VERIFICACIÓN BIOMÉTRICA DE IDENTIDAD USANDO RECONOCIMIENTO DE ROSTRO Y PATRONES DE TECLEO

Luis Felipe Gómez Gómez
Ingeniería de Telecomunicaciones

Asesor:
MSc. Juan Camilo Vásquez Correa

Universidad de Antioquia
Facultad de Ingeniería
2018

Contenido

- Introducción.
- Objetivos.
- Marco Teórico.
  - Análisis de patrones de tecleo.
  - Detección de rostros.
  - Aprendizaje automático.
- Metodología.
- Resultados y Análisis.
  - Reconocimiento de rostros.
  - Dinámica de tecleo
- Conclusiones.

Introducción

- Problema: Falsificación de identidad:

Introducción

- Propuesta:
  - Desarrollo de un sistema biométrico basado en reconocimiento de rostros y patrones de tecleo.

- Ventajas:
  - Eliminar el factor humano.
  - Fácilmente escalable.
  - Muchas Aplicaciones.

Introducción

- Los sistemas biométricos pueden dividirse en dos categorías:
  - Sistemas basados en características fisiológicas.
  - Sistemas basados en características conductuales.

- El reconocimiento de rostros se desarrollo entre los años 60 y 80.
- El análisis de patrones de tecleo se inició durante la Segunda Guerra Mundial.

Introducción

Fisiológicas

Huellas Dactilares

Rostro

Ojos

Conductuales

Voz

Tecleo

Objetivos

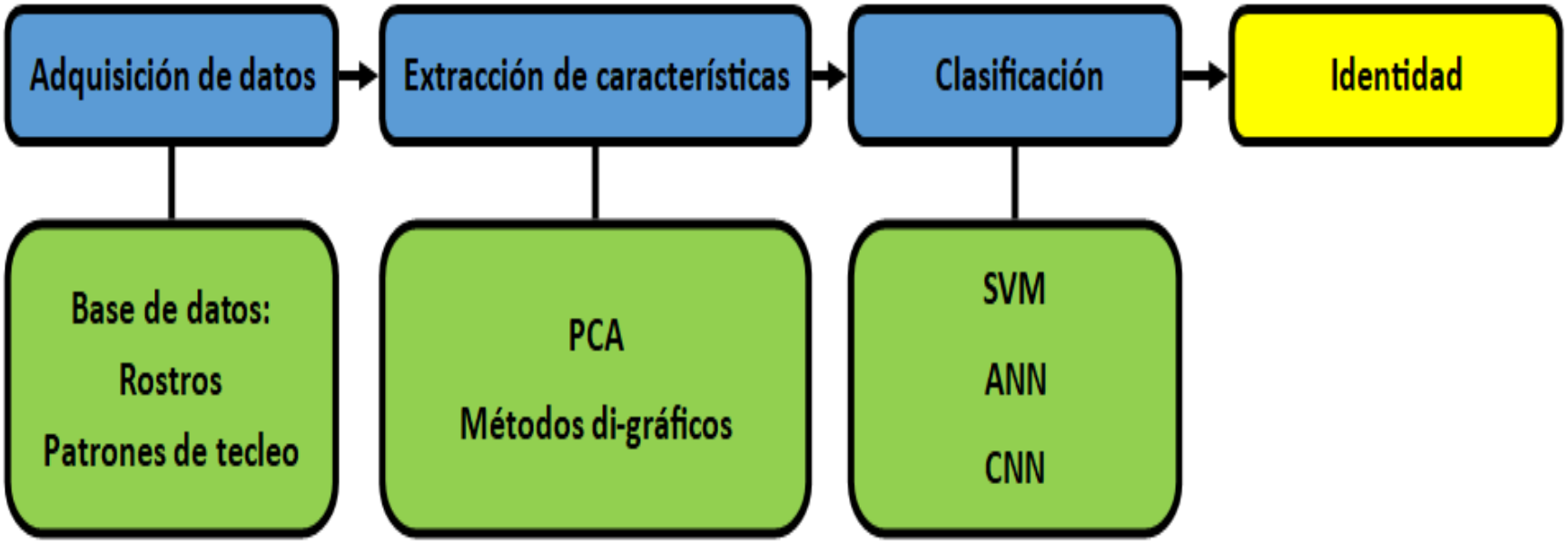
- **Objetivo general:**

  – Desarrollar un sistema de reconocimiento biométrico el cual identifique a las personas en dos etapas, a través de la identificación de su rostro y la comprobación de su patrón de tecleo.

Objetivos

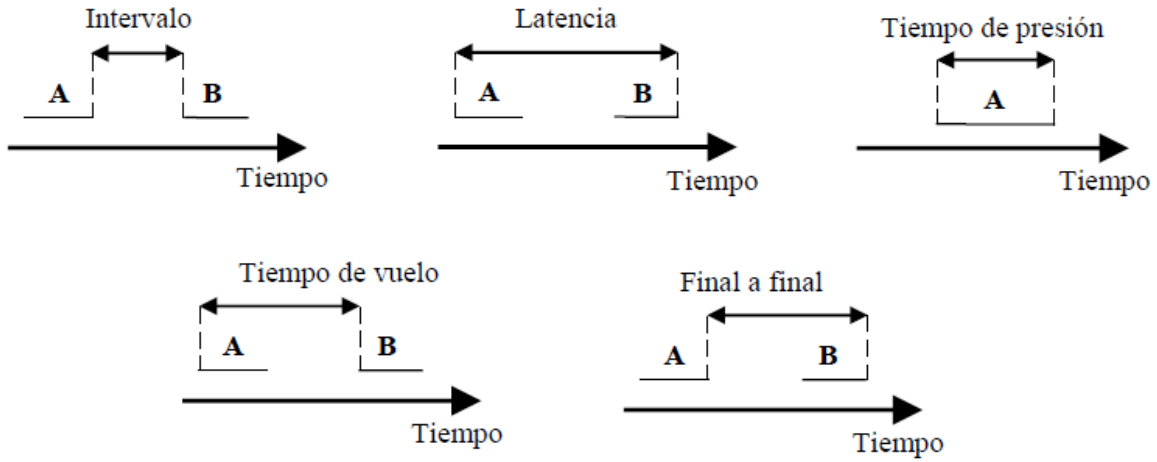
- **Objetivos específicos:**
  - Recolectar una base de datos de rostros y patrones de tecleo de personas para la implementación del sistema biométrico.
  - Implementar algoritmos que permitan extraer la información más relevante de rostros de personas para su posterior reconocimiento.
  - Implementar algoritmos que permitan extraer medidas de tiempos entre diferentes teclas presionadas por el usuario para su posterior reconocimiento.
  - Identificar e implementar los métodos de clasificación más eficientes para el reconocimiento en cada modalidad.

Marco teórico

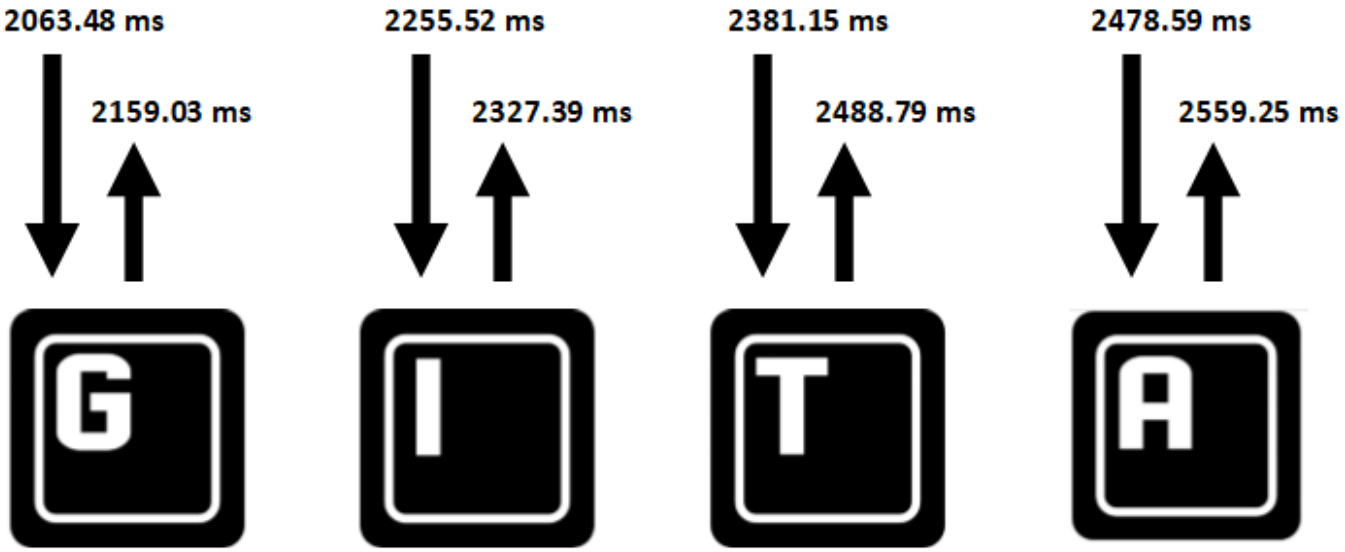


Marco teórico

- Análisis de patrones de tecleo.
  - La dinámica de tecleo provee información sobre dos eventos comunes:
    - La presión de la tecla a usar.
    - La liberación de la tecla a usar.



Marco teórico



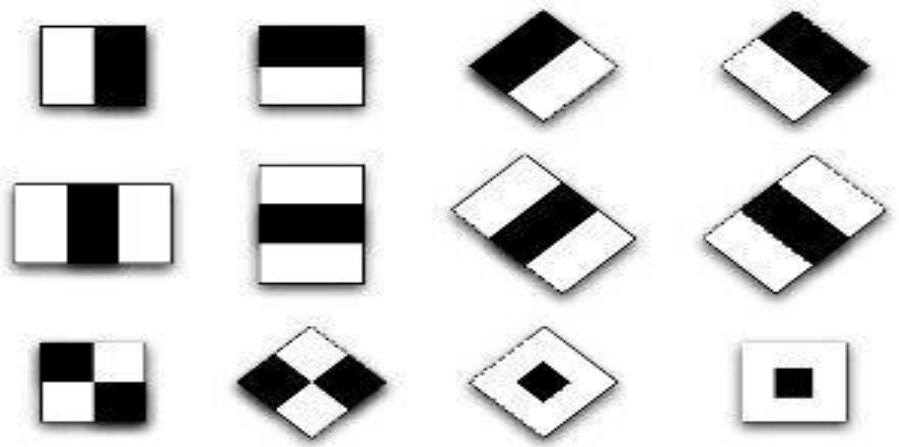
Marco teórico

- Detección de rostros.
  - El rostro humano es altamente variable.
  - En los 90 de desarrollaron algoritmos de detección de rostros:
    - Cascada Haar.
    - PCA.

Marco teórico

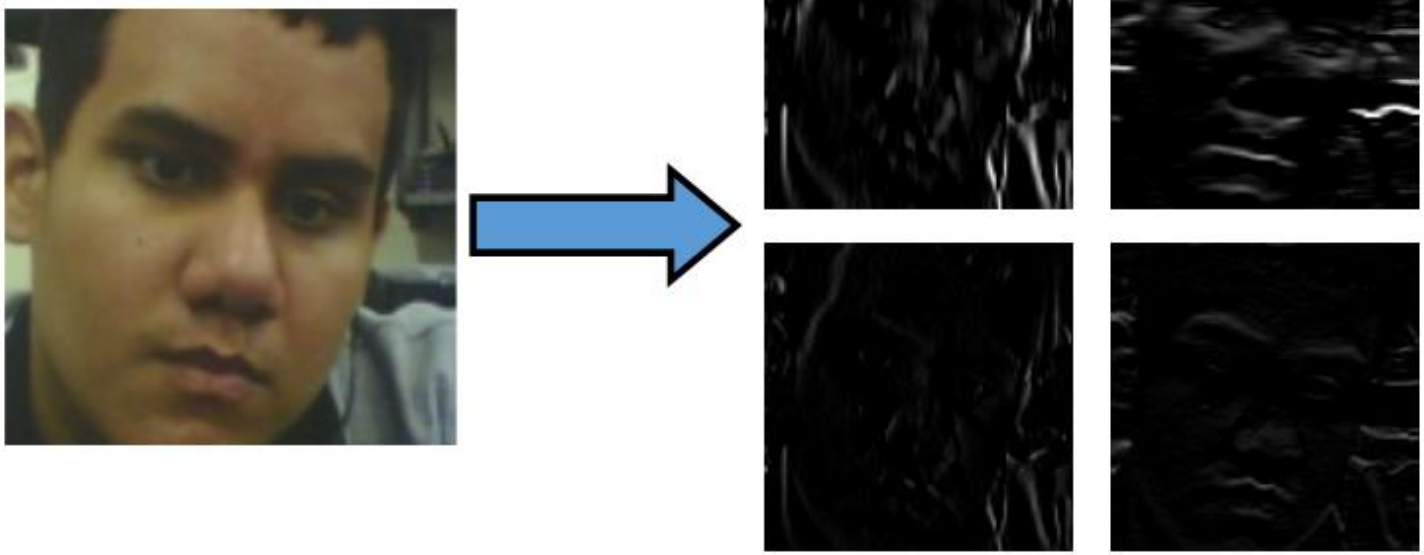
Cascadas Haar.

Serie de filtros que buscan encontrar un objeto (o rostro) en una imagen.



Mascaras de filtros de Haar

Marco teórico



Marco teórico

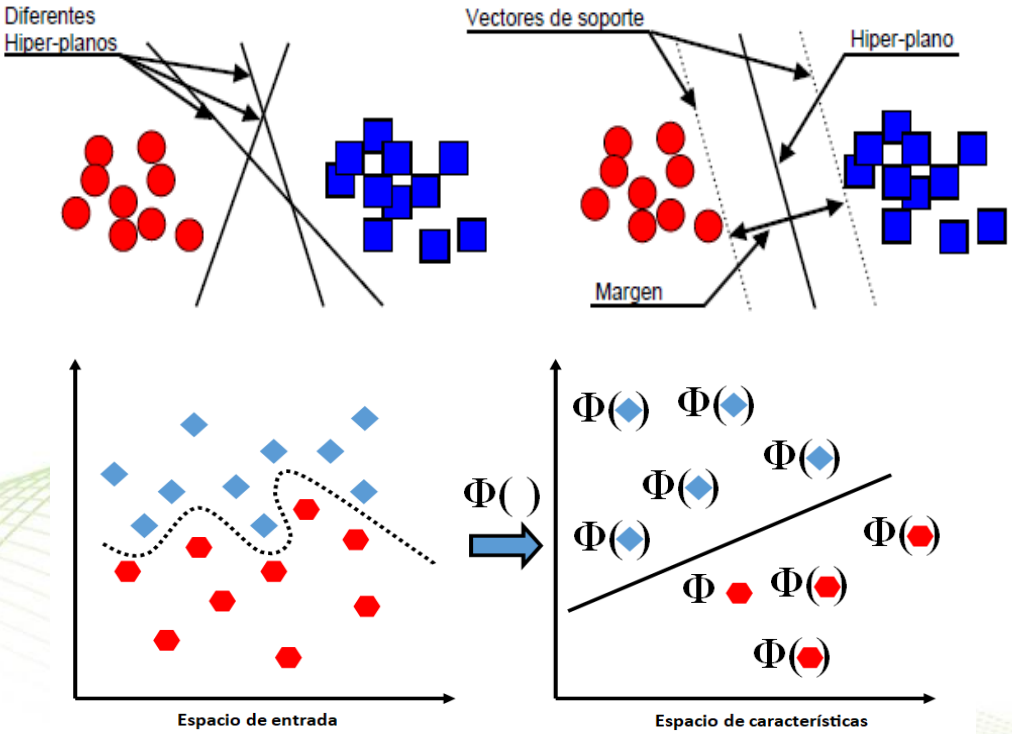
Análisis de componentes principales (PCA)

Método no supervisado de reducción de dimensión que mantiene la información más relevante de los rostros de las personas.

[1]Database: http://cvc.yale.edu/projects/yalefacesB/yalefacesB.html

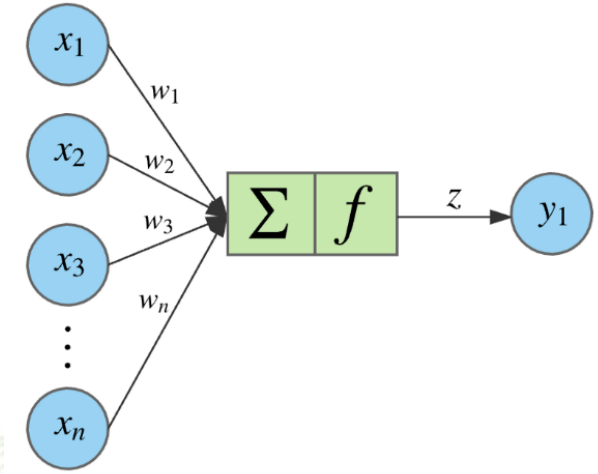
Marco teórico

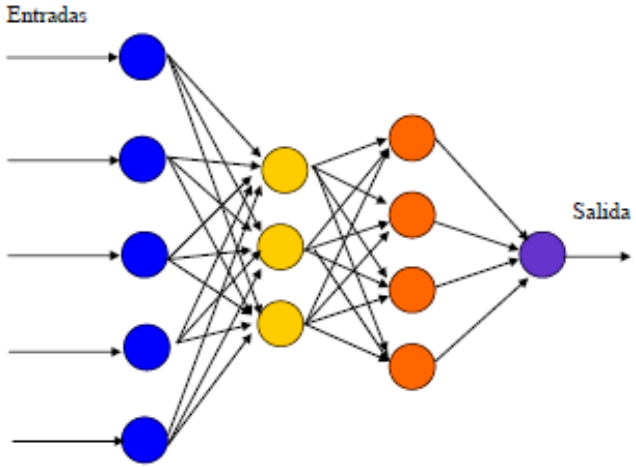
- Aprendizaje Automático.
  - Maquinas de Soporte Vectorial.



Marco teórico

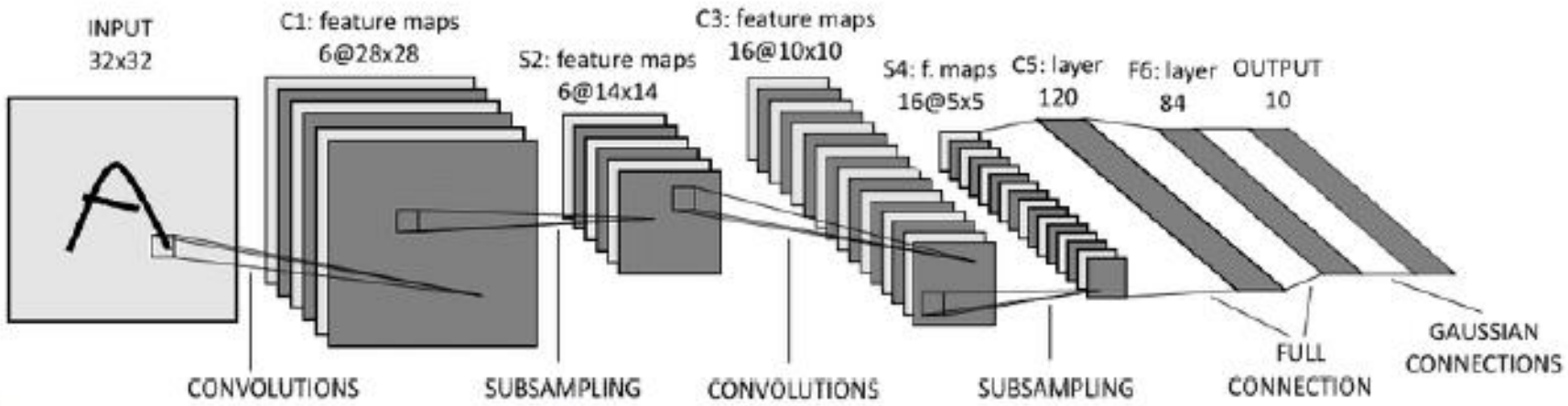
- Aprendizaje Automático.
  - Redes neuronales artificiales (RNA).



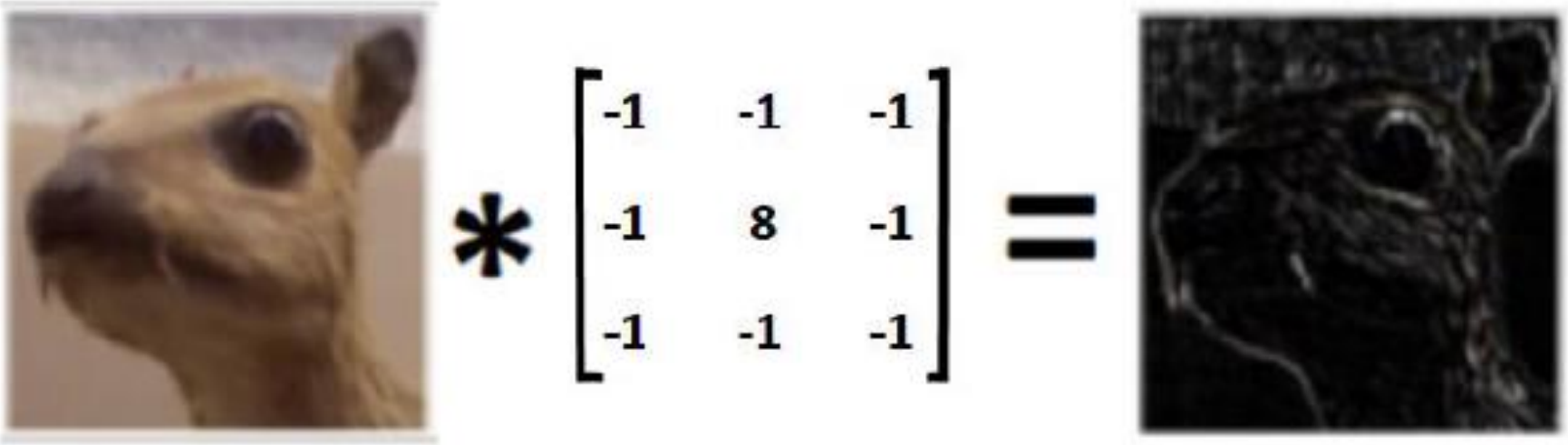


Marco teórico

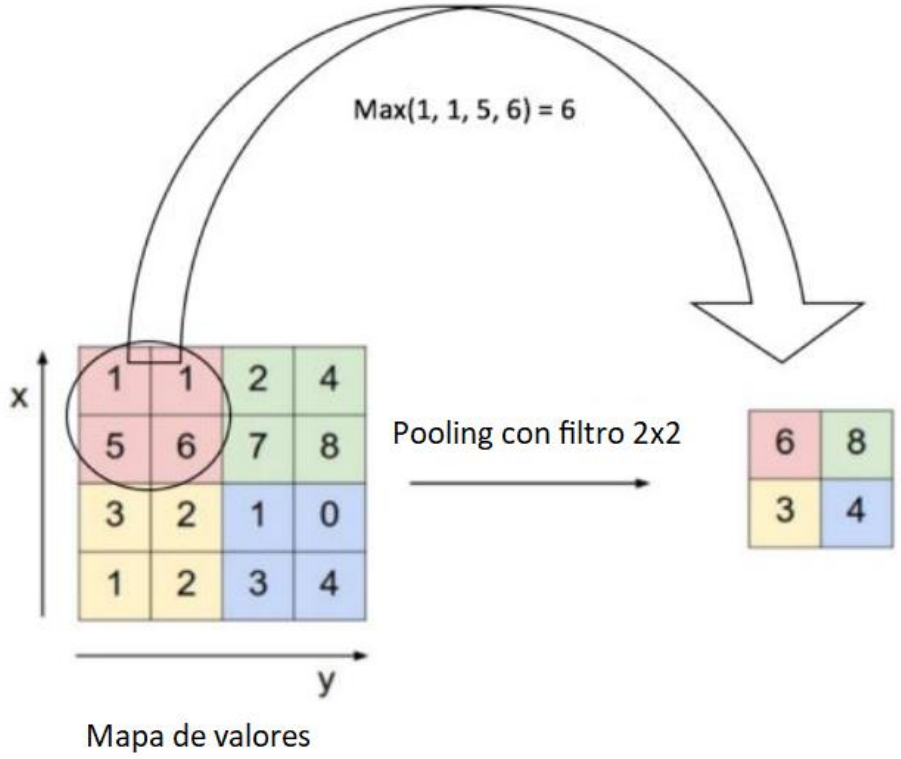
- Aprendizaje Automático.
  - Redes neuronales convolucionales (CNN).
    - Las imágenes pasan por una serie de filtros y se submuestrean.
    - Finalmente los datos pasan por una red neuronal de múltiples capas.



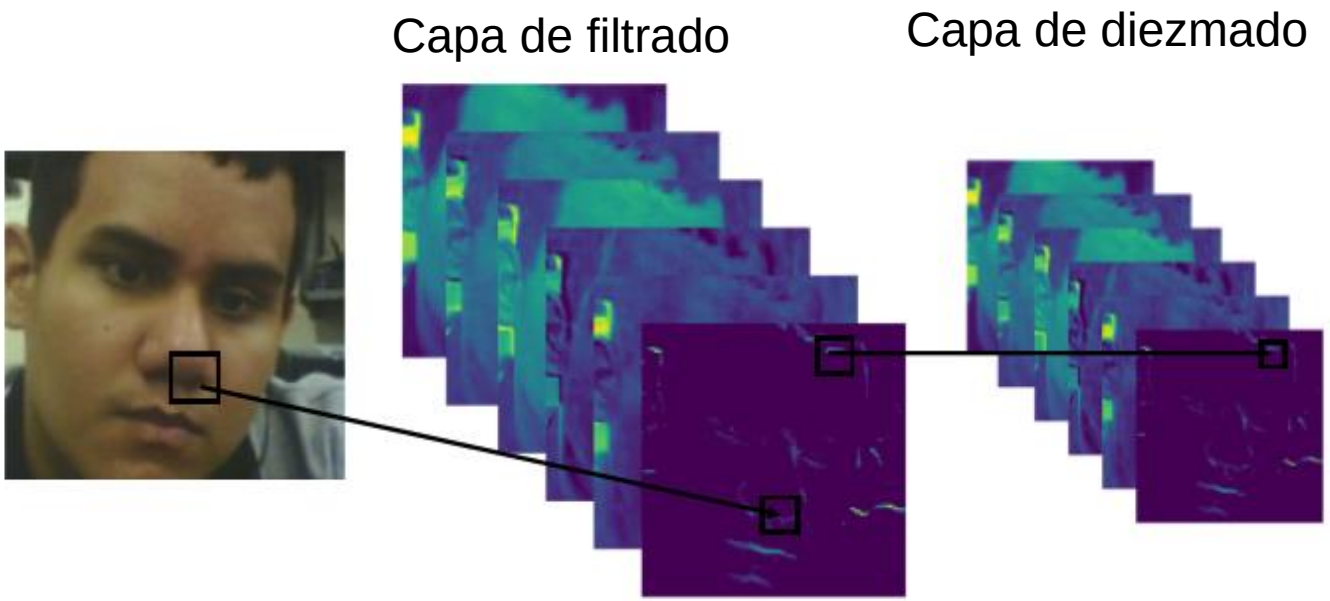
Marco teórico



Marco teórico

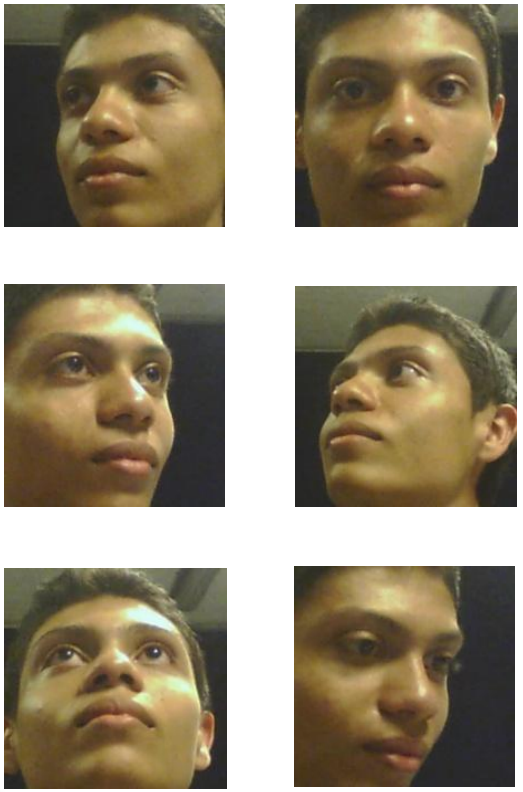


Marco teórico



Metodología

- Base de datos.
  - 52 rostros de estudiantes de la Universidad de Antioquia.
    - 34 hombres y 18 mujeres entre los 19 y 26 años.
  - Archivos con información mecanográfica de los estudiantes.
    - Tiempos de presión y liberación.



Metodología

Actividades realizadas:

- Rostros:
  - 5 fotografías/sesión.
  - Diferentes ambientes (iluminación).
  - Cambios de inclinación del rostro.
- Patrones de tecleo:
  - Captura de tiempos en tres frases (5 capturas/sesión):
    1. “universidad gita”.
    2. “laboratorio led”
    3. “investigacion udea”
- Captura simultanea rostros/tecleo.

Metodología

- Sistema de verificación de rostros.
  - Extracción de características.
    - Filtros de cascadas Haar.
    - PCA.
    - Se empleo desde el 70 al 90% de la información de los rostros originales.

Metodología

(a)

(b)

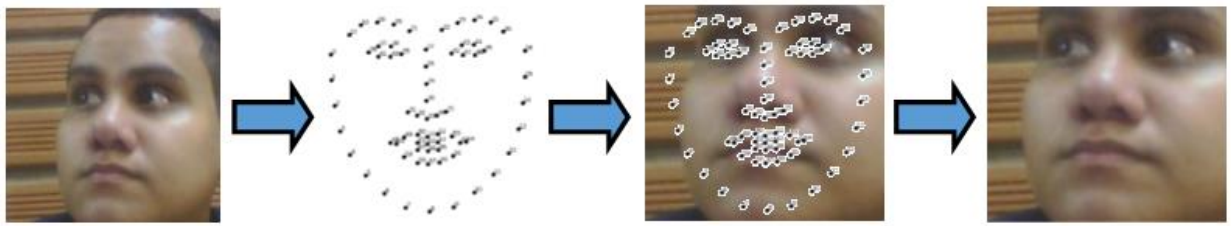
(a) Conjunto original de fotos. (b) Conjunto reconstruido con el 90% de la información original.

Metodología

- Sistema de verificación de rostros.
  - Clasificación.
    - SVM, variando el parámetro C.

C	10-3	10-2	10-1	100	101	102	103	104

    - CNN: Fine-tuning de red neuronal entrenada para detección de rostros. Los rostros se normalizan respecto a una posición central.



[2]Database: http://vis-www.cs.umass.edu/lfw/

Metodología

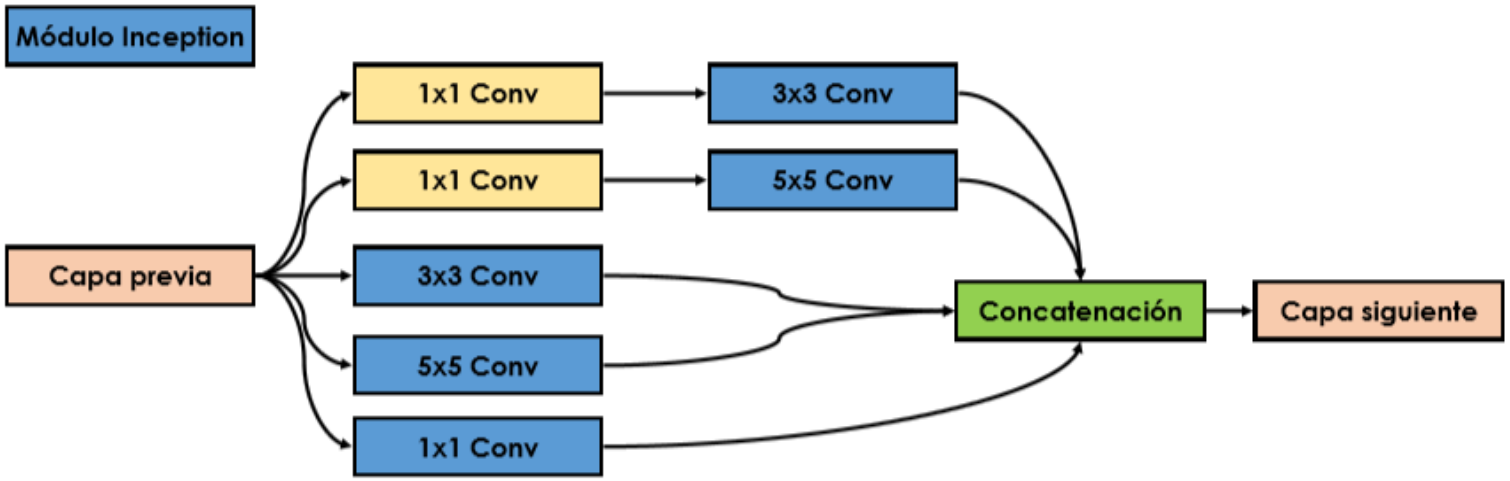
CNN
Facenet

- CNN con 128 salidas
- En capas intermedias hay módulos de inception.
- Regularización norma L2 para evitar overfitting

Tipo de capa	Tamaño de salida
conv1 (7x7x3,2)	112x112x64
max pool + norm	56x56x64
inception (2)	56x56x192
norm + max pool	28x28x192
inception (3a)	28x28x256
inception (3b)	28x28x320
inception (3c)	14x14x640
inception (4a)	14x14x640
inception (4b)	14x14x640
inception (4c)	14x14x640
inception (4d)	14x14x640
inception (4e)	7x7x1024
inception (5a)	7x7x1024
inception (5b)	7x7x1024
avg pool	1x1x1024
fully conn	1x1x128
L2 normalization	1x1x128

Metodología

Módulo inception:
Filtros convolucionales 1x1, 3x3 y 5x5 en paralelo.



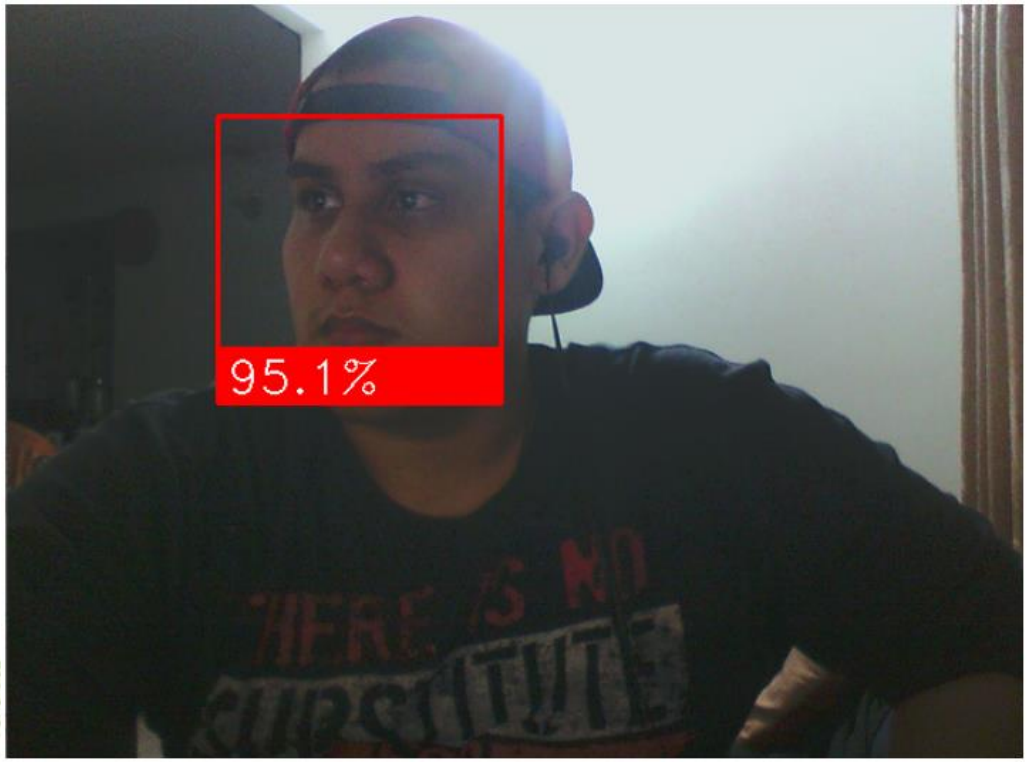
Metodología

- Sistema final:
  - El usuario escribe su documento de identidad mientras la cámara captura el rostro.

- El rostro capturado se procesa (PCA+SVM, o CNN), y se compara con las características obtenidas en la base de datos:

  - Distancia coseno.
  - Función de activación sigmoidal.

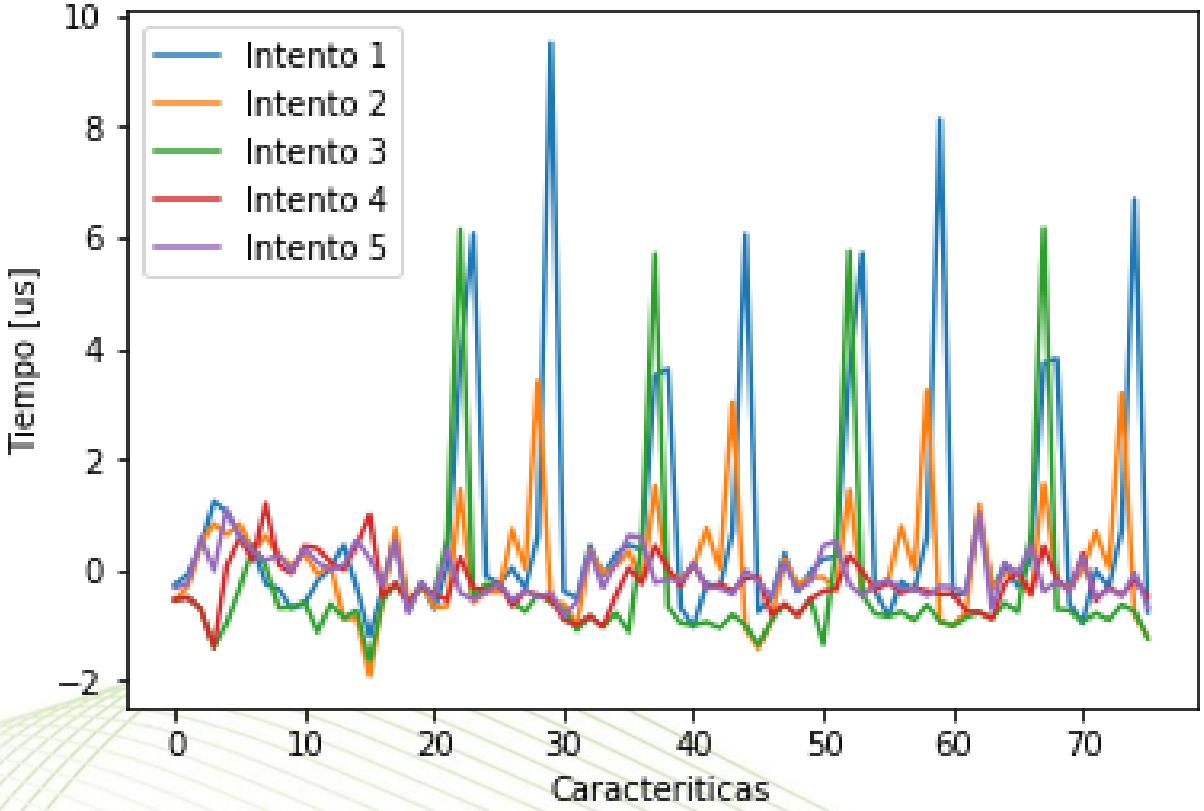
Metodología



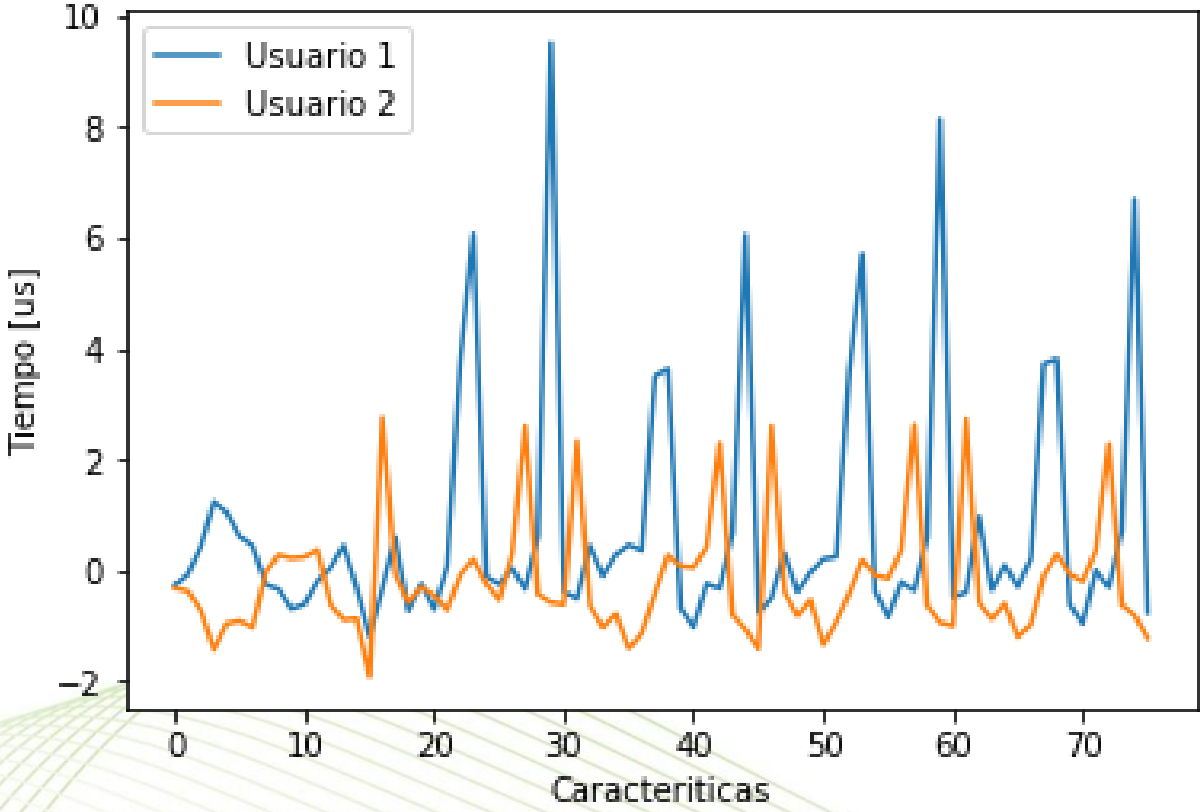
Metodología

- Dinámica de tecleo.
  - Toma archivos .csv
  - Divide los datos en dos columnas:
    - Teclas presionadas.
    - Tiempo de liberación de las teclas.
  - Se encontraron 5 métricas diferentes:
    - Duración.
    - Latencia.
    - Intervalo
    - Tiempo de vuelo
    - Final a final

Metodología



Metodología



Metodología

- Dinámica de tecleo.
- 5 Sistemas divididos en dos grupos:
  - Medidas de similitud entre los datos de prueba y los de la base de datos

    1. Distancia euclidiana.
    2. Distancia coseno
    3. Coeficiente de correlación (Spearman o Pearson).

  - Sistemas de clasificación supervisada:

    4. SVM
    5. ANN

Resultados y análisis

- Reconocimiento de rostros.
  - PCA – SVM

PCA	Aciertos entrenamiento	Aciertos prueba	Valor C de la SVM
70 %	78 %	64 %	10
75 %	84 %	76 %	100
80 %	98 %	82 %	10
85 %	99 %	84 %	1000
90 %	99 %	87%	100

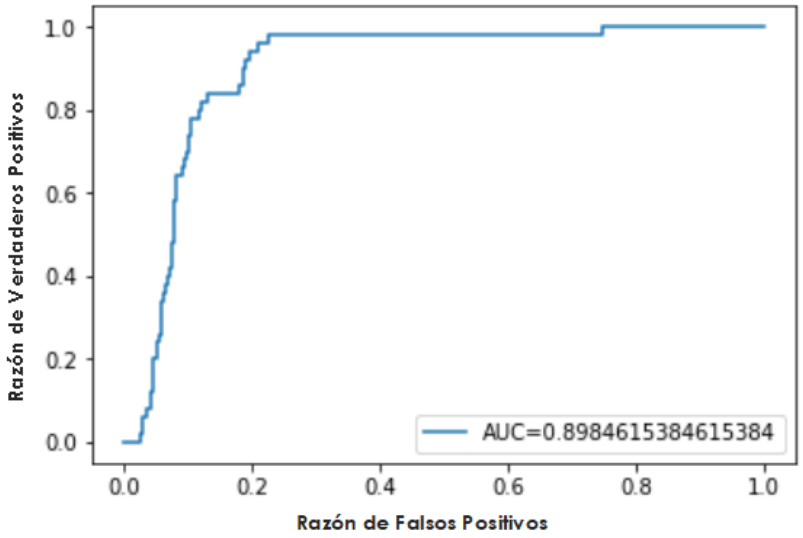
Ambiente de prueba	Porcentaje de aciertos
Controlado	70 %
Reales	33 %
Cambios en la inclinación del rostro	46 %

Resultados y análisis

- Reconocimiento de rostros.
  - CNN

Métricas	Porcentaje
FPR	7.95 % ± 5.09 %
FNR	8.41 % ± 4.31%

Ambiente de prueba	Porcentaje de aciertos
Controlado	92.4 %
Reales	85.3 %
Cambios en la inclinación del rostro	88.7 %



Resultados y análisis

- Dinámica de Tecleo.

Método	Aciertos en pruebas
Distancia Euclidiana	23 %
Coeficiente de correlación	55 %
Distancia coseno	53 %
SVM	62 %
RNA	71 %

Conclusiones

- El reconocimiento de rostros basado en PCA+SVM presenta altas fallas cuando se utiliza en condiciones no controladas.

- Tasa de aciertos se reduce del 80% al 35%.

- El reconocimiento basado en CNN usando Facenet funciona muy bien en condiciones no controladas, pasando del 92% al 88%.

Conclusiones

- El sistema de reconocimiento de patrones de tecleo ofrece aciertos de hasta el 76% usando las características di-graficas implementadas.

- Con una base de datos más grande, y un esquema de clasificación mas robusto se pueden mejorar los resultados.

Trabajo futuro

Mejorar el desempeño del sistema de verificación de identidad:

- Implementar sistemas multimodales.
- Implementar métodos como las redes neuronales recurrentes (RNN) con unidades de larga memoria de corto plazo (LSTM).

UNIVERSIDAD DE ANTIOQUIA
1803

Muchas gracias.