Estudio Comparativo de Algoritmos de Compresión de Imágenes de Huellas Digitales Implementados en una DSP de la Familia C6000.

ERWIN. Jurado ALARCON[1] , PEDRO. Vargas[1] , J.A. Ortega[2]
[1] Facultad de Ingeniería en Electricidad y Computación (FIEC)
Escuela Superior Politécnica del Litoral (ESPOL)
Campus Gustavo Galindo, Km 30.5 vía Perimetral, Apartado 09-01-5863, Guayaquil, Ecuador.
[2]Grupo de Accionamiento Electrónicos y Aplicaciones Industriales (MCIA)
Universidad Politécnica de Cataluña (UPC)
Campus Terrassa, C/Colom # 1, Código Postal 08222, Terrassa, España.
ejurado@fiec.espol.edu.ec, pvargas@espol.edu.ec, juan.antonio.ortega@mcia.upc.edu

Resumen

Este artículo tiene como objetivo mejorar la eficiencia de un sistema de verificación de huellas digitales, en lo que respecta al tamaño de base de datos y velocidad de transmisión de datos. Para lograrlo se hizo un estudio comparativo entre diferentes algoritmos de compresión de huellas digitales (JPEG, Hadamard y Binaria), puesto que al comprimir las imágenes de las huellas se logra disminuir, tanto el tamaño de la base de datos como su tiempo de transmisión. Se implementó usando un sistema de verificación de huellas (sistema FADT, tarjeta de adquisición de datos TMS320C6713DSK y sensor de huellas FPC1010).
El análisis de resultados se realizó usando parámetros de seguridad establecidos (tasa de falso rechazo y falsa aceptación, entre más bajo son estos valores, el sistema de seguridad es más eficiente) y el nivel de compresión de los algoritmos. De los indicadores usados, los parámetros de seguridad tenían mayor prioridad al momento de dar la conclusión, en base a esto se dedujo que la Compresión Binaria optimizaba el sistema de verificación pues obtuvo el nivel mas bajo de tasa de falso rechazo y falsa aceptación.
Este estudio puede servir como base para la implementación de un sistema real de verificación a distancia.

Palabras claves: *compresión de huellas digitales, verificación de huellas digitales, Procesadores de Señales Digitales (DSP), tasas de falsa aceptación y falso rechazo.*

Abstract

This paper aims to improve the efficiency of a system for verifying fingerprints, as regards the size of database and data rate. To achieve this was a comparative study between different compression algorithms fingerprint (JPEG, Hadamard and Binary), as to compress the images of fingerprints is achieved reducing both the size of the database as its transmission time. We implemented using a fingerprint verification system (FADT system, data acquisition board TMS320C6713DSK and FPC1010 sensor footprints).
The results were analyzed by using parameters established security (rate of false rejection and false acceptance among these values are lower, the security system is more efficient) and the level of compression algorithms. Of the indicators used, the safety parameters had more time to give priority to the conclusion, based on this information it emerged that the Binary Compression optimized the verification system because the level was lower rate of false rejection and false acceptance.
This study may serve as a basis for the implementation of a real system of verification distance.

Keywords: c*ompression fingerprints, verification of fingerprints, Digital Signal Processors (DSP), charges of false acceptance and false rejection.*

1. Introducción

En la actualidad la verificación de personas a través de una huella digital es un método eficiente de seguridad para salvaguardar las pertenencias de las personas [7] [8] [9] [10]. El problema se presenta cuando se forma la base de datos y cuando se transmiten a través de medios informáticos por su tamaño, pues a mayor calidad de imagen, mas alta es la cantidad de bytes que se almacenan [4].

Esta investigación pretende encontrar un método de compresión que permita reducir el tamaño de la imagen de la huella minimizando en lo posible los errores que se presentan en los métodos de verificación [4], esto es que se realice una falsa aceptación (que siendo la persona equivocada el sistema lo acepte) o un falso rechazo (siendo la persona correcta el sistema lo acepte) de la persona que se autentifica [2] [7] [10].

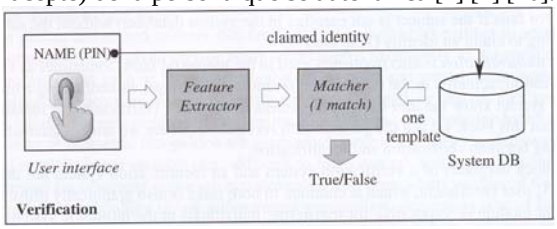


Figura 1: Proceso de verificación

Es importante indicar que un método de verificación permite en sus niveles de seguridad ciertos valores de falso rechazo, pero es inadmisible permitir niveles de falsa aceptación pues esto acarrearía un riesgo al sistema [4] [9] [10].

Se implementan tres métodos de compresión (JPEG, Hadamard y Binaria), para luego mediante parámetros estadísticos (Tasa de falsa aceptación y falso rechazo) determinar cual método me permite una óptima compresión y minimizar el valor de la tasa de falsas aceptaciones [4].

La implementación de los métodos se la realiza usando un DSP de la familia C6000 (TMS320C6713) y el sistema FADT de verificación de huellas digitales.

2. Características de la huella digital

Las imágenes de huellas digitales se capturan al colocar las yemas de los dedos sobre una superficial lisa. Estas normalmente se capturan en tonalidades grises (en adelante la denominaremos como '*en escala de grises'*). La estructura característica de una huella es un modelo de líneas de crestas y valles entrelazados; en una imagen de huella digital las crestas son oscuras y los valles son claros, generalmente viajan en paralelo [6].

La imagen digitalizada de una huella en escala de grises se representa como una función de dos dimensiones de n niveles grises; en donde, cada valor de esta función representa su nivel de intensidad en la imagen y cada posición de la imagen, que se identifica con las coordenadas x i y, se denomina píxel. Las líneas de crestas se la relacionan con los píxeles oscuros (valores cercanos a cero en la escala de grises) y los valles con los píxeles claros (valores cercanos a n-1 en la escala de grises) [2].

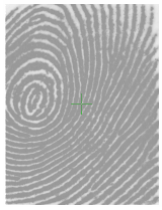


Figura 2: Imagen de una huella digital

3. Técnicas de Compresión de Huellas Digitales

Las técnicas de compresión con pérdidas permiten reducir la cantidad de datos en una imagen eliminando datos redundantes. La redundancia psicovisual, permite eliminar datos para la vista humana irrelevantes; la redundancia entre píxeles, permite eliminar la correlación de datos usando la transformación lineal de las imágenes; la redundancia de código, permite eliminar datos al usar un código diferente para cada dato según sea mas o menos probable su aparición en la imagen [1].

3.1 Compresión JPEG

La compresión JPEG elimina las redundancias del tipo entre píxeles, psicovisual y de código [1].

La compresión se realiza en tres etapas: cálculo de Transformada Coseno Discreta (DCT), cuantificación y asignación de un código de longitud variable [1] [2] [3].

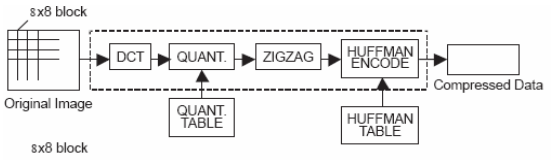


Figura 3: Esquema compresión JPEG

La descompresión JPEG se realiza tres etapas: descodificación Huffman, decuantificación y cálculo de la Transformada Inversa Coseno Discreta [1] [2] [3].

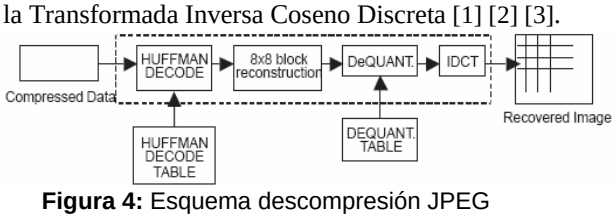


Figura 4: Esquema descompresión JPEG

3.1.1 Transformada Coseno Discreta

Es una transformada real y ortogonal, tiene unas características óptimas en cuanto a compactación de

energía y a decorrelacionar coeficientes. Esta definida por la ecuación (1)

Su aplicación más importante es la compresión de imágenes (para lo cual la imagen se subdivide en matrices de 8x8) [3].

$$F_{v,u} = \frac{1}{4} c_u c_v \sum_{x=0}^{7} \sum_{y=0}^{7} f_{y,x} \cos\frac{(2x+1)u\pi}{16} \cos\frac{(2y+1)v\pi}{16} \quad (1)$$

$$C_U = C_V = \begin{cases} \frac{1}{\sqrt{2}} & \text{para u, v = 0} \\ 1 & \text{para otro caso.} \end{cases}$$

3.2 Compresión Hadamard

La compresión Hadamard elimina las redundancias del tipo entre píxeles y psicovisual [1].

El método de compresión Hadamard se basa en dos etapas: cálculo de la Transformación Hadamard y cuantificación [1] [2].

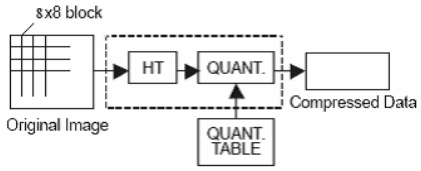


Figura 5: Esquema compresión Hadamard

La descompresión tiene dos etapas; decuantificación y cálculo de la Transformada Inversa Hadamard [1] [2].

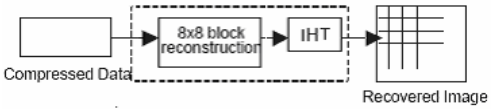


Figura 5: Esquema descompresión Hadamard

3.2.1 Transformada Hadamard

Es una transformación real, simétrica y ortogonal, de cálculo rápido, posee una buena compactación de energía para imágenes altamente correlacionadas. Esta definida por la ecuación (2)

$$H(u,v) = \frac{1}{N} \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} x[m,n] \cdot (-1)^{\sum_{i=0}^{t-1} [b_i(m)b_i(u) + b_i(n)b_i(v)]} \quad (2)$$

$$a_{u,v}(m,n) = \frac{1}{N} \cdot (-1)^{\sum_{i=0}^{t-1} [b_i(m)b_i(u) + b_i(n)b_i(v)]}$$

3.3 Compresión Binaria

La compresión Binaria elimina las redundancias de código [1].

Esta compresión se basa en la binarización de las imágenes de entrada. La escala de grises usada en el proyecto inicia en cero y termina en 255, es de 256 niveles.

Se elige un valor de umbral, si el valor del píxel es mayor al de umbral entonces se le da el valor de 255 (blanco en la escala de grises) y si el valor del píxel es menor al de umbral entonces se le da el valor de cero (negro en la escala de grises) [4].

Los valores de 0 y 255 siguen teniendo 8 bits para su descripción, por eso estos valores se convierten en 0 y 1, respectivamente, para describir cada píxel con un solo bit. Esto hace que la compresión sea fija, de ocho a uno; inmediatamente se encripta los datos, de tal manera que en un byte el espacio que antes ocupaba 1 píxeles, ahora lo ocupan 8 píxeles [4].

Para la descompresión se usa el mismo procedimiento indicado anteriormente, pero de manera inversa.

4. Análisis Estadístico

Para el análisis estadístico de las compresiones implementadas, no vamos a utilizar los criterios de fidelidad comunes para ellas, como lo que se desea es saber que tan fiable son estos métodos de compresión para poder realizar la verificación de personas usaremos las variables estadísticas: Tasa de Falsa Aceptación (FAR) y Tasa de Falso Rechazo (FRR).

4.1 Base de Datos

En este proyecto se han almacenado un total de 50 huellas digitales tomadas de 10 personas diferentes, tomando de cada uno cinco huellas al azar. La edad comprendida de estas personas oscila entre 22 y 41 años; mientras que por sexo, la cantidad de hombres y mujeres es la misma, es decir, cinco para cada grupo.

Cada huella fue capturada dos veces, la primera para obtener un patrón de la huella (proceso de registro) y la otra para capturar la imagen de la huella de manera total, esta imagen es llamada Imagen Original, y es la que servirá para obtener las imágenes de los tres métodos de compresión implementados.

4.2 Comparación o Estudio Realizados

Para ser objetivo en nuestro análisis comparativo debemos tomar alguna referencia.

Para el caso del proyecto, tomaremos como referencia la tasa de falsa aceptación y la tasa de falso rechazo de las imágenes originales. Un dato importante de resaltar es que las verificaciones que se realicen con las imágenes originales se realizarán con un nivel de seguridad o sensibilidad de 1/1000 o 0,1% de Falsa Aceptación (es preciso recordar que el nivel de máxima seguridad es de 1/100000 o 0,00001% de Falsa Aceptación) [5].

Todas las imágenes originales serán comprimidas usando los tres tipos de compresión implementados, luego cada una de estas imágenes serán descomprimidas, para inmediatamente ser verificadas.

Todos los resultados serán agrupados por compresión y almacenados para luego calcular la Tasa de Falsa Aceptación y Tasa de Falso Rechazo de cada

uno de estos grupos y poder definir una conclusión apropiada.

4.3 Verificación de Huellas Procesadas

Las 50 imágenes originales fueron comprimidas en los tres métodos de compresión implementados, la descompresión de estas imágenes dio como resultado cuatro grupos de imágenes de huellas digitales descomprimidas (se implementó la compresión Hadamard con dos tipo de niveles de compresión diferentes: 4:1 y 1,78:1).

Cada uno de estos grupos fueron independientemente verificados. Cada uno de los patrones de huella fueron comparados con las cincuenta huellas originales y las descomprimidas, lo que da como resultado **2500 comparaciones** por cada tipo de huellas (entre original y descomprimida).

Para el cálculo de la tasa de falsa aceptación, se toma como referencia la cantidad de comparaciones en donde teóricamente debe existir rechazo, en el caso de este análisis, seria de **2450 comparaciones**.

Para el cálculo de la tasa de falso rechazo, se toma como referencia la cantidad de comparaciones en donde teóricamente debe existir aceptación, en el caso de este análisis, seria de **50 comparaciones**.

Esto hace que en conjunto, entre verificación de huellas originales y descomprimidas, en comparación con los patrones de las huellas se llegue a un total de **12500 comparaciones**.

5. Resultados

5.1 Compresión JPEG

Este método de compresión alcanzo niveles de compresión que van de 6,2 a 15,2.

La aplicación de la etapa de verificación en donde comparamos huellas con los patrones que, teóricamente deben coincidir, da como resultado que 18 huellas digitales descomprimidas no satisfacen la verificación; lo cual indica que este método posee una tasa de falsa aceptación de 36%.

Mientras que la comparación de huellas que, teóricamente no coinciden con el patrón de la huella, da como resultado cero huellas digitales que satisfacen la verificación; lo cual indica una tasa de falso rechazo de 0%.

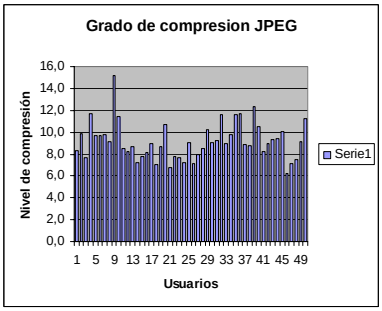
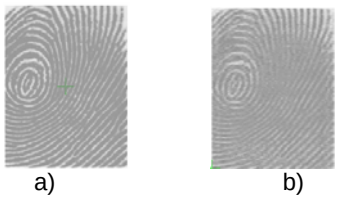


Figura 6: Niveles de compresión en el método JPEG



a) b)

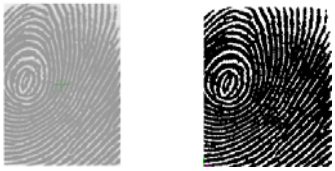
Figura 7: a) Imagen Original b) Imagen JPEG descomprimida

5.2 Compresión Binaria

Este método de compresión tuvo un nivel de compresión de 8:1.

La aplicación de la etapa de verificación en donde comparamos huellas con los patrones que, teóricamente deben coincidir, da como resultado que una huella digital descomprimida no satisface la verificación; lo cual indica que este método posee una tasa de falsa aceptación de 2%.

Mientras que la comparación de huellas que, teóricamente no coinciden con el patrón de la huella, da como resultado cero huellas digitales que satisfacen la verificación; lo cual indica una tasa de falso rechazo de 0%.



a) b)

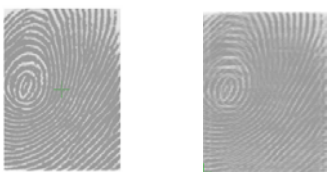
Figura 8: a) Imagen Original b) Imagen Binaria descomprimida

5.3 Compresión Hadamard (Primera Implementación)

Este método de compresión tuvo un nivel de compresión de 4:1.

La aplicación de la etapa de verificación en donde comparamos huellas con los patrones que, teóricamente deben coincidir, da como resultado que 27 huellas digitales descomprimidas no satisfacen la verificación; lo cual indica que este método posee una tasa de falsa aceptación de 54%.

Mientras que la comparación de huellas que, teóricamente no coinciden con el patrón de la huella, da como resultado cero huellas digitales que satisfacen la verificación; lo cual indica una tasa de falso rechazo de 0%.



a) b)

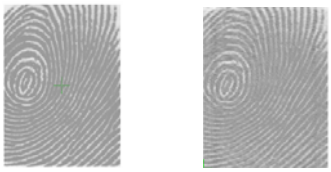
Figura 8: a) Imagen Original b) Imagen Hadamard 4:1 descomprimida

5.4 Compresión Hadamard (Segunda Implementación)

Este método de compresión tuvo un nivel de compresión de 1,78:1.

La aplicación de la etapa de verificación en donde comparamos huellas con los patrones que, teóricamente deben coincidir, da como resultado que 5 huellas digitales descomprimidas no satisfacen la verificación; lo cual indica que este método posee una tasa de falsa aceptación de 10%.

Mientras que la comparación de huellas que, teóricamente no coinciden con el patrón de la huella, da como resultado cero huellas digitales que satisfacen la verificación; lo cual indica una tasa de falso rechazo de 0%.



a) b)

Figura 8: a) Imagen Original b) Imagen Hadamard 1,78:1 descomprimida

5.5 Comparación de las Tasas de Falsa Aceptación y Falso Rechazo

Tabla 1: Resumen de los resultados en relación a niveles de compresión, porcentajes de Tasa de falsas aceptaciones (FAR) y Tasa de falsos rechazos (FRR)

MÉTODO DE COMPRESIÓN	Nivel de compresión	FRR	FAR
Hadamard 1º implementación.	4	54%	0%
JPEG	6,2 – 15,2	36%	0%
Binaria	8	2%	0%
Hadamard 2º implementación.	1,78	10%	0%

6. Conclusiones

La compresión Binaria posee mayor nivel de seguridad, pues el FAR es del 2% y el FRR del 0%.

La compresión JPEG contiene el mayor nivel de compresión, puesto que 36 de las 50 imágenes tienen un nivel de compresión mayor a ocho.

Si el nivel de compresión de Hadamard disminuye a un 44,5% entonces el valor de FAR disminuye al 18, 5%, aumenta el nivel de seguridad del sistema.

Para implementar un sistema de verificación remoto se usaría la compresión Binaria, por su nivel de seguridad.

7. Perspectivas de Futuro

Aumentar el tamaño de la base de datos para mejorar la eficiencia del cálculo de FAR y FRR.

Para mejorar el estudio, realizar la captura de los patrones de las imágenes descomprimidas pues es probable que las tasa de FAR bajen.

Implementar la compresión binaria con el estándar Grupo 4 del CCITT.

Futura implementación de este sistema de verificación e identificación a través de tecnología GPRS, en la cual un PDA seria un elemento de captura remota y el servidor, ubicado en un centro de información de una institución o empresa tendría almacenado los patrones para verificaciones o identificaciones.

8. Agradecimientos

Mis más sinceros agradecimientos para el Grupo de Accionamientos Electrónicos y Aplicaciones Industriales (MCIA) de la Universidad Politécnica de Cataluña en España.

En especial deseo mostrar un especial agradecimiento a los Drs. Juan Antonio Ortega y José Luís Romeral por la paciencia y sabios consejos que me brindaron en la realización del trabajo y en todo el tiempo que estuve en España, ellos unos grandes amigos.

9. Referencias

[1] González Rafael C., Woods Richard E.; *Tratamiento digital de imágenes*; Addison - Wesley Iberoamérica; Estados Unidos 1996; Capítulo 3: páginas 149,156-157, y Capítulo 6: páginas 335-352,373-439.

[2] Maltoni Davide, Maio Dario, Jain Anil K. Prabhakar Salil; *Handbook of Fingerprint Recognition*; Springer Science+Bussiness Media, Inc; Estados Unidos 2003; Capítulo 1: páginas 3-4, Capítulo 2: páginas 53-57, 59-65, y Capítulo 3: páginas 83-87.

[3] **Http://** www.fuac.edu.co/autonoma/pregrado/ingenieria/ingelec/proyectosgrado/compresvideo/index.htm**;** *Compresión de Video Digital*: Bajo los Estándares MPEG; Capítulo 6: páginas 1, 3 y 6.

[4] E. Jurado, Tesis de grado *Estudio Comparativo de Algoritmos de Compresión de Imágenes de Huellas Digitales Implementados en una DSP de la Familia C6000.* FIEC-ESPOL, 2008

[5] Fringerprint Cards AB; *User Manual FPCore Demo For Texas Instruments TMS320C6713 and TMS320C5510 DSP Started Kits* (Revisión D); Suecia, Noviembre 2003; páginas 3 y 12.
[6] R. Capella, A. Erol, D. Maio, D. Maltoni; *Synthetic Fingerprint-image Generation*; in proc. ICPR2000; Barcelona; Septiembre 2000; Volumen 3 página 471.
[7] IEEE Spectrum Febrero 1994; *Vital Signs of Identity*; IEEE; Estados Unidos; páginas 22 y 25.
[8] PC Plus Marzo 2000; *Sistemas de Reconocimiento Digital*; PC Plus; página 56.
[9] Short B.; *Bob's biometric fingerprint primer*; Noviembre 2002; http://www.technologyreports.net/securefrontiers/index.html?articleID=897
[10] Goméz H., Ormella C.; *Autenticación Biométrica*; Revista LAN &WAN, numero 81; http://www.angelfire.com/la2/revistalanandwan