UNIVERSIDAD SAN PEDRO
VICERRECTORADO DE INVESTIGACIÓN
Dirección General de Investigación

FACULTAD DE INGENIERÍA

# SISTEMA DE VIGILANCIA BIOMÉTRICO FACIAL PARA EL CONTROL DELINCUENCIAL EN LA DIVISIÓN POLICIAL CHIMBOTE

Marlene R Paredes Jacinto
Gothy Krishmo Alvarón Fernández
Fernando Vega Huincho
Miguel Arturo Valle Pelaez
Kenedy Johnson Gutierrez Mendoza

Chimbote - Perú
2016

# PALABRAS CLAVE

| | |
|---|---|
| **Tema** | Sistema Biométrico |
| **Especialidad** | Biometría |

| | |
|---|---|
| **Topic** | Biometric system |
| **Specialty** | Biometrics |

## LÍNEA DE INVESTIGACIÓN

**General** : 24 Ciencias de la vida

**Especifica** : 2405 Biometría

# TITULO:

# "SISTEMA DE VIGILANCIA BIOMÉTRICO FACIAL PARA EL CONTROL DELI NCUENCIAL EN LA DIVISIÓN POLICIAL CHIMBOTE"

# RESUMEN

Desde hace tiempo se están utilizando cámaras de seguridad en calles y plazas de ciudades en todo el mundo con el objetivo de identificar amenazas que atenten contra los ciudadanos, con nuestra investigación a lo que ya existe hemos desarrollado un sistema que apoye en la vigilancia e identifique a un requisitoriado.

Para el desarrollo del sistema se analizó diferentes algoritmos de reconocimiento e identificación de rostros y se aplicó la técnica de Análisis por Componentes Principales o alguna derivación de ella: todos ellos utilizan cálculos y métricas que se llevan a cabo en un espacio denominado Euclidiano o $L_2$

Como resultado de la investigación, se obtuvo un interesante sistema de vigilancia biométrico facial para el control delincuencial en la policial judicial de Chimbote, el cual va a permitir integrar a dos institución fundamentales en seguridad ciudadana como son: la Municipalidad Provincial del Santa con la Policía Judicial de Chimbote.

# ABSTRACT

Security cameras have been used on streets and squares around the world for a long time in order to identify threats that threaten citizens. With our investigation of what already exists, we have developed a system that supports surveillance and identifies to a requisitoriado.

For the development of the system different algorithms of recognition and identification of faces were analyzed and the technique of Analysis by Principal Components or some derivation of it was applied: they all use calculations and metrics that are carried out in a space denominated Euclidiano or L2.

As a result of the investigation, an interesting biometric facial surveillance system was obtained for the criminal control in the judicial police of Chimbote, which will allow to integrate two fundamental institutions in citizen security such as: the Santa Provincial Municipality with the Police Judicial of Chimbote.

# INTRODUCCIÓN

Durante el proceso de análisis documentario, se ha encontrado trabajos de investigación relacionado directamente con el tema investigado, de la importancia de un sistema de video vigilancia basado en un sistema biométrico, la cual tiene como propósito la identificación de personas por medio de sus diversas características físicas (voz, huellas digitales, características faciales, etc.):

Amaya y Meneses (2006) El reconocimiento de rostros usando correlación tridimensional (3D) discreta, es una técnica de gran alcance en tareas biométricas del reconocimiento. En este trabajo un procedimiento que usa la información de la gama que captura un sistema de la reconstrucción 3D se propone. La superficie de la cara es 3D-scanned y dispuesto en un correlativo arsenal del volumen y entonces 3D. Los resultados para seis caras tomadas de una base de datos se presentan. Permite desarrollar algoritmos para capturar el rostro para aplicación de la biometría de reconocimientos para construir objetos en 3D.

Capuñay, C.; Liliana, R., Soto, P. (2012). En Lima – Perú, llevaron a cabo la investigación denominada, "Implementación de un Sistema de Videocámaras utilizando Cloud Computing a Nivel Educativo en el distrito de Comas". La vigilancia digital se ha inclinado de forma natural hacia el Protocolo de Internet por tratarse de un medio idóneo para dicha actividad. El protocolo IP se caracteriza por su versatilidad, ya que no tiene limitaciones de magnitud, así como por su robustez y ubicuidad, pues permite utilizar cada terminal de vigilancia como un nexo con el resto de la red.

En tal sentido "sistema de vigilancia biométrico facial para el control delincuencial en la policial judicial de Chimbote", es justificable porque el Sistema de vigilancia biométrico facial, va permitir a la policial judicial de Chimbote disminuir las requisitorias, logrando un beneficio para la población de la ciudad de Chimbote el no contar en su ciudad con tantos delincuentes o personal que evaden la ley.

Desde el punto de vista del conocimiento, el desarrollo del sistema de identificación basado en la biometría actualmente es muy conveniente de usar porque no requieren información adicional de seguridad (tarjetas inteligentes, contraseñas, etc.). Se aplicó algoritmo de búsqueda, comparación y de reconocimiento.

La identificación biométrica es uno de los avances más importantes dentro del control y reconocimiento de personal perteneciente a una entidad sin importar su actividad económica, la biometría es una tecnología basada en el reconocimiento de una característica de seguridad y en el reconocimiento de una característica física e intransferible de las personas.

La detección facial es el proceso de encontrar una cara en imágenes o videos. detección de caras está basado en una función que busca regiones rectangulares dentro de una imagen, regiones que contengan objetos que con una alta probabilidad se parezcan a otros de un conjunto de entrenamiento, devolviendo la región rectangular de la imagen donde se han encontrado. La función escanea varias veces la imagen y con diferentes escalas para encontrar objetos parecidos pero de diferentes tamaños.

Por tanto, para detectar caras, únicamente hay que pasarle a la función el conjunto de caras de entrenamiento con las características deseadas para que las caras detectadas sean parecidas a la base de búsqueda.

El reconocimiento facial es un área de investigación muy activa especializada en cómo reconocer caras en imágenes o vídeos. El reconocimiento facial es el proceso de hacer corresponder la cara detectada a una de las muchas caras conocidas por el sistema de ficheros.

Existen multitud de algoritmos disponibles para llevar a cabo el reconocimiento facial de entre los que se destacan:

- Eigenfaces o método de Análisis de Componentes Principales (PCA).
- Fisherfaces o método de Análisis Lineal Discriminante
- Métodos Kernel
- Métodos de reconocimiento facial 3D
- Método de Gabor Wavelets
- Modelos ocultos de Markov
- Modelos de Apariencia Activa

La criminalidad y violencia en nuestro país, constituyen en la actualidad un problema social de primer orden, que exige la necesidad de implementar medidas concretas para disminuirlas, en particular contra la delincuencia común, cuyos efectos los padece la población en general.

La Región Ancash, principalmente la Provincia del Santa, y el Distrito Capital - Chimbote, no ha sido ajena a estos actos, ya que ha sufrido en mayor dimensión los avatares de la violencia y criminalidad en atentados con consecuencia de muerte de autoridades y personajes de nuestra colectividad.

Para entender la magnitud de la inseguridad ciudadana que estamos viviendo, es necesario comprender que no solo afecta la tranquilidad y seguridad de la población, afecta tanto la inversión local como extranjera. Nadie quiere invertir en ciudades violentas, el turismo también se ve seriamente afectado por este fenómeno.

La División Policial de Chimbote ha proporcionado información relacionada a la incidencia delictiva del distrito de Chimbote describiendo, según consta en los siguientes cuadros:

| | DELITOS | Enero | Febrero | Marzo | Abril | Mayo | Junio | Julio | Agosto | Setiembre | Octubre | TOTAL |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Homicidio | 0 | 2 | 2 | 0 | 0 | 1 | 2 | 1 | 5 | 2 | 17 |
| 2 | Homicidio Calificado | 0 | 3 | 2 | 0 | 2 | 0 | 0 | 0 | 2 | 0 | 9 |
| 3 | Secuestro | 2 | 4 | 0 | 3 | 1 | 0 | 2 | 0 | 1 | 3 | 16 |
| 4 | Aborto | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 5 | Lesiones Graves | 25 | 24 | 19 | 32 | 27 | 23 | 14 | 21 | 14 | 17 | 217 |
| 6 | Violación de la Libertad Personal | 3 | 5 | 6 | 7 | 3 | 3 | 4 | 3 | 7 | 4 | 45 |
| 7 | Violación de la Libertad Sexual | 7 | 1 | 8 | 10 | 10 | 9 | 8 | 5 | 10 | 6 | 84 |
| 8 | Omisión a la asistencia Familiar | 1 | 2 | 0 | 0 | 2 | 14 | 6 | 3 | 0 | 0 | 29 |
| 9 | Delitos Contra la Fe Pública | 0 | 1 | 3 | 2 | 1 | 1 | 3 | 3 | 7 | 0 | 22 |
| 10 | Falsificación de Moneda | 1 | 1 | 0 | 0 | 4 | 1 | 0 | 1 | 0 | 2 | 10 |
| 11 | Hurto Simple y Hurto agravado | 109 | 104 | 108 | 112 | 105 | 93 | 82 | 96 | 125 | 90 | 1024 |
| 12 | Robo Simple y Robo Agravado | 54 | 69 | 63 | 55 | 60 | 52 | 65 | 62 | 63 | 77 | 720 |
| 13 | Abigeato | 2 | 1 | 0 | 1 | 0 | 1 | 2 | 1 | 2 | 0 | 10 |
| 14 | Estafa | 8 | 8 | 12 | 6 | 7 | 0 | 15 | 8 | 3 | 6 | 77 |
| 15 | Apropiación Ilícita | 4 | 3 | 2 | 2 | 2 | 2 | 1 | 0 | 1 | 2 | 19 |
| 16 | Peligro Comun | 28 | 32 | 49 | 66 | 32 | 22 | 43 | 20 | 49 | 15 | 356 |
| 17 | Tráfico ilícito de Drogas | 2 | 1 | 3 | 10 | 6 | 17 | 10 | 7 | 9 | 6 | 81 |
| 18 | Micro comercialización de Drogas | 1 | 6 | 34 | 10 | 18 | 10 | 3 | 8 | 2 | 1 | 102 |
| 19 | Violencia Familiar | 254 | 288 | 278 | 226 | 258 | 248 | 232 | 257 | 204 | 231 | 2440 |
| 20 | Tenencia ilegal de Armas | 8 | 8 | 6 | 4 | 7 | 2 | 8 | 4 | 4 | 1 | 44 |
| 21 | Violencia y Resistencia a la Autoridad | 1 | 5 | 1 | 3 | 1 | 1 | 7 | 2 | 1 | 2 | 23 |
| 22 | Delitos Contra la Persona | 54 | 54 | 63 | 59 | 79 | 48 | 63 | 53 | 69 | 37 | 579 |
| 23 | Extorsión | 15 | 25 | 22 | 25 | 22 | 20 | 26 | 11 | 27 | 10 | 223 |

Figura 01: Estadística Policial sobre Acciones Delictivas

Fuente: DIVPOL Chimbote

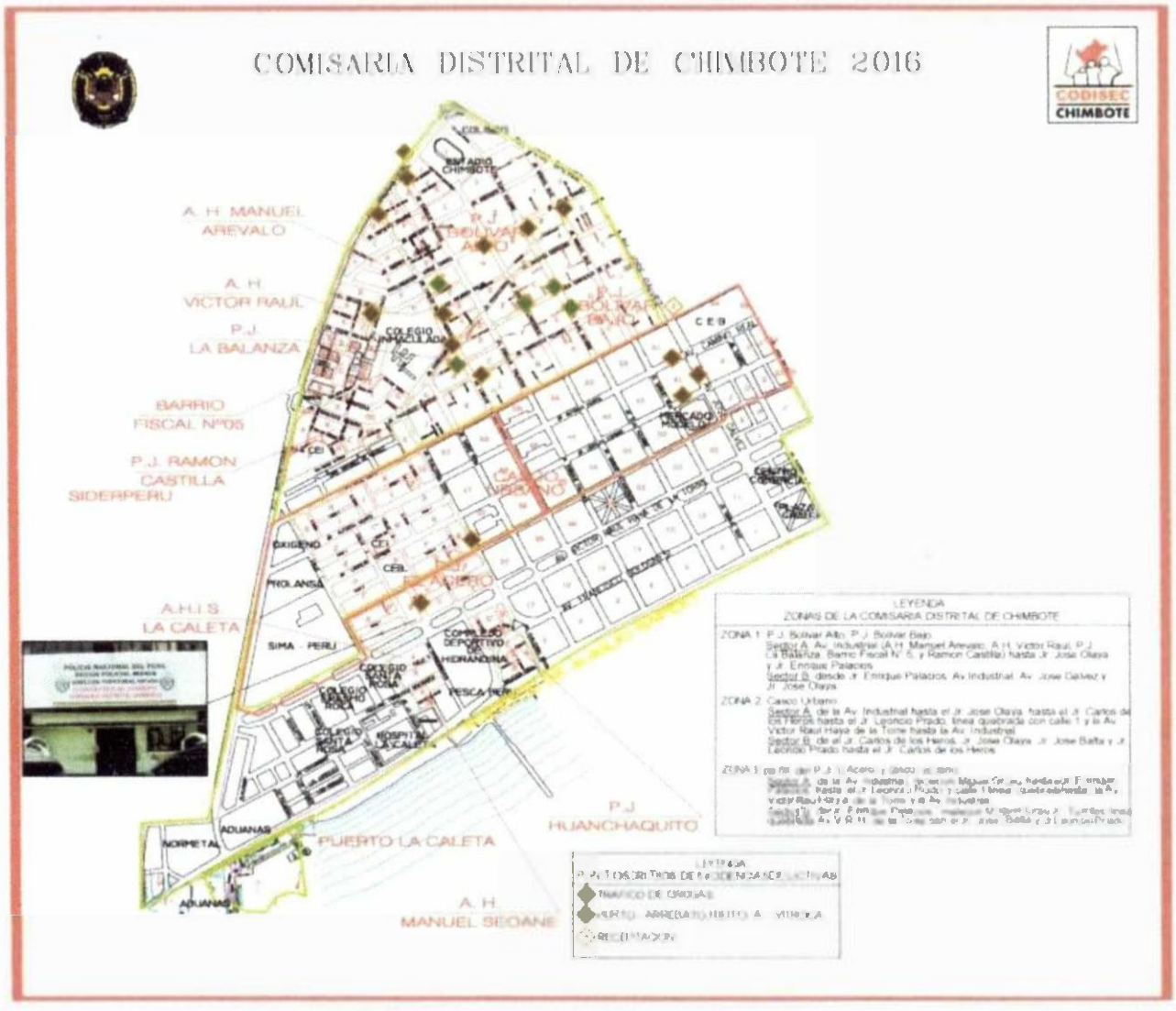


Figura 02: Mapa Delictivo de la Comisaria PNP – Chimbote

Fuente: Plan Distrital de Seguridad Ciudadana 2016

La Municipalidad Distrital de Chimbote cuenta con 64 cámaras de video vigilancia.

Chimbote en Línea, publica que: El jefe de Seguridad Ciudadana de la Municipalidad del Santa, comandante PNP Enrique Larraín Sobrino, dijo que es necesario contar con gran cantidad de cámaras de vigilancia para atender los 100 puntos calientes o lugares donde incurren mayores actos delictivos.

Refirió que si bien la comuna provincial cuenta con 40 cámaras operativas es necesario contar con mayor cantidad de estos equipos para atender en las zonas donde no se cobertura y no hay atención, pese a que son lugares oscuros y donde más se producen robos y actos delincuenciales.

"Nos gustaría contar con estos aparatos en gran parte de la ciudad, pero significa recursos y medios logísticos. Las cámaras operativas que tenemos son insuficientes. Necesitamos contar con un promedio de 100 para hacer una mejor vigilancia"

Figura 03: Centro de monitoreo de las cámaras de vigilancia – Chimbote

Fuente: http://www.chimbotenlinea.com/politica

Ante tal problemática, para tal fin se planteó la siguiente interrogante: ¿Cómo Desarrollar un Sistema biométrico facial para el control delincuencial en la policial judicial de Chimbote?

## RECONOCIMIENTO FACIAL

Los humanos a menudo utilizan los rostros para reconocer individuos y los avances en las capacidades de computación en las últimas décadas, ahora permiten reconocimientos similares en forma automática. Los algoritmos de reconocimiento facial anteriores usaban modelos geométricos simples, pero el proceso de reconocimiento actualmente ha madurado en una Ciencia de Sofisticadas representaciones matemáticas y procesos de coincidencia. Importantes avances e iniciativas en los pasados diez a quince años han propulsado a la tecnología de reconocimiento facial al centro de la atención.

Hay dos enfoques predominantes en el problema de reconocimiento facial:

- El geométrico (basado en rasgos) y
- el fotométrico (basado en lo visual).

Conforme a que el interés investigador en reconocimiento facial continuó, fueron desarrollados muchos algoritmos diferentes, tres de los cuales han sido bien estudiados en la literatura del reconocimiento facial:

- Análisis de componentes principales (Principal Components Analysis, PCA),
- Análisis lineal discriminante (Linear Discriminant Analysis, LDA), y
- Correspondencia entre agrupaciones de grafos elásticos Elastic Bunch Graph Matching, EBGM).

**Análisis de componentes principales (Principal Component Analysis, PCA):** PCA, comúnmente referida al uso de Eigenfaces, es la técnica impulsada por Kirby & Sirivich en 1988. Con PCA, el sondeo y la galería de imágenes deben ser del mismo tamaño y deben ser normalizadas previamente para alinear los ojos y bocas de los sujetos en las imágenes. La aproximación de PCA es luego utilizado para reducir la dimensión de los datos por medio de fundamentos de compresión de datos y revela la más efectiva estructura de baja dimensión de los patrones faciales. Esta reducción en las dimensiones quita información que no es útil [4] y descompone de manera precisa la estructura facial en componentes ortogonales (no correlativos) conocidos como Eigenfaces. Cada imagen facial puede ser representada como una suma ponderada (vector de rasgo) de los eigenfaces, las cuales son almacenadas en un conjunto 1D.

Una imagen de sondeo es comparada con una gallería de imágenes midiendo la distancia entre sus respectivos vectores de rasgos. La aproximación PCA típicamente requiere la cara completa de frente para ser presentada cada vez; de otra forma la imagen dará un resultado de bajo rendimiento. La ventaja primaria de esta técnica es que puede reducir los datos necesarios para identificar el individuo a 1/1000 de los datos presentados.

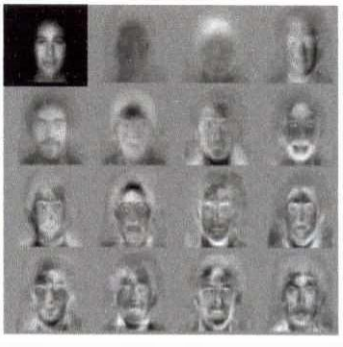

Figura 04: Eigenfaces estándar.

Los vectores de los rasgos son derivados utilizando Eigenfaces

**Análisis lineal discriminante (Linear Discriminant Analysis, LDA):** LDA es una aproximación estadística para clasificar muestras de clases desconocidas basadas en ejemplos de entrenamiento con clases conocidas (Figura 05) Esta técnica tiene la intención de maximizar la varianza entre clases (ej. Entre usuarios) y minimizar la varianza de cada clase (Ej. De cada usuario). En la figura 05 donde cada bloque representa una clase, hay grandes variaciones entre clases, pero pequeñas en cada clase. Cuando se trata con datos faciales de alta dimensión, esta técnica enfrenta el problema de muestras de tamaño pequeño que surge donde hay un número pequeño de ejemplos de entrenamiento comparados a la dimensionalidad del espacio de muestra.

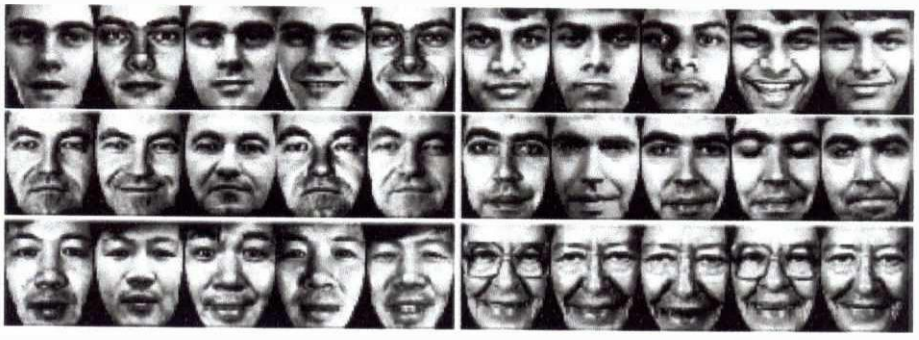

Figura 05: ejemplo de seis clases usando LDA

**Correspondencia entre agrupaciones de grafos elásticos Elastic Bunch Graph Matching, EBGM):** EBGM tiene en cuenta que las imágenes faciales reales tienen muchas características no lineales que no son tratadas en los métodos lineales de análisis discutidos previamente, tales como variaciones en la iluminación (Iluminación de exteriores vs. Interior fluorescente), postura (frontal vs. inclinada) y expresión (sonrisa vs. ceño fruncido).

Una ondeleta de transformación Gabor crea una arquitectura de enlace dinámico que proyecta el rostro sobre la planilla elástica. El Jet Gabor es un nodo en la planilla elástica, manifestado por círculos en la imagen debajo. El cual describe el comportamiento de la imagen alrededor de un píxel. Este es el resultado de una convulsión de la imagen con un filtro Gabor, el cual es usado para detectar formas y extraer características utilizando procesamiento de imagen. (Una convulsión expresa la suma de solapamientos de las funciones en la mezcla de funciones entre si) El reconocimiento está basado en la similitud de la respuesta del filtro Gabor a cada nodo Gabor. Este método biológicamente basado utilizando filtros Gabor es un proceso ejecutado en la corteza visual de los mamíferos más grandes. La dificultad con este método es el requerimiento de la precisa localización

del punto de referencia el cual puede ser algunas veces logrado combinando los métodos PCA y LDA.

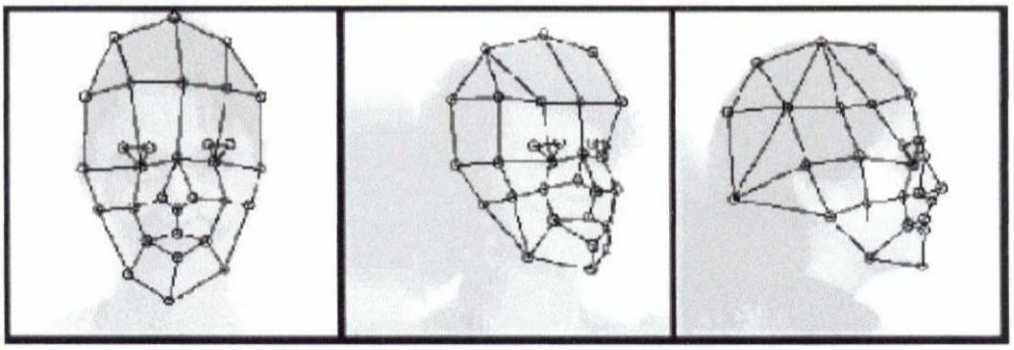

Figura 06: Correspondencia entre agrupaciones de grafos elásticos

El software de reconocimiento facial busca las caras que aparecen en el vídeo en tiempo real en una base de datos con imágenes de caras guardadas previamente. Las caras de la base de datos pueden dividirse en diferentes categorías en función de cuál sea su objetivo (control de acceso, detección de personas VIP o identificación de delincuentes conocidos).Cuando la cámara captura una cara, se realiza la búsqueda en la base de datos en tiempo real y, según el resultado, se permite o deniega el acceso, o se activa una alarma para que las personas responsables del control puedan tomar las medidas adecuadas.

El enfoque de desarrollo en el que se sustenta la presente investigación es: ¿cómo funciona la tecnología de reconocimiento facial y cuáles son los problemas que hay que tener en cuenta?

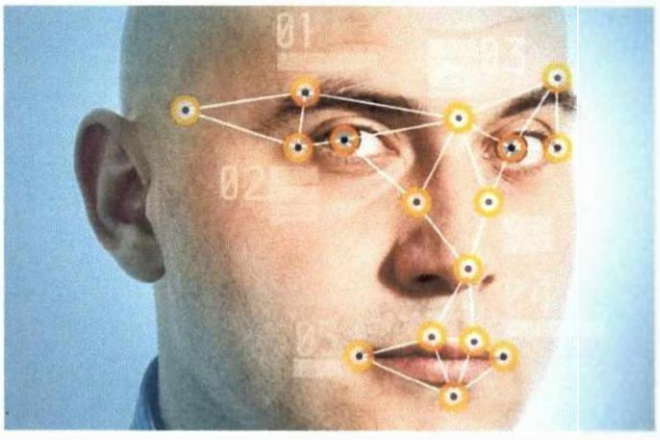

Figura 07: Puntos básicos de reconocimiento facial

Fuente:

La tecnología de reconocimiento facial no es precisamente un fenómeno nuevo, ni tampoco lo es la biometría, a pesar de todos los titulares recientes. Los primeros experimentos con esta tecnología se remontan a la década de **1960**, aunque, en aquel entonces, la investigación para comenzar con su desarrollo se mantuvo en secreto.

Si bien hoy en día la ciencia detrás del *software* es mucho más matemática, automática y cuenta con el respaldo de los potentes equipos sofisticados actuales, los primeros modelos requerían un mayor nivel de intervención humana y, por lo tanto, eran **automatizados** solo en forma parcial.

Además, su desarrollo era mayormente de nicho. Nadie en aquel entonces podría haberse imaginado que, medio siglo después, el *software* de reconocimiento facial tendría tanta difusión, ya sea desde el punto de vista de la **seguridad** (lo utilizan la policía, los profesionales de seguridad y el gobierno), o como un **beneficio** para el consumidor (para reconocer a la gente en una cámara o como medio para proteger un dispositivo con contraseña).

Aunque sin duda ya es algo común, el *software* de reconocimiento facial apenas está comenzando y le falta mucho para llegar a la cima.

Por ejemplo, **Microsoft** está utilizando la tecnología de reconocimiento facial para la autenticación en Windows 10; **Apple** aparentemente está buscando la manera en que los usuarios de iOS puedan compartir automáticamente las fotos con amigos "etiquetados", mientras que tanto **Facebook** como **Google** han estado usando el reconocimiento facial para etiquetar amigos y encontrar fotos de uno mismo.

Por otra parte, unos profesores chinos afirman haber creado el primer cajero automático de reconocimiento facial del mundo, mientras que 30 iglesias en todo el mundo han estado utilizando el *software* "Churchix" para saber **quién va a misa**.

A su vez, unos investigadores en Alemania estuvieron desarrollando una nueva tecnología de reconocimiento facial que puede funcionar en la oscuridad, lo que probablemente sea una señal del **futuro** de esta tecnología y que quizá demuestre que la película Minority Report (2002) de Tom Cruise puede no haber sido tan descabellada después de todo.

La situación actual

Figura 08: Puntos básicos de reconocimiento facial
Fuente:

En los últimos años, el reconocimiento facial se ha empleado más que nada en aeropuertos, en las esquinas y en otras áreas públicas. Su uso en estos casos es relativamente sencillo: una cámara de video recopila las imágenes, que luego se transmiten a un **sistema de vigilancia** monitoreado por un trabajador manual.

El trabajador saca una imagen de un individuo determinado de la transmisión e intenta compararla con las personas presentes en la **base de datos** existente. Mediante el uso de un **algoritmo** informático, el sistema trata de identificar a alguien; para ello mide ciertos rasgos de su rostro, como la distancia entre sus ojos o el ancho de la nariz.

Dicho todo esto, aún hoy en día, el proceso dista mucho de ser simple y directo. Existen muchas cámaras que aún siguen grabando imágenes con una **resolución muy baja**, lo que hace que la identificación sea casi imposible. Además, los propios sistemas de vigilancia por video tienen poca tolerancia a los cambios de luz, las expresiones faciales o las imágenes capturadas en ángulos diferentes.

Sin embargo, algunos avances son positivos. Por ejemplo, el cambio del procesamiento de imágenes de 2D a 3D ayudó a **mejorar la identificación**. Las imágenes ahora son capaces de recopilar una gran cantidad de información adicional basada en **submililitros** (o microondas) para muchos aspectos faciales, desde la estructura ósea hasta las curvas alrededor de la cuenca del ojo, la nariz y

la pera. Esto ayuda a reconstruir la estructura del rostro y, en última instancia, mejora la identificación y la hace más precisa.

Por otro lado, el hecho de que el modelado en 3D tenga **menos limitaciones** en cuanto a la iluminación y los ángulos también es fundamental. Las imágenes se pueden convertir fácilmente de 3D a 2D cuando es necesario, sin perder ningún dato o identificador clave.

En caso de que el reconocimiento facial no funcione, varios fabricantes ya están trabajando en la biometría de la piel para proporcionar más datos que faciliten la identificación. Este método analiza una imagen tomada de un sector de **piel** y la divide en fragmentos más pequeños para poder medirla. El sistema luego puede distinguir las líneas, los poros y la textura real de la piel.

El *sofiware* aparentemente es capaz de identificar las diferencias entre gemelos idénticos, lo que aún no es posible mediante el uso de tecnología de reconocimiento facial por sí sola, aunque también presenta otros problemas como el uso de anteojos y lentes de sol, el cabello sobre la cara, la iluminación y la resolución de la imagen.

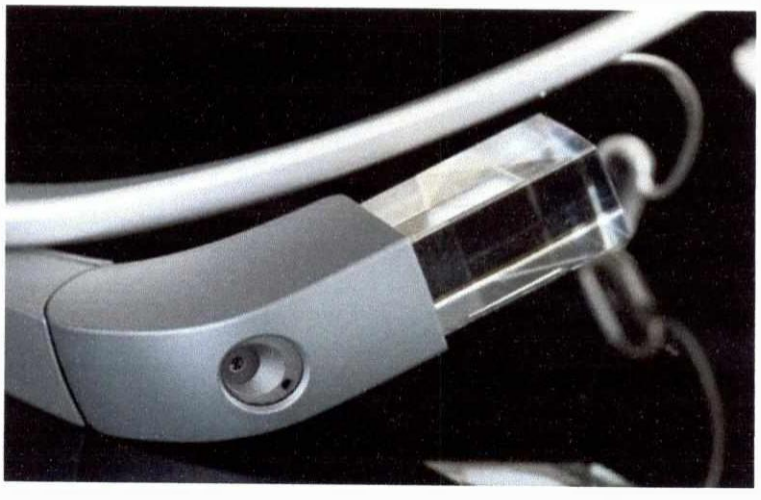

Figura 09: Convertidos de imagenes

Fuente:

Al parecer, el reconocimiento facial se encuentra en un auge inevitable, pero todavía se enfrenta a unos cuantos desafíos. Las **dificultades técnicas** probablemente se vayan disipando a medida que más fabricantes trabajen en esto, aunque la eficacia de identificación es un gran dilema: la BBC recientemente informó que la policía del Reino Unido solo logró identificar a una persona de 4.000 imágenes tomadas de los disturbios de Londres en 2011.

Ahora también existe el problema de la **privacidad**, la seguridad y la transparencia de los datos. Muchas personas consideran que los dispositivos portátiles como Google Glass son una invasión a su privacidad y hay una creciente sospecha de los datos que Google, Facebook o Twitter, entre otros servicios, están recopilando sobre sus usuarios.

Los expertos en seguridad dicen que esto destaca la necesidad de que exista una **mayor transparencia** sobre los datos que se recogen, y sobre la forma en que se almacenan y se protegen. Además, iniciativas como Privacy Visor, los anteojos que evitan el reconocimiento facial, sugieren que los usuarios finales podrían rebelarse contra los gigantes de Internet y el uso que hacen de los datos biométricos si no comienzan a dar este tipo de explicaciones en forma adecuada.

Otros también están empezando a considerar el asunto desde un punto de vista **legal**. Jennifer Lynch, abogada de Electronic Frontier Foundation, un grupo que se ocupa de los derechos a la privacidad, dijo recientemente a Bloomberg: "Los datos de reconocimiento facial se pueden recoger sin el conocimiento de la persona en cuestión. En cambio, es muy difícil que se le pueda tomar una huella digital sin su conocimiento".

**Programación extrema**

Programación extrema de ahora en adelante XP, es una metodología de desarrollo de software ágil, que considera a las personas como un factor decisivo para lograr el éxito de un proyecto. Por ser un proceso ágil tiene como principal característica su adaptación a entornos cambiantes. Esto es posible porque el proceso está diseñado para adaptarse en forma inmediata a los cambios, con bajos costos asociados en cualquier etapa del ciclo de vida. Está diseñada para trabajar en pequeños o medianos equipos de hasta 12 integrantes. Esto fomenta la comunicación e interacción entre sus integrantes, logrando el trabajo en equipo. De esta forma, es posible reducir el costo de transferir información entre los mismos, al tener a todo el equipo compartiendo un mismo lugar de trabajo. El cliente cumple un rol fundamental en XP, dirigiendo el proyecto a lo largo del mismo. Este es quién fija las prioridades, y los programadores desarrollan lo que es necesario para ese momento en particular. En pequeñas iteraciones el sistema va creciendo según los requerimientos solicitados por el cliente, el cual puede observar el avance del proyecto en todo momento (Beck, 2000).


Figura 10. Ciclo de vida de la Programación extrema.
Fuente: http://oness.sourceforge.net/proyecto/html/index.html, ONess,

La metodología XP está compuesta por las siguientes fases:

**a. Fase 1: Planificación del proyecto**

Historias de usuario:

El primer paso de cualquier proyecto que siga la metodología X.P es definir las historias de usuario con el cliente. Las historias de usuario tienen la misma finalidad que los casos de uso pero con algunas diferencias: Constan de 3 ó 4 líneas escritas por el cliente en un lenguaje no técnico sin hacer mucho hincapié en los detalles; no se debe hablar ni de posibles algoritmos para su implementación ni de diseños de base de datos adecuados, etc. Son usadas para estimar tiempos de desarrollo de la parte de la aplicación que describen. También se utilizan en la fase de pruebas, para verificar si el programa cumple con lo que especifica la historia de usuario. Cuando llega la hora de implementar una historia de usuario, el cliente y los desarrolladores se reúnen para concretar y detallar lo que tiene que hacer dicha historia. El tiempo de desarrollo ideal para una historia de usuario es entre 1 y 3 semanas.

La Velocidad del Proyecto: es una medida que representa la rapidez con la que se desarrolla el proyecto; estimarla es muy sencillo, basta con contar el número de historias de usuario que se pueden implementar en una iteración; de esta forma, se sabrá el cupo de historias que se pueden desarrollar en las distintas iteraciones. Usando la velocidad del proyecto controlaremos

que todas las tareas se puedan desarrollar en el tiempo del que dispone la iteración. Programación en Parejas: La metodología X.P. aconseja la programación en parejas pues incrementa la productividad y la calidad del software desarrollado. El trabajo en pareja involucra a dos programadores trabajando en el mismo equipo; mientras uno codifica haciendo hincapié en la calidad de la función o método que está implementando, el otro analiza si ese método o función es adecuado y está bien diseñado. De esta forma se consigue un código y diseño con gran calidad.

**b. Fase 2: Diseño.**

Diseños Simples: La metodología X.P sugiere que hay que conseguir diseños simples y sencillos. Hay que procurar hacerlo todo lo menos complicado posible para conseguir un diseño fácilmente entendible y fácil de implementar, que a la larga costará menos tiempo y esfuerzo desarrollar.

Glosarios de Términos: Usar glosarios de términos y una correcta especificación de los nombres de métodos y clases ayudará a comprender el diseño y facilitará sus posteriores ampliaciones y la reutilización del código.

Riesgos: Si surgen problemas potenciales durante el diseño, X.P sugiere utilizar una pareja de desarrolladores para que investiguen y reduzcan al máximo el riesgo que supone ese problema.

Funcionabilidad extra: Nunca se debe añadir funcionalidad extra al programa aunque se piense que en un futuro será utilizada. Sólo el 10% de la misma es utilizada, lo que implica que el desarrollo de funcionalidad extra es un desperdicio de tiempo y recursos.

Refactorizar: La actividad de refactorizar es mejorar y modificar la estructura y codificación de códigos ya creados sin alterar su funcionalidad. Refactorizar supone revisar de nuevo estos códigos para procurar optimizar su funcionamiento. Es muy común rehusar códigos ya creados que contienen funcionalidades que no serán usadas y diseños obsoletos.

**c. Fase 3: Codificación.**

El cliente es una parte más del equipo de desarrollo; su presencia es indispensable en las distintas fases de X.P. A la hora de codificar una historia de usuario su presencia es aún más

necesaria. No olvidemos que los clientes son los que crean las historias de usuario y negocian los tiempos en los que serán implementadas. Antes del desarrollo de cada historia de usuario el cliente debe especificar detalladamente lo que ésta hará y también tendrá que estar presente cuando se realicen los test que verifiquen que la historia implementada cumple la funcionalidad especificada. La codificación debe hacerse ateniendo a estándares de codificación ya creados. Programar bajo estándares mantiene el código consistente y facilita su comprensión y escalabilidad.

**d. Fase 4: Pruebas.**

Uno de los pilares de la metodología X.Pes el uso de test para comprobar el funcionamiento de los códigos que vayamos implementando. El uso de los test en X.P es el siguiente:

- Se deben crear las aplicaciones que realizarán los test con un entorno de desarrollo específico para test.
- Hay que someter a pruebas las distintas clases del sistema omitiendo los métodos más triviales.
- Se deben crear los test que pasarán los códigos antes de implementarlos; en el apartado anterior se explicó la importancia de crear antes los test que el código.

Un punto importante es crear test que no tengan ninguna dependencia del código que en un futuro evaluará. Como se comentó anteriormente los distintos test se deben subir al repositorio de código acompañados del código que verifican.

Test de aceptación. Los test mencionados anteriormente sirven para evaluar las distintas tareas en las que ha sido dividida una historia de usuario. Al ser las distintas funcionalidades de nuestra aplicación no demasiado extensas, no se harán test que analicen partes de las mismas, sino que las pruebas se realizarán para las funcionalidades generales que debe cumplir el programa especificado en la descripción de requisitos.

En el presente trabajo de investigación se la plantea la hipótesis de carácter descriptivo por lo que la hipótesis se puede no o enunciar.

Para el desarrollo del trabajo de investigación se planteó como objetivo general: Desarrollar un Sistema de vigilancia biométrico facial para el control delincuencial en la policial judicial de Chimbote

Para tal fin se considera los objetivos específicos:

a) Realizar un estudio de los diferentes algoritmos de reconocimiento facial.
b) Determinar los requerimientos y la tecnología a utilizar para el desarrollo del sistema de vigilancia biométrico facial.
c) Construir un sistema de vigilancia biométrico facial haciendo uso de las metodologías XP para el control delincuencial de ciudadanos requisitoriados que evaden la ley en la ciudad de Chimbote.

# METODOLOGÍA DE TRABAJO

La presente investigación en cuanto a los objetivos planteados, se trata de una investigación tecnológica porque busca desarrollar un diseño de un producto software que permita identificar a ciudadanos que han sido sentenciados por un delito y que evaden la ley porque no se presentaron a la lectura de su sentencia, todo ello se realizó haciendo uso de las técnicas y algoritmos de reconocimiento facial del Sistema Biométrico.

El diseño de la Investigación corresponde al no experimental, transaccional porque recopilamos información de los expertos en Sistemas Biométricos específicamente en el facial y contar con información de imágenes de ciudadanos requisitoriados por la policía judicial de Chimbote.

Los métodos y técnicas utilizados fueron los que a continuación se detallan:

- ✓ **Técnica documental:**

  Se analizaron los documentos emitidos por la policía judicial de Chimbote, el registro del sistema de vigilancia de la Municipalidad y del plan local de seguridad ciudadana.

- ✓ **La entrevista:**

  Instrumento que permitió complementar la recolección de información que permitió hacer partícipe a las autoridades y gobernantes como principal fuente de información de la presente investigación al estar haciendo uso de sus funciones como representantes de seguridad ciudadana e identificación de un requisitoriado por parte de la policía judicial

La información recolectada ha sido debidamente seleccionada y tratada en función de los pasos de la metodología de diseño utilizada tal y como es el caso de las fases de identificación de la tarea y que han servido para la fase 2, desarrollo de los prototipos.

# RESULTADOS

De los estudios realizados sobre reconocimiento facial se procedió a la elaboración del algoritmo, el cual consta de cuatro procesos principales:

1. Detección de la cara: detecta que hay una cara en la imagen, sin identificarla. Si se trata de un video, también podemos hacer un seguimiento de la cara. Proporciona la localización y la escala a la que encontramos la cara.
2. Alineación de la cara: localiza las componentes de la cara y, mediante transformaciones geométricas, la normaliza respecto propiedades geométricas, como el tamaño y la pose, y fotometricas, como la iluminación. Para normalizar las imágenes de caras, se pueden seguir diferentes reglas, como la distancia entre las pupilas, la posición de la nariz, o la distancia entre las comisuras de los labios. También se debe definir el tamaño de las imágenes y la gama de colores. Normalmente, para disminuir la carga computacional del sistema, se acostumbra a utilizar imágenes pequeñas en escala de grises. A veces también se realiza una ecualización del histograma.
3. Extracción de características: proporciona información para distinguir entre las caras de diferentes personas según variaciones geométricas o fotométricas.
4. Reconocimiento: el vector de características extraído se compara con los vectores de características extraídos de las caras de la base de datos. Si encuentra uno con un porcentaje elevado de similitud, nos devuelve la identidad de la cara; si no, nos indica que es una cara desconocida.

Los resultados obtenidos dependen de las características extraídas para representar el patrón de la cara y de los métodos de clasificación utilizados para distinguir los rostros, pero para extraer estas características apropiadamente, hace falta localizar y normalizar la cara adecuadamente.

## COMO SE CREAL EL ALGORITMO DE RECONOCIMIENTO FACIAL

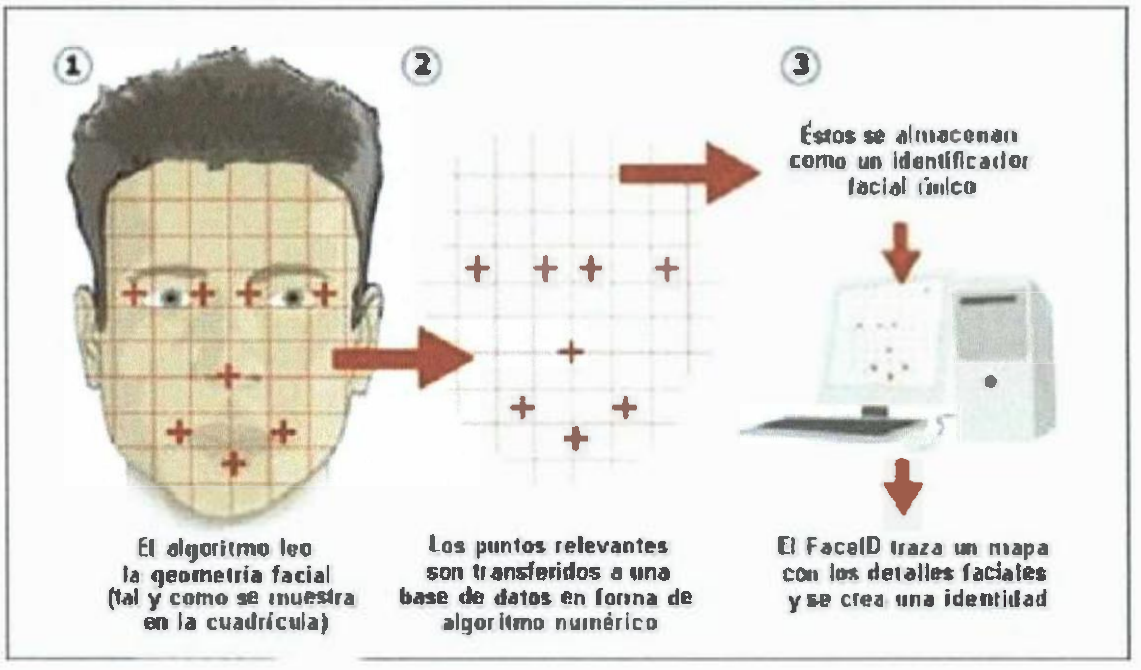


Figura 12: Identificación de los puntos básicos de un rostro

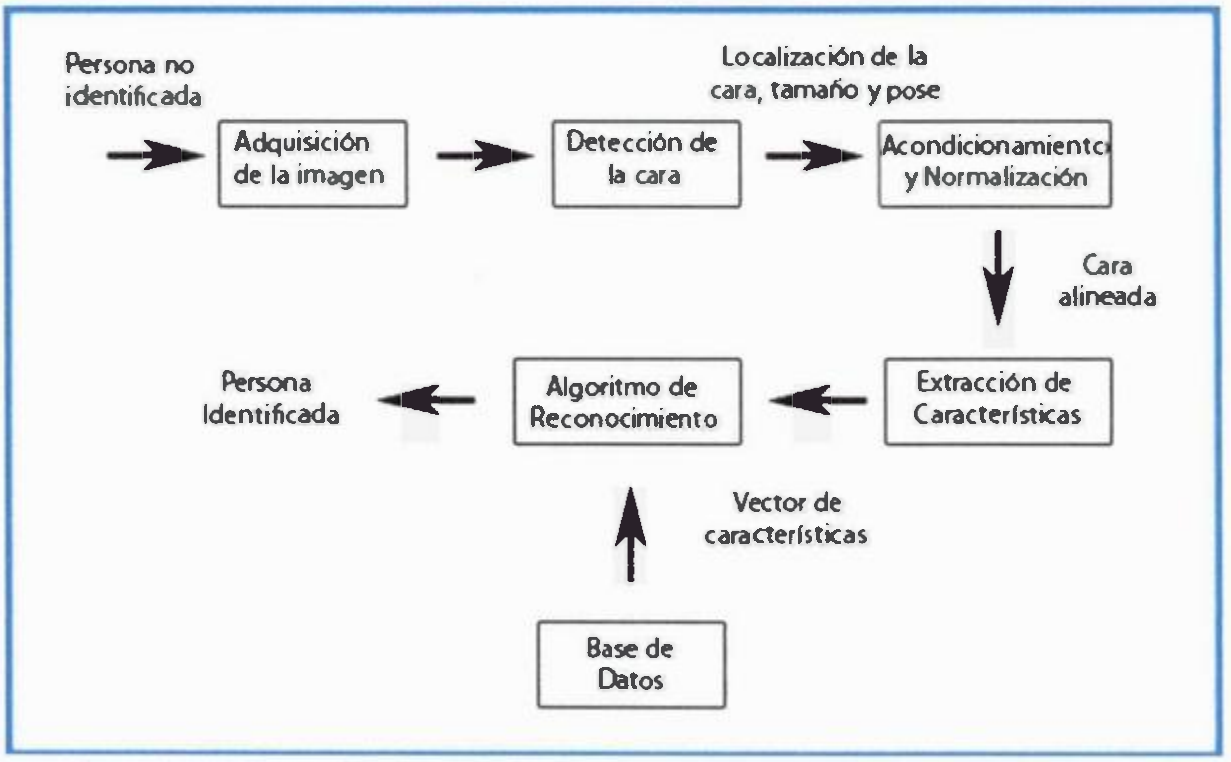


Figura 13: Módulos considerados en el algoritmo

**Sistema Web de reconocimiento facial**

El presente software de reconocimiento facial, para la división policial de Chimbote, tiene su fundamento en el reconocimiento de patrones, esencialmente de utiliza la librería EmguCV, para la creación de estos patrones y realizar el reconocimiento facial.

El sistema web de reconocimiento tiene el siguiente funcionamiento:

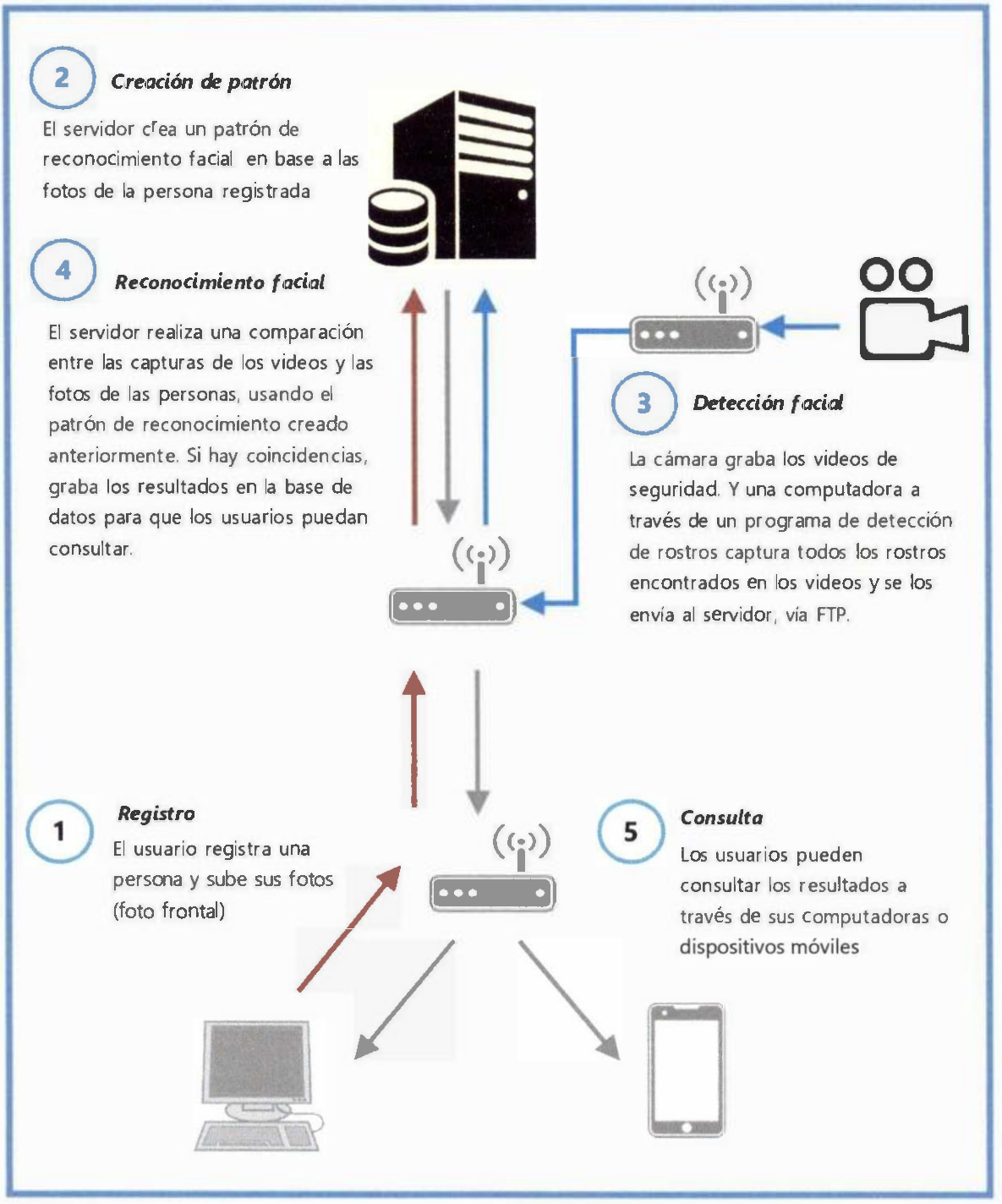


Figura 14: Esquema de funcionamiento del sistema de reconocimiento facial
Fuente: Elaboración propia

**Descripción:**

- **Los puntos 1 y 5,** son funcionalidades del sistema web, consistente en el registro búsquedas y consulta de los resultados del reconocimiento facial.
- **El punto 3,** consiste en una aplicación de escritorio que se ejecuta como un proceso en una computadora conectada a la cámara y se encarga de la detección facial, para capturar los rostros presentes en los videos para enviarlos al servidor.
- **El punto 2 y 4,** consiste en una aplicación de escritorio que se ejecuta como un proceso del lado del servidor, y se encarga del entrenamiento del patrón facial el cual se guarda como un archivo XML dentro del servidor. También se encarga del reconocimiento facial y de guardar los resultados en la base de datos.

**Detalles técnicos:**

- Las imágenes de los rostros tanto de las fotos como de las capturas de las cámaras deben estar en escala de grises, todas deben ser del mismo tamaño, y tener el mismo alto y ancho (forma cuadrada). El lado de la foto debe tener una longitud potencia de 2, aquí se ha utilizado el tamaño 256px por lado ($2^8$).
- El sistema está construido en el lenguaje de programación Visual C#, y utiliza una base de datos en SQL Server.
- Se utiliza el archivo entrenado XML haarcascade_frontalface.xml, para la detección facial.
- Se utiliza el algoritmo de reconocimiento EigenFaces para el entrenamiento y reconocimiento facial.

**Interfaz web que pueden utilizar los usuarios de la división policial:**

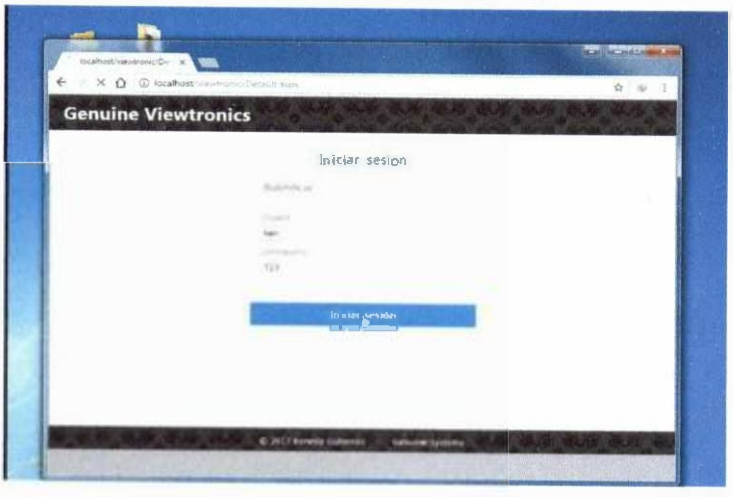


Figura 25: Interfaz de acceso al sistema web
Fuente: Elaboración propia


Figura 36: Interfaz con opciones del sistema web
Fuente: Elaboración propia

## A. Búsquedas

Ejemplo de registro de una persona requisitoriada: se ingresan sus fotos y el sistema automáticamente detecta los rostros (formato escala de grises 256x256) y se las envía al servidor para ser procesadas por el servidor:

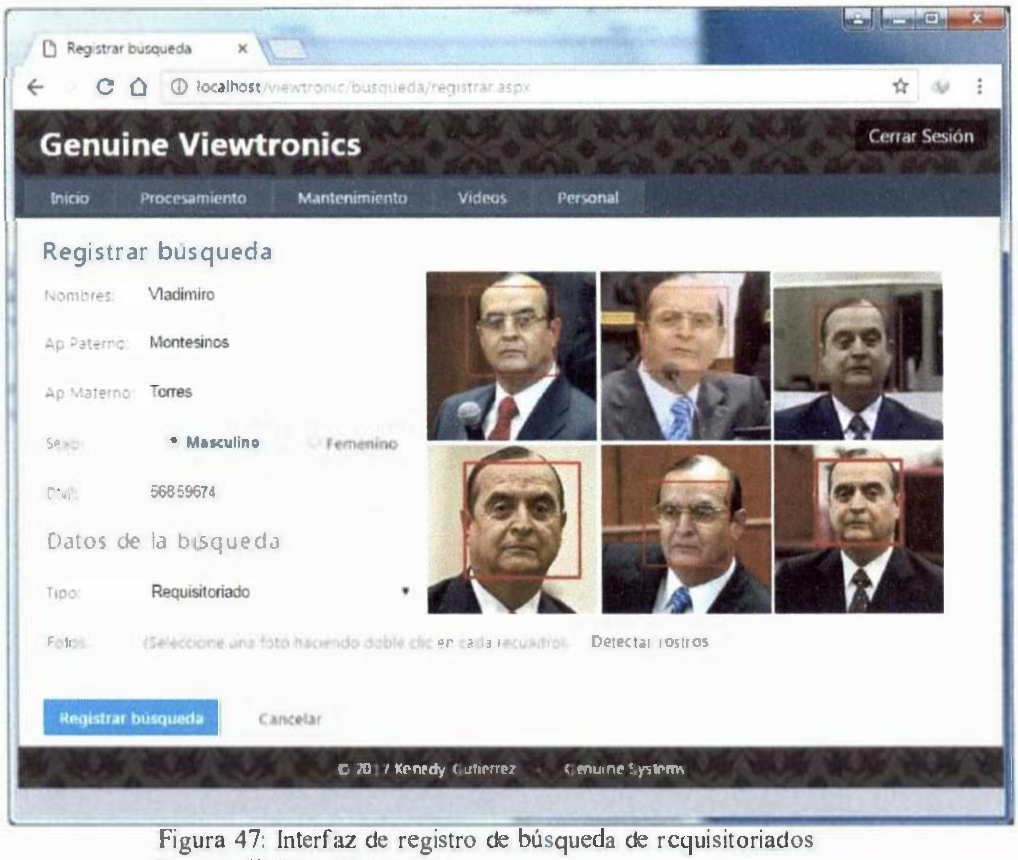


Figura 47: Interfaz de registro de búsqueda de requisitoriados
Fuente: Elaboración propia

## B. Consulta de resultados

En la siguiente pantalla se puede consultar los resultados de la búsqueda, se puede visualizar: la foto capturada de la persona en la cámara de vigilancia, el código de la cámara, la fecha de captura, la diferencia de similitud con la foto de la persona buscada, y el número de la foto (número de frame en el video).

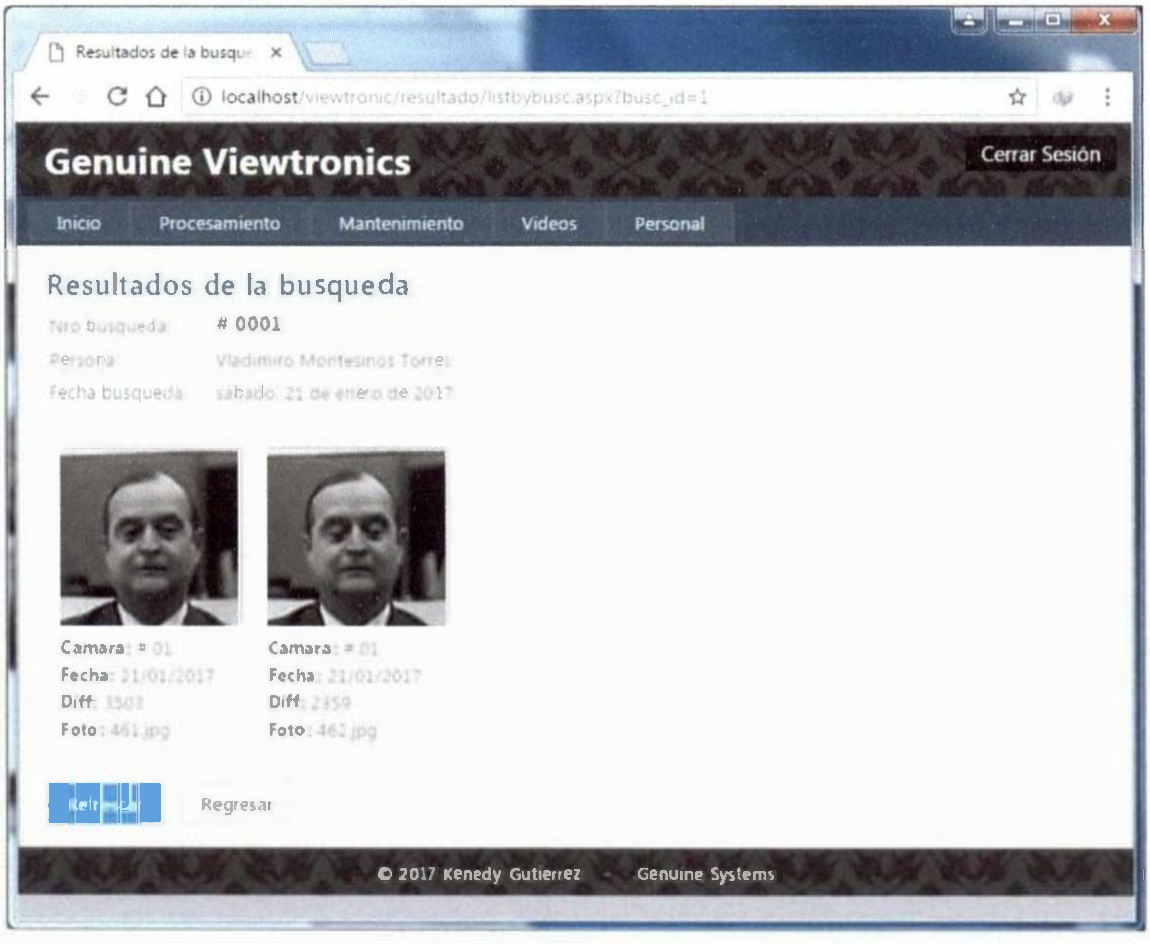


Figura 58: Interfaz de resultado d búsqueda de un requisitoriado
Fuente: Elaboración propia

# ANÁLISIS Y DISCUSIÓN

Diversos estudios de investigadores en materia de seguridad ciudadana a nivel mundial y con el desarrolló en los sistema biométricos permite un aporte con la aplicación de la informática en dar solución a la identificación de ciudadanos que evaden la a ley. En tal sentido de los antecedentes de:

Amaya y Meneses (2006) El reconocimiento de rostros usando correlación tridimensional (3D) discreta, es una técnica de gran alcance en tareas biométricas del reconocimiento. En este trabajo un procedimiento que usa la información de la gama que captura un sistema de la reconstrucción 3D se propone. La superficie de la cara es 3D-scanned y dispuesto en un correlativo arsenal del volumen y entonces 3D. Los resultados para seis caras tomadas de una base de datos se presentan. Permite desarrollar algoritmos para capturar el rostro para aplicación de la biometría de reconocimientos para construir objetos en 3D.

En relación a la investigación de Capuñay, C., Liliana, R., Soto, P. (2012). En Lima – Perú, llevaron a cabo la investigación denominada, "Implementación de un Sistema de Videocámaras utilizando Cloud Computing a Nivel Educativo en el distrito de Comas". La vigilancia digital se ha inclinado de forma natural hacia el Protocolo de Internet por tratarse de un medio idóneo para dicha actividad. El protocolo IP se caracteriza por su versatilidad, ya que no tiene limitaciones de magnitud, así como por su robustez y ubicuidad, pues permite utilizar cada terminal de vigilancia como un nexo con el resto de la red. El sistema desarrollado fue utilizando El Cloud Computing o Computación en la Nube que es un nuevo modelo de computación en el que los servicios informáticos, como correo electrónico, aplicaciones, almacenamiento de archivos y sistemas de gestión, son brindados a través de Internet. En otras palabras, gracias al Cloud Computing los recursos informáticos que se desarrollen están disponibles en cualquier dispositivo con conexión a internet, todos los días, las 24 horas desde nuestros datacenters o centros de computación.

# CONCLUSIONES Y RECOMENDACIONES

Como resultado del desarrollo de los objetivos se ha llegado a las siguientes conclusiones

a) Con los estudios realizados de los diferentes algoritmos de reconocimiento facial a facilito la tarea de determinar los módulos que se planteó en el algoritmo de reconocimiento e identificación de un ciudadano requisitoriado.

b) Se ha logrado determinar los requerimientos funcionales que debe cumplir con el sistema el cual tiene como propósito para identificar personas con requisitoria en la ciudad de Chimbote.

c) Utilizando las metodologías XP influyo positivamente en la construcción del sistema biométrico facial para el control delincuencial en la policial judicial de Chimbote e.

Según nuestras conclusiones podemos recomendar lo siguiente:

a) Se recomienda que las dos instituciones pilares de la seguridad ciudadana trabajen en equipo como son la Policía Judicial y la Municipalidad.
La municipalidad compartiendo los equipos de monitoreo con cámaras de vigilancia.
La Policía Judicial, permitiendo el acceso a la imágenes de la personas requisitoriados.

b) Se deberá capacitar a cada uno de los usuarios finales del sistema para que se encarguen periódicamente realizar verificaciones del funcionamiento.

c) Se debe realizar evaluaciones periódicas de los puntos de riesgos para mejorar las funciones de monitoreo del sistema.

d) Se puede dar uso también para buscar a personas desaparecidas.

# REFERENCIAS BIBLIOGRÁFICAS

Roger Gimeno, Estudio De Técnicas De Reconocimiento Facial. Tesis (Magíster en Ciencias). Barcelona, España. Universidad de Cataluña, Departamento de Señales y Comunicaciones, 2010. 86 h.

Últimos Avances en Biometría (2011) [En línea] http://papeldigital.info/eespecialesal/index.html?2011082201# [consulta: enero 2016].

Reconocimiento facial en Seguridad [En línea] <http://www.csospain.es/El-FBI-invierte-1.000-millones-en-un-sistema-de-reconocimien/seccion-actualidad/noticia-125601> [Consulta: enero 2016]

Biometría Tu Eres la Llave (2010) [En línea] <http://www.gigabytes.cl/biometria-tu-eres-la-llave.php>. Revista digital de tecnología. [Consulta: agosto 2016]