

# SISTEMA DE VIGILANCIA MEDIANTE CÁMARAS IP CON UN SOFTWARE DE DETECCIÓN DE ROSTRO

## SURVEILLANCE SYSTEM USING IP CAMERAS WITH FACE DETECTION SOFTWARE

Gema Victoria Zambrano Zambrano

Carrera Informática, Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, Campus Politécnico sitio El Limón, Calcuta, Manabí, Ecuador

Contacto: vicky\_victoriazam@hotmail.com

### RESUMEN

Esta investigación tuvo como objetivo la implementación de un sistema de vigilancia con la alternativa de un software de reconocimiento facial, desarrollado mediante el comportamiento de los algoritmos de visión por computador, este trabajo se realizó en la Capitanía del Puerto de Manta donde se manipula equipos de elevado valor tanto económico como operativo. El sistema propuesto se desarrolló mediante códigos empleados en el lenguaje de programación de Java y Eclipse como entorno de desarrollo con ayuda de las librerías opencv y javacv, el cual fue diseñado para ser monitoreado por las cámaras de seguridad Trendnet TV-IP551W. Los resultados muestran que el sistema es una aplicación útil y de fácil manipulación que permite controlar e identificar a las personas que ingresan a una empresa, detectando si realizó algún tipo de actividad que ponga en riesgo el funcionamiento de ésta.

**Palabras clave:** Seguridad informática, reconocimiento facial, algoritmos de reconocimientos.

### ABSTRACT

This research aimed to implement a monitoring system with a facial recognition software, developed through the behavior of computer vision algorithms, this work was performed at the Port Authority of Manta where economic and operational valuable equipment are handled. The proposed system was developed through Java and Eclipse programming language as the development environment with the help of opencv and javacv libraries, which was designed to be monitored by Trendnet TV-IP551W security cameras. The results show that the system is a useful and easy to handle application that allows to control and identify people entering the monitored places, detecting potential dangers, which could act in breach of them.

**Keywords:** Computer Security, facial recognition, recognition algorithms.

---

**Recibido:** 22 de Enero del 2014  
**Aceptado:** 17 de Mayo del 2014  
**ESPAMCIENCIA** 5(1): 47-52/2014

## INTRODUCCIÓN

La vigilancia siempre ha sido una prioridad para los gobiernos y autoridades locales, a todo nivel, esto abarca el control de tráfico y la supervisión de las grandes operaciones de seguridad en caso de eventos excepcionales (Trujillo, 2009). Debido a los ataques a la seguridad, los sistemas de monitoreo están sujetos a un creciente análisis, por la información que pueden captar y por la manera de facilitar una reacción veloz y eficaz a los equipos de seguridad (Morales, 2008).

La información es una ventaja estratégica que se convierte en algo atractivo para la frecuencia de los ataques a los activos de una organización. Esto conduce a que las organizaciones empiecen a incorporar prácticas seguras de protección de la información, aspecto que requiere de tiempo y compromiso (Engel *et al.*, 2012).

En las organizaciones se requiere gestionar la seguridad informática para asegurar un entorno informático institucional, para ello es necesario emplear dispositivos reguladores de las funciones y actividades desarrolladas por el personal de la institución; ya que permiten asegurar la información en los sistemas garantizando proteger la red, siempre que haya una persona-física que administre los sistemas, la cual debe ser capaz de analizar situaciones futuras y tomar decisiones (Villegas *et al.*, 2011).

En la actualidad, los escenarios donde los seres humanos interactúan, son del tipo inteligente generados por las nuevas tecnologías de información, debido a que su capacidad para la interconexión posibilita innumerables relaciones entre los diferentes dominios, elementos y agentes de tales actividades (Camacho *et al.*, 2009).

Según Catania (2008) afrontar este problema es que en los últimos años han surgido propuestas para la aplicación de técnicas de inteligencia artificial en el ámbito de la seguridad informática, presentando propuestas de algoritmos genéticos para el reconocimiento facial, como punto de partida para abordar un problema de mayor amplitud como lo es la detección de intrusos. Para Blázquez (2013), los algoritmos de reconocimiento de imágenes son ampliamente utilizados en aplicaciones de visión por computador. Y durante los últimos años ha existido un creciente interés en el enfoque basado en la descripción de un objeto, utilizando descriptores locales (Yasir, 2012).

El presente trabajo tuvo como objetivo la implementación de un sistema de vigilancia con la alternativa de un software de reconocimiento facial, desarrollado median-

te el comportamiento de los algoritmos de visión por computador, los cuales se enfocan en la detección del rostro humano.

## MATERIALES Y MÉTODOS

La ejecución se realizó mediante el método informático ciclo en v y las medidas técnicas de ITIL, de los cuales se lleva las siguientes fases:

### Fase de especificaciones

Esta fase detalla el análisis de procedimientos que se realizan dentro de una oficina iniciando como punto de partida los requisitos del sistema de vigilancia, mediante una entrevista a su personal donde se pudo verificar que el 80% de los trabajadores estuvieron conformes con el sistema implementado mientras el 20% presentaron disconformidad (Figura 1).

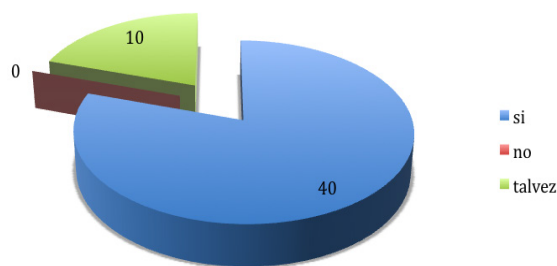
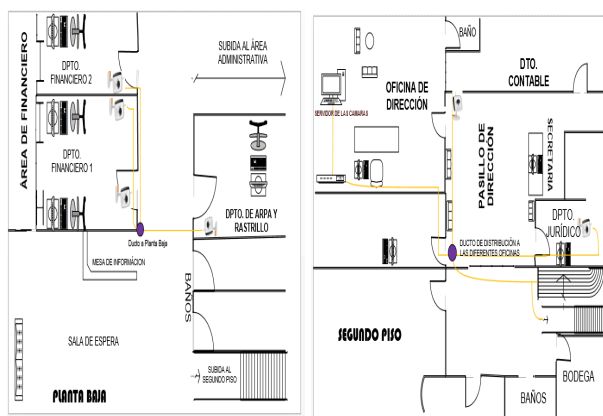


Figura 1. Tabulación de la acogida del sistema mediante la encuesta realizada.

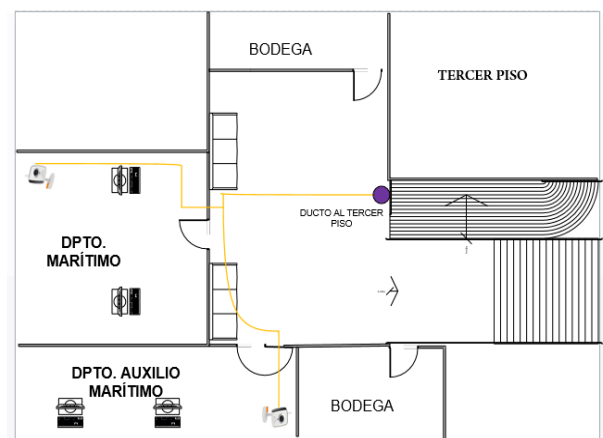
### Fase de diseño de alto nivel y de detalle

Mediante esta fase se realizó el boceto de la ubicación de las cámaras, diseñado en *visio professional* 2013, analizando las posibles interferencias que puedan ocurrir en base a su mala ubicación.

El sistema propuesto parte en las oficinas de la Capitanía del Puerto de Manta, que consta de tres pisos con departamentos a los cuales se les implementó las cámaras de vigilancia trendnet TV-IP551W. Situando el servidor en el segundo piso en la oficina de dirección y así mismo los puntos de red, el patch panel; empezando la distribución de cables hacia los departamentos financiero uno y dos, arpa y rastrillo, jurídico, marítimo, personal marítimo y pasillo de dirección. Dichas instalaciones internas fueron cubiertas con canaletas (Figura 2 y 3).



**Figura 2.** Ubicación de las cámaras en la planta baja y segundo piso del edificio de la Capitanía del Puerto de Manta.



**Figura 3.** Ubicación de las cámaras en el tercer piso del edificio de la Capitanía del Puerto de Manta.

De acuerdo al diseño estructurado, en la instalación del sistema de vigilancia fue necesario adquirir un switch de 16 puertos, herramientas de ferretería, canaletas, patch cord, cable UTP cat 5e, Conectores RJ45, 8 cámaras IP Trendnet TV-IP551W; además de una computadora de escritorio con procesador core i7, 4 Gb en RAM, disco duro de 1 Tb y una tarjeta de video.

## Fase de implementación

Para la parte de implementación se trabajó de dos maneras: la instalación de las cámaras, iniciando con la ubicación de canaletas y la postura de cable UTP cat 5e cerrando las coberturas de las mismas, continuando el recorrido con el ponchado de los cables y de acuerdo al estándar de red 568 B, se ubicaron las cámaras Trendnet TV-IP551W tomando en cuenta el ángulo que se deseaba visualizar o capturar. Por último se procedió a la instalación y configuración del sistema de detección de rostro

sobre las cámaras con el servidor para establecer comunicación entre ellos.

## Fases del test unitario, de integración y operacional

Para verificar si las cámaras estaban ubicadas en puntos claves se realizaron pruebas de video durante unos días; también se realizó ping a los dispositivos para concretar que los equipos se encuentren conectados con el servidor.

Además, para una verificación exhaustiva era necesario ver el funcionamiento de los módulos del software, debido a que la existencia de imágenes dentro de la base de datos pueden robustecer las transformaciones de las imágenes; estas mejoras se consiguen mediante la reducción de la dimensionalidad y complejidad en el cálculo de los vectores del algoritmo de entrenamiento quien inicia el proceso para posteriormente acceder al algoritmo de reconocimiento, logrando que los datos se calculen con precisión en el tiempo requerido.

Las funcionalidades del software son, no solo conocer en todo momento la cantidad de personas que se encuentran dentro de la zona vigilada, sino que por medio de esta aplicación se pueda conocer su identidad.

Para el esquema de detección del software se emplearon las librerías de visión artificial que son opencv y javacv, que funcionan mediante un código entrenado y librerías que contienen archivos xml; haciendo uso de los algoritmos de entrenamiento y detección que buscan una aproximación de rasgos del rostro mediante cálculos matemáticos. El algoritmo de entrenamiento es un archivo que entrena las características de las personas y determina si es o no mediante el algoritmo de reconocimiento, como se ve en el siguiente esquema:

```
//Entrenamiento
/* IplImage[ ] trainImages = new IplImage[10];
for(int i=1; i<=10; i++){
//trainImages[i-1]=cvLoadImage("C:/facerecognizer/
data/images/training/terry"+i+".jpg");
trainImages[i-1]=cvLoadImage("C:/facerecognizer/
data/images/training/cr7"+i+".jpg");
CvSeq faces = reconocer.detectFace(trainImages[i-1]);
CvRect r = new CvRect(cvGetSeqElem(faces,0));
trainImages[i-1]=reconocer.preprocessImage(trainI-
mages[i-1], r); }
reconocer.learnNewFace("cr", trainImages); */
//Reconocimiento
IplImage target = new IplImage();
```

```
//target = cvLoadImage("C:/facerecognizer/data/ima-
ges/training/terry_target.jpg");
target = cvLoadImage("C:/facerecognizer/data/images/
training/cr7_target.jpg");
CvSeq faces2 = reconocer.detectFace(target);
CvRect r2 = new CvRect(cvGetSeqElem(faces2,0));
target=reconocer.preprocessImage(target, r2);
System.out.println("PERSONA IDENTIFICADA: "+re-
conocer.identifyFace(target));
```

## RESULTADOS Y DISCUSIÓN

En la actualidad dentro de las oficinas de la Capitanía del Puerto de la ciudad de Manta se encuentra en ejecución un sistema de vigilancia mediante cámaras IP, basado en un software de detección de rostro aplicado para el monitoreo y control de las personas que ingresan a esta entidad.

### Fase de especificaciones

El software detecta el rostro de cada una de las personas y las compara con los registros almacenados en los días anteriores, su principal característica es mostrar la identificación de las personas que son capturadas por las cámaras de vigilancia. Además, mediante la implementación del sistema se consiguió tener un registro de las imágenes y videos de las actividades que se realizan a diario (Figura 4).

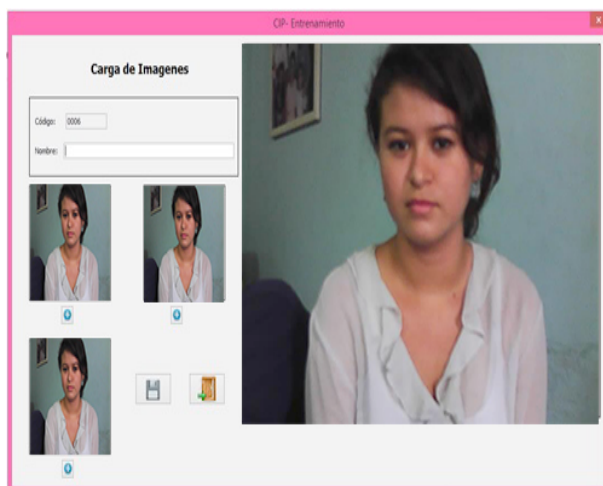


Figura 4. Pantalla de captura de imágenes para realizar prueba de detección de rostro.

### Fase de diseño de alto nivel y de detalle

La utilización de cámaras IP requiere configuraciones de sus protocolos por lo que se le asignó las direcciones IP para verificar su conectividad con el servidor (Figura 5) (Cuadro 1).

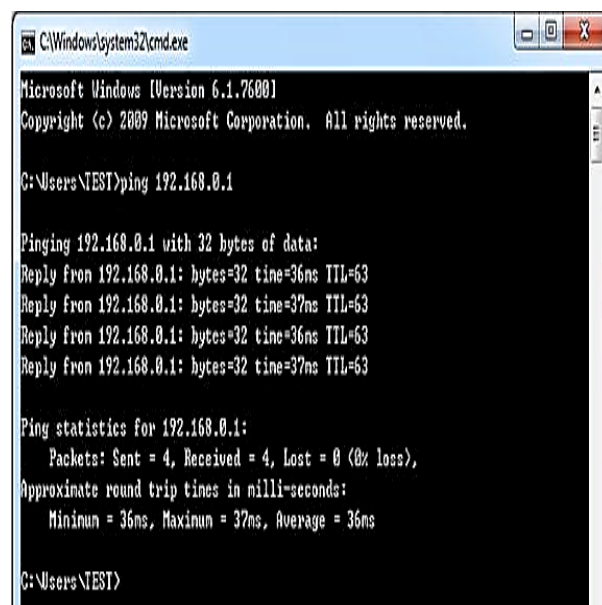


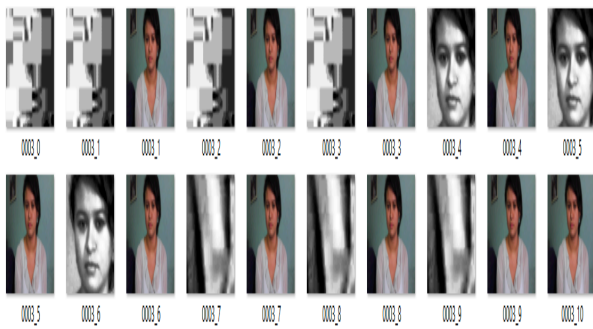
Figura 5. Tiempo de respuesta del servidor y el tráfico de espera de la cámara IP.

Cuadro 1. Direcciones IP asignados y puerto de enlace.

| Nombre de las cámaras  | Dirección IP  | Puerto de enlace asignado |
|------------------------|---------------|---------------------------|
| Dpto_Financiero1_Caja1 | 192.168.10.18 | 89                        |
| Dpto_Financiero1_Caja2 | 192.168.10.12 | 82                        |
| Dpto_Financiero2_Caja3 | 192.168.10.13 | 83                        |
| Dpto_Zarpe Arriba      | 192.168.10.11 | 81                        |
| Dpto_Jurídico          | 192.168.10.17 | 88                        |
| Pasillo Dirección      | 192.168.10.14 | 84                        |
| Dpto_Marítimo          | 192.168.10.16 | 86                        |
| Dpto_Personal_Marítimo | 192.168.10.15 | 85                        |

### Fase de implementación

La manera de representar los individuos de la población es uno de los principales componentes de los algoritmos genéticos que necesita ser adaptado al dominio de aplicación (Ñauñay *et al.*, 2013). Se consideró proveniente la validación del software durante los primeros días, generando información necesaria como captura de imágenes y grabación de videos dentro del servidor para realizar una comparación de los datos almacenados (Figura 6).



**Figura 6.** Rostro de una persona, se genera varias fotografías para capturar el rostro para su detección.

El software posee fácil visualización y manipulación para el usuario siendo necesario limitar el acceso solo al personal autorizado, y así evitar que existan posibles configuraciones previas a las ya realizadas (Figura 7).

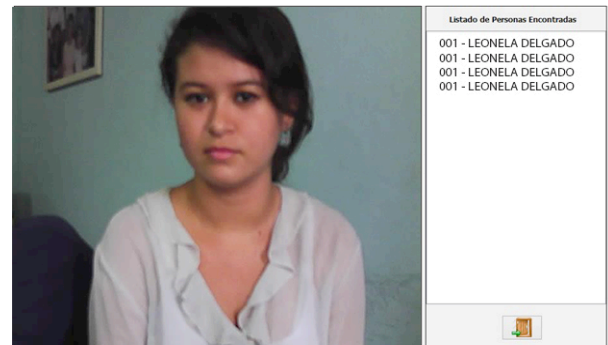


**Figura 7.** Pantalla principal del software en modo web

Guevara *et al.*, (2012) realizaron la implementación de una técnica de detección de rostros frontales como etapa inicial de un sistema automático para el reconocimiento de emociones a partir del análisis del movimiento y deformación del rostro.

### Fases del test unitario, de integración y operacional

El porcentaje de detección mediante esta técnica se calcula como la relación de la cantidad de rostros detectados sobre el número de imágenes usadas, una investigación insuficiente debido a que el sistema de vigilancia mediante cámaras IP genera automáticamente el número de imágenes necesarias para la detección, ya que el uso del algoritmo de entrenamiento hace el reconocimiento en 2.20 m menos que la metodología de clasificadores en cascada, usado por dichos investigadores (Figura 8).



**Figura 8.** Pantalla de identificación de personas, cantidad de veces que detecta a la persona.

La detección facial se atribuye a que el algoritmo de entrenamiento debe realizar una búsqueda sobre las imágenes, esto se puede mejorar aplicando el método únicamente sobre la región que ha sido detectada como rostro, ya que se estaría descartando información del fondo, y además se disminuiría el tiempo de procesamiento. En el entorno existen pocos trabajos de investigación dedicados a la detección de rostro y al monitoreo mediante cámaras IP como se estipula en este medio, pero es de vital importancia.

## CONCLUSIONES

La implementación del sistema de vigilancia dentro de las oficinas de la Capitanía del Puerto de la ciudad de Manta constituyó una necesidad primordial para el control y monitoreo de zonas de acceso frecuente.

Con el uso de un sistema de detección de rostro se pudo identificar cada una de las personas que se encuentran registradas dentro del sistema, mostrando el nombre de la persona.

Los altos porcentajes de detección y bajo tiempo de procesamiento demuestran la efectividad de los algoritmos de entrenamiento y reconocimiento; para la detección de rostro y características faciales, dan la posibilidad al sistema una aplicación en tiempo real.

## LITERATURA CITADA

- Blázquez, L. 2013. Reconocimiento facial basado en puntos característicos de la cara en entornos no controlados. Universidad Autónoma de Madrid. Tesis, Ing. Telecomunicaciones. Madrid, Es. p 11-30.
- Camacho, M; González, N; Garriga, E. 2009. Sistemas De Información En Salud. Aportes De La Maestría Informática En Salud. Revista Habanera de Ciencias Médica. Cuba. 8(3): 1-35.



- Catania, C. 2008. Reconocimiento de Patrones en el Tráfico de Red Basado en Algoritmos Genéticos. Revista Iberoamericana de Inteligencia Artificial. España. 12(37): 65-75.
- Engel, D; Stütz, T and Uhl, A. 2012. Assessing JPEG2000 encryption with key-dependent wavelet packets. University of Applied Sciences. Computer Sciences. Salzburg, Austria. 3-16.
- Guevara, M; Echeverry, J; Urueña, W. 2012. Detección de rostro en imágenes digitales usando clasificadores en cascada. Revista Scientia et Technica. Pereira, Co. 38(14): 1-6.
- Morales, R. 2008. Los Medios Informáticos: Tratamiento Procesal. Revista Dikaion. Bogotá, Co. 22(17): 297-324.
- Ñauñay, M; Tipantuña, L; Raura, G; Gualotuña, T. 2013. Análisis de eficiencia en algoritmos de reconocimiento de imágenes digitales aplicables a dispositivos móviles bajo la plataforma Android. Escuela Superior Politécnica del Ejército. Ingeniería en Sistemas. Sangolquí, Ec. p 1-10.
- Trujillo, F. 2009. Diseño de un Sistema de Vigilancia no Convencional basado en Redes Zigbee (802.15.4) para realizar un Control sobre Equipos de Video e Integración a Sistemas de Supervisión de mayor Jerarquía. Tesis. Ing. Eléctrico y Comunicaciones. Sangolquí. Ec. p 24.
- Villegas, M; Meza, M and Pilar, L. 2011. Las métricas, elemento fundamental en la construcción de modelos de madurez de la seguridad informática. Universidad Rafael Bellosó Chacín. Revistas Electrónica de Estudios Tele-máticos. Venezuela. 10(1): 1-16.
- Yasir Malik, M. 2012. Power Consumption Analysis of a Modern Smartphone. Seoul National University. 2(12):5-11.