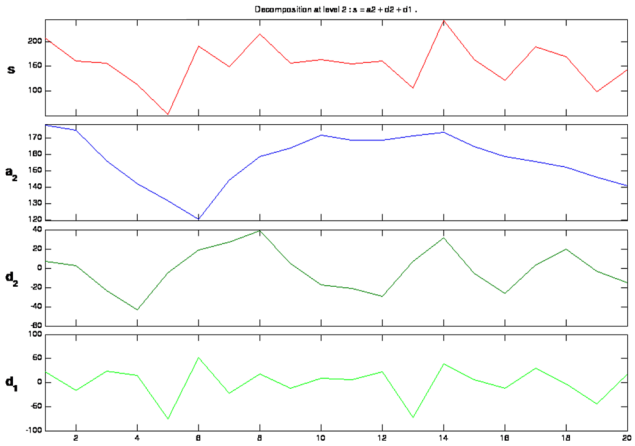
La figura 16 muestra la llave que genera el algoritmo diseñado, mientras que en la figura 17 se observa el comportamiento de ésta en tiempo y frecuencia.

Figura 16. Llave de cifrado obtenida en una iteración del algoritmo diseñado



Fuente: Elaboración propia

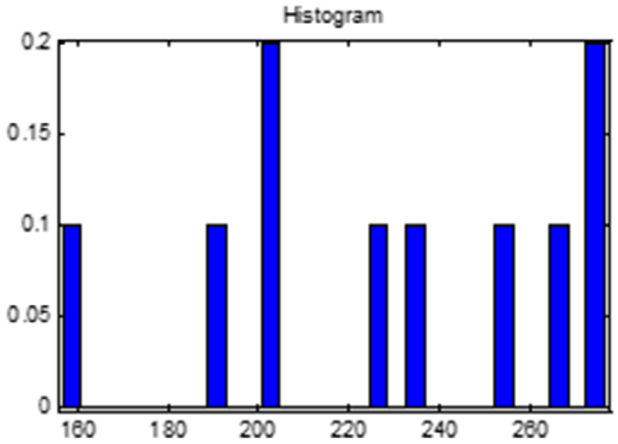
Figura 17. Descomposición Wavelet de la llave de cifrado



Fuente: Elaboración propia

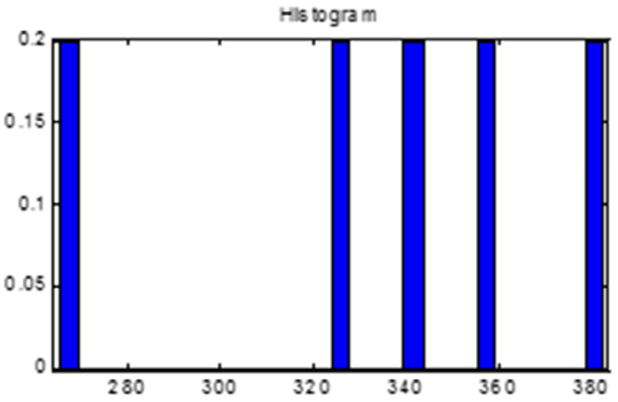
Los histogramas Wavelet muestran la probabilidad de ocurrencia de los símbolos contenidos en el vector que contiene la llave de cifrado. Por ejemplo, el coeficiente d1 (figura 17) muestra que la ocurrencia de los símbolos no superan el 20 % y que estos están distribuidos a partir del valor de 160 aproximadamente (ver figura 18). Ahora bien, respecto al coeficiente de aproximación de d2 (figura 17), los valores de mayor probabilidad de ocurrencias se encuentra en el intervalo de 325 a 380 aproximadamente y NO de manera continua (ver figura 19).

Figura 18. Histograma Wavelet coeficiente d1 (Número de ocurrencias Vs Probabilidad de ocurrencia)



Fuente: Elaboración propia

Figura 19. Histograma Wavelet coeficiente d2



Fuente: Elaboración propia

De acuerdo con lo anterior, la llave generada muestra un nivel de entropía significativo, lo cual reafirma que usar patrones biométricos del rostro humano como fuente generadora es apropiado para el diseño de un sistema de cifrado de información o de certificados digitales.

CONCLUSIONES

Implementar el vector gradiente haciendo uso de la segunda derivada permitió encontrar contornos definidos en los patrones biométricos faciales en las imágenes que contienen rostros humanos. Esto se debe a la información que entrega la segunda derivada que es el criterio de concavidad, pues se determina el comportamiento de la energía en la vecindad de los pixeles.

Para garantizar la autenticidad de la fuente, es decir, la asociación directa que tiene un individuo con una fotografía de su rostro, se implementó la correlación de imágenes, demostrando que esta técnica es apropiada para asociar a nivel de señales las características propias del individuo y la fotografía en comparación con otros rostros humanos. Sin embargo, se debe tener un especial cuidado con variables como la luminosidad de la imagen, que puede afectar el criterio de intensidad, dado que cambia algunos valores de los pixeles, ocasionando un aumento de la distancia entre imágenes con los mismos rostros.

Al tomar la llave generada de 20 muestras aleatorias como una señal continua en el tiempo y someterla a la transformada Wavelet, se descubrió que esta herramienta matemática permite encontrar a través de los coeficientes de aproximación, la probabilidad de aparición de un dato en una llave, que se puede interpretar de dos formas. La primera, que la técnica de análisis por coeficientes Wavelet puede ser implementada en el análisis de seguridad de llaves de cifrado; y la segunda, que la entropía de la señal está directamente asociada con la discontinuidad de ocurrencia de valores en el espectro de la frecuencia de los datos que conforma una llave de cifrado.

Distancias elevadas de ocurrencia de un dato no implican una probabilidad de ocurrencia baja (o alta), de acuerdo a los resultados de análisis de los histogramas de los coeficientes Wavelet.

Cabe mencionar que las pruebas de seguridad aplicadas sobre la llave de cifrado generada por el algoritmo propuesto se aplicaron a criterio del autor. Sin embargo, se sugiere que se apliquen pruebas más especializadas con el fin de determinar vulnerabilidades no halladas en esta primera fase de diseño.

Para concluir, este trabajo presenta un aporte a la seguridad informática, pues actualmente existen muchos sistemas que generan llaves de cifrando con niveles entrópicos altos basados en algoritmos estocásticos. No obstante, existe la limitante de portar la llave, la cual está sujeta a ser robada o perdida. Con el algoritmo se pretende que las personas porten su llave sin que tengan conocimiento de cómo es la misma.

REFERENCIAS

1. Acurio del Pino, S. (2007). *Delitos Informáticos: Generalidades*. Recuperado de http://www.oas.org/juridico/spanish/cyb_edu_delitos_inform.pdf.

2. Biscione, C. (2005). *Ingeniería social para no creyentes*. Recuperado de http://52.1.175.72/portal/sites/all/themes/argo/assets/img/Pagina/IngenieriaSocial_CarlosBiscione.pdf.

3. Blázquez, L., (2013) *Reconocimiento Facila Basado en Puntos Caractéristicos de la Cara en Entornos no controlados*. [Monografía]. Recuperado de http://atvs.ii.uam.es/seminars/PFC_Luis_Blazquez.pdf.

4. Colprensa y Redacción El País. (2012, 31 de Diciembre). En Colombia las cifras de delitos informáticos van en aumento. (Dic. 2012). *El País*. Recuperado de http://www.elpais.com.co/elpais/judicial/noticias/colombia-cifras-delitos-informaticos-van-aumento.

5. Crean En España un Nuevo Sistemas de reconocimiento facial 3D. (2012, 18 de Septiembre). *Europa Press*. Recuperado de http://www.europapress.es/portal/sector/noticia-crean-espana-nuevo-sistema-reconocimiento-facial-3d-20120918092506.html

6. Cuevas, E., Pérez, M. y Zaldivar, D. (2010). *Procesamiento Digital de Imágenes con Matlab y Simulink*. México D.F.: Grupo Alfaomega.

7. División de Política y Seguimiento de la Tecnología del UIT-T. (ene., 2010). *Biometría y normas: un informe Technology Watch*. Recuperado de http://www.itu.int/net/itunews/issues/2010/01/05-es.aspx.

8. Gimeno, R. (2010). *Estudio de Técnica de Reconocimiento Facial*. [Monografía]. Recuperado de http://upcommons.upc.edu/bitstream/handle/2099.1/9782/PFC_RogerGimeno.pdf

9. Imamoto, K. (2001). A design of Diffie-Hellman based key exchange using one-time ID in pre-shared key model. En S. Kawada (Editora), *18th Internacional Conference on Advanced Information Networking and Applications, 2004*. (vol. 1, p. 327-332). Piscataway: The Institute of Electrical and Electronics Engineers, Inc.

10. Moreno, A. (2004). *Reconocimiento Facial Atomático mediante Técnicas de Visión Tridimencional* (Tesis doctoral, Universidad politécnica de Madrid). Recuperada de: http://oa.upm.es/625/1/10200408.pdf.

11. Ramos, F. (2012). Definición Gradiente. En: *Matematicas UNI*. Recuperado de http://matematicasuni.com/definicion-gradiente.