UNIVERSIDAD DE CÓRDOBA

ESCUELA POLITÉCNICA SUPERIOR
INGENIERÍA TÉCNICA EN INFORMÁTICA DE SISTEMAS
PROYECTO FIN DE CARRERA

MARCAS DE AGUA EN IMÁGENES DIGITALES

AUTOR: RAÚL PÉRULA MARTÍNEZ

DIRECTORA: ÁNGELA ROJAS MATAS

ÍNDICE

ÍNDICE

1. Introducción

¿Qué es el marcado digital o watermarking?

- Es una técnica de ocultación de información que forma parte de las conocidas como esteganográficas.
- Las marcas de agua digitales pretenden proteger los derechos de autor. Pueden ser visibles o invisibles. En este estudio sólo se tratarán las invisibles.

¿Para qué se utilizan?

- La identificación de propiedad intelectual o copyright
- Protección de múltiples copias no autorizadas
- Aplicaciones médicas

1. Introducción

¿Cuándo tiene éxito el marcado de una imagen digital?

Cuando se cumplen las siguientes características:

- Robustez de la marca de agua (baja cantidad de errores).
- Calidad de la imagen receptora (alto valor del PSNR, que es un tipo de métrica que muestra una medida aproximada de la modificación que sufre la imagen).
- Resistencia a posibles ataques.
- Una buena clave secreta de ocultación.

ÍNDICE

2. Objetivos

- El objetivo principal es:
  - Realizar un estudio, análisis e implementación de las diferentes técnicas de inserción y extracción de marcas de agua digitales propuestas en artículos de investigación recientemente publicados.

- Entre estas técnicas se distinguirán tres tipos:
  - Las del dominio espacial.
  - Las del dominio de las frecuencias.
  - Otros dominios.

ÍNDICE

3. Restricciones

Estrategia usada:

- Sistema operativo Windows
- Matlab 7.6 (R2008a)
- Imágenes en formato Windows Bitmap (.bmp)
- Para la documentación:
  - Microsoft Word 2007

ÍNDICE

3.1. Tipos de algoritmos

- Dominio Espacial (tratan la imagen directamente):
  - Método Basado en Correlación.
  - Algoritmo de Cox.
  - Método del Bit Menos Significativo (LSB).
- Dominio de las Frecuencias (realizan una transformada):
  - Transformada Discreta del Coseno (DCT).
  - Acceso Múltiple por División de Código (CDMA).
  - Transformada Discreta Wavelet (DWT).
- Otros dominios (otro tipo de métodos):
  - Descomposición en Valores Singulares (SVD).
  - Métodos basados en Secuencias Caóticas.
  - Métodos basados en Análisis de Componentes Principales (PCA).

3.2. Algoritmo basado en la Descomposición en Valores Singulares (SVD)

- La SVD es una técnica del Álgebra Lineal usada para diagonalizar matrices en análisis numérico.

- La SVD se define como:

$$A = USV^t$$

donde U y V son matrices ortogonales y S es una matriz diagonal.

3.2. Algoritmo basado en la Descomposición en Valores Singulares (SVD)

- Estructura de la marca de agua
  - La marca de agua con dimensiones MxN es una secuencia pseudoaleatoria de números pertenecientes a una normal N(0,1), con media 0 y varianza 1.

Ejemplo: (-0.6436 1.6924)

(0.5077 0.5913)

  - La imagen portadora será una imagen en escala de grises de dimensiones Mx

3.2. Algoritmo basado en la Descomposición en Valores Singulares (SVD)

- Proceso de ocultación:
  - Se añade una marca de agua W (también representada como una matriz) en la matriz S.
  - Se realiza la SVD en la nueva matriz $S + \alpha W$ para obtener U_W, S_W, y V_W ($S + \alpha W = U_W S_W V_W^T$), donde la constante positiva es el factor de escala que controla la fuerza con la que va a ser insertada la marca de agua.
  - Se obtiene la imagen marcada A_W por la multiplicación de las matrices U, S_W, y V^T.

3.2. Algoritmo basado en la Descomposición en Valores Singulares (SVD)

- Proceso de ocultación:
  - Siendo:
    - A la imagen original.
    - W la marca de agua.
  - Se obtendrá la imagen marcada A_W mediante los siguientes pasos:

$$A \Rightarrow USV^T$$

$$S + \alpha W \Rightarrow U_W S_W V_W^T$$

$$A_W \Leftarrow US_W V^T$$

3.2. Algoritmo basado en la Descomposición en Valores Singulares (SVD)

- Proceso de extracción:
  - Dadas las matrices U_W, S, V_W.
  - Y la imagen marcada A_W^*.
  - Se extrae la marca de agua W^* haciendo la operación inversa al proceso de marcado.

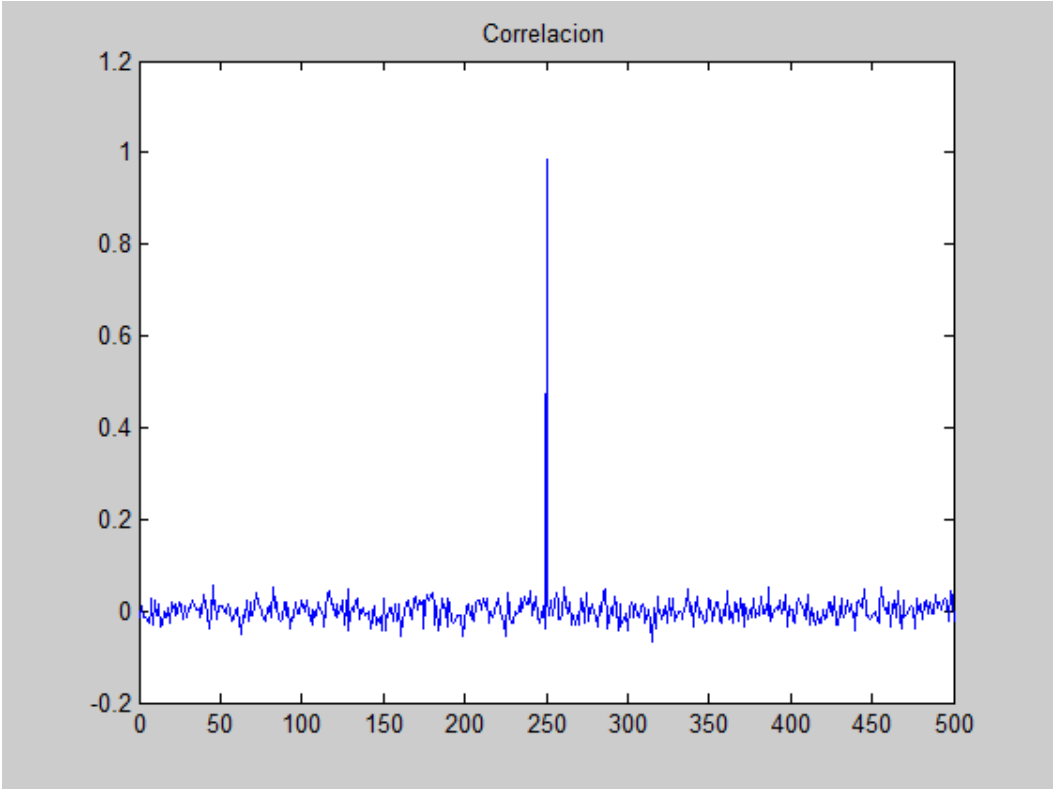
$$A_W^* \Rightarrow U^* S^*_W V^{*T}$$

$$D^* \Leftarrow U_W S^*_W V_W^T$$

$$W^* \Leftarrow (1/\alpha)(D^* - S)$$

3.2. Algoritmo basado en la Descomposición en Valores Singulares (SVD)

- Proceso de extracción:
  - Para comprobar que la extracción de la marca de agua es buena o mala se realizará el gráfico de correlaciones.



ÍNDICE

5. Pruebas y ataques

Se ha realizado dos tipos de pruebas:

1. Primero se ha hecho un estudio individual de cada algoritmo:
   - Se comprobó como se comportaba el algoritmo en función de los parámetros de los que dependía.
   - La calidad de la imagen marcada (PSNR).
   - La imagen que se extraía como marca de agua o el gráfico de similaridad o correlación entre las secuencias pseudoaleatorias.
   - El número de errores que existía en la extracción de la marca con respecto a la original.

5. Pruebas y ataques

2. Una vez obtenidos los datos de las pruebas individuales se procedió a las pruebas comunes o de comparación entre los algoritmos:

- Estudio común entre los algoritmos que son comparables.
- Estudio de los tiempos de computación que tiene cada algoritmo.
- Estudio comparativo de resistencia a los ataques.

5. Pruebas y ataques

Para comprobar la efectividad de los algoritmos propuestos por los autores, a las imágenes marcadas se les realizó una serie de ataques para ver qué resistencia tienen a éstos cuando se extrae la marca.

Los ataques que se realizaron:

- Compresión JPEG
- Inserción de ruido gaussiano (ruido muy común)
- Aplicación de un filtro de paso bajo basado en la media (suavizado)
- Recortado de la imagen marcada
- Escalado de la imagen marcada (doble tamaño)
- Rotación de la imagen marcada (90º)

ÍNDICE

6. Ejemplo

Para ver las salidas que se han obtenido en las pruebas se va a realizar un ejemplo con una interfaz gráfica básica donde se podrá observar los resultados obtenidos.

Se podrá observar:

- La imagen de cobertura u original
- La marca de agua original
- La imagen marcada
- La marca de agua extraída
- El PSNR de la imagen marcada
- El número de errores entre marcas

ÍNDICE

7. Resultados y Conclusiones

Dos tipos de resultados:

- Resultados obtenidos del estudio de cada algoritmo.
- Resultados obtenidos del estudio común.

Resultados obtenidos de cada algoritmo:

- Se ha comprobado el comportamiento que tenían los algoritmos a la variabilidad de los parámetros de los que dependían.
- Y se han obtenido resultados de la resistencia o no de los algoritmos a los ataques.

7. Resultados y Conclusiones

Resultados obtenidos del estudio común:

- Se ha comparado los tiempos de ejecución que ofrecen los diferentes algoritmos observando cuál es más rápido y cuál más lento.
- Se ha comparado los tipos de algoritmos que se han estudiado viendo cuales necesitan algo para la extracción junto con lo que necesitan y cuales no necesitan nada.
- Se ha comparado la resistencia a los ataques realizados entre los diferentes algoritmos llevados a estudio.

7. Resultados y Conclusiones

Comparativa de los tiempos de ejecución:

	Tiempo Inserción	Tiempo Extracción
Técnicas basadas en correlación	0.2433 seg.	0.3182 seg.
	0.2433 seg.	0.1653 seg.
Cox	0.5241 seg.	0.3775 seg.
DCT	1.5756 seg.	0.8205 seg.
DCT y Correlación	1.5101 seg.	1.3556 seg.
CDMA	2.7534 seg.	4.6816 seg.
CDMA en el dominio wavelet	12.2492 seg.	21.3752 seg.
DWT y la transformada de Haar	3.0654 seg.	0.3370 seg.
DWT basado en la paridad	0.6256 seg.	0.3869 seg.
SVD	0.8752 seg.	0.5023 seg.
SVD con la transformada de Arnold	17.5439 seg.	16.4690 seg.
SVD basado en el intercambio de valores	0.9688 seg.	0.9079 seg.
SVD basado en el orden de los coeficientes	0.2668 seg.	0.2200 seg.
SVD basado en la proximidad a un intervalo	0.3822 seg.	0.2668 seg.
LSB	0.6895 seg.	0.4914 seg.
Secuencias Caóticas	0.3962 seg.	1.6864 seg.
Secuencias Caóticas y DCT	1.3541 seg.	0.6895 seg.
	0.5569 seg.	0.2964 seg.
PCA	1.8143 seg.	1.6115 seg.
PCA para construir la imagen de referencia	1.5803 seg.	0.9797 seg.

7. Resultados y Conclusiones

- Conclusiones para los tiempos de ejecución:
  - La mayoría de los algoritmos rondan entre el medio segundo y los dos segundos de tiempo de ejecución.
  - Las **inserciones** suelen ser **más lentas** que las **extracciones**, predominando en las extracciones los tiempos de ejecución por debajo del segundo.
  - El algoritmo **más rápido**, ya sea en la inserción o extracción, es el algoritmo de **técnicas basadas en correlación**, en concreto el algoritmo modificado.
  - El algoritmo **más lento** en realizar la **inserción** es el algoritmo **SVD con la transformada de Arnold** y en la **extracción** es el algoritmo **CDMA en el dominio wavelet**.

7. Resultados y Conclusiones

Comparativa de los tipos de algoritmos:

			Requiere		
	Blind	Semiblind	Imagen original	Marca original	Parámetros
Técnicas basadas en correlación	X		NO	NO	NO
Cox		X	SI	NO	NO
DCT	X		NO	NO	NO
DCT y Correlación	X		NO	NO	NO
CDMA	X		NO	NO	NO

7. Resultados y Conclusiones

- Conclusiones para los tipos de algoritmos:
  - **La mayoría** de los algoritmos realizan la extracción **sin utilizar nada adicional** (blind o a ciegas).
  - **Ninguno** utiliza la imagen **y** la marca de agua originales para la **extracción**, con lo que esto dice mucho de la calidad de los algoritmos.
  - **Solamente tres** necesitan de la imagen **o** la marca de agua originales para la **extracción**, **dos** necesitan de la **imagen original** y **uno** de la **marca de agua original.**
  - Sólo **cinco** hacen uso de alguna variable o parámetro adicional (semiblind).

7. Resultados y Conclusiones

Comparativa de la resistencia a los ataques:

	Resistencia a ataque					
	JPEG	**Ruido**	**Filtro**	**Recortado**	**Escalado**	**Rotación**
Técnicas basadas en correlación	NO	SI	NO	NO PERMITE	NO PERMITE	SI
Cox	SI	SI	SI	NO PERMITE	NO	NO
DCT	NO	NO	NO	NO PERMITE	NO	NO
DCT y Correlación	SI	NO	NO	NO PERMITE	NO	NO
CDMA	SI	SI	NO	NO	NO	NO

7. Resultados y Conclusiones

- Conclusiones de resistencia a ataques:
  - El ataque al cual un algoritmo es **más vulnerable** es el **filtro de paso bajo basado en la media**.
  - Los algoritmos son **más resistente** a la **compresión JPEG**.
  - El ataque que **no se puede aplicar** en la mayoría de los casos por culpa del algoritmo es el **recortado**.
  - El algoritmo que **más ataques ha superado** ha sido el **algoritmo de Cox**. Este método tiene **alta probabilidad** de mejorarse en el caso de una **futura aplicación real**.

ÍNDICE

8. Futuras mejoras

- Algoritmos:
  - Nuevos algoritmos
  - Trabajar con imágenes en colores, ya sea para las imágenes de cobertura o las marcas de agua
  - Trabajar con otros tipos de ficheros digitales (audio, video…)
- Programa:
  - Realizar un programa que reúna todos los algoritmos estudiados
- Interfaz:
  - Realizar una interfaz gráfica para el programa propuesto

Bibliografía

- Shoemaker, C. Hidden Bits: A Survey of Techniques for Digital Watermarking, Union College, Schenectady, NY, 2002, última visita 23-Julio-2009, http://www.vu.union.edu/~shoemakc/watermarking/.
- Godoy, M.; Mignola, C. Marcas de Agua (Watermarking) en Imágenes, Aplicadas en el Dominio Espacial Basadas en Correlación, 2004, última visita 23-Julio-2009, http://cpdsi-fich.wdfiles.com/local--files/tpsaplicacion/2004_GodoyMignola-WatermarkingCorrelacion.pdf
- Cox, I.J.; Kilian, J.; Leighton, F.T.; Shamoon, T. Secure Spread Spectrum Watermarking for Multimedia, IEEE, Volume: 6, Issue: 12-Dec-1997, Page(s): 1673-1687.
- Maity, Santi P.; Kundu, Malay K. A Blind CDMA Image Watermarking Scheme in Wavelet Domain, 2004, última visita 24-Julio-2009, http://www.isical.ac.in/~malay/Papers/Conf/ICIP%2704_1595.pdf
- Jiang-Lung Liu; Der-Chyuan Lou; Ming-Chang Chang; et al. A Robust Watermarking Scheme Using Self-reference Image, ScienceDirect, Computer Standards & Interfaces, Volume: 28, Issue: 3-Jan-2006, Page(s): 356-367.
- Ruizhen Liu; Tieniu Tan. A SVD-Based Watermarking Scheme for Protecting Rightful Ownership, IEEE, IEEE Transactions on Multimedia, Volume: 4, Issue: 1-Mar-2002, Page(s): 121-128.
- Roman Rykaczewski. Comments on “An SVD-Based Watermarking Scheme for Protecting Rightful Ownership”, IEEE, IEEE Transactions on Multimedia, Volume: 9, Issue: 2, Page(s): 421-423.
- Deyun Peng; Jiazhen Wang; Sumin Yang; et al. CDMA Based Multiple-User Digital Watermarking, IEEE, International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2006. IIH-MSP '06. Dec-2006, Page(s): 75 – 78.
- Yan Xing; Jieqing Tan. A Color Watermarking Scheme Based on Block-SVD and Arnold Transformation, IEEE, Second Workshop on Digital Media and its Application in Museum & Heritages, 10-12 Dec-2007, Page(s): 3 – 8.
- Belkacem, S.; Dibi, Z.; Bouridane, A. Color Image Watermarking based on Chaotic Map, IEEE, 14th IEEE International Conference on Electronics, Circuits and Systems, 2007. ICECS 2007, 11-14 Dec-2007, Page(s): 343 – 346.
- Chin-Chen Chang; Piyu Tsai; Chia-Chen Lin. SVD-based digital image watermarking scheme, ScienceDirect, Pattern Recognition Letters, Volume: 26, Issue: 10-15 Jul-2005, Page(s): 1577-1586.
- B.Chandra Mohan, S. Srinivas Kumar. A Robust Image Watermarking Scheme using Singular Value Decomposition, Journal Of Multimedia, Vol. 3, No. 1, May-2008.
- Chrysochos, E.; Fotopoulos, V.; Skodras, A. N. Robust Watermarking of Digital Images Based on Chaotic Mapping and DCT, 2008, última visita 04-Agosto-2009, http://www.eurasip.org/Proceedings/Eusipco/Eusipco2008/papers/1569104383.pdf
- Thai D Hien; Yen-Wei Chen; Zensho Nakao. PCA Based Digital Watermarking, SpringerLink, Knowledge-Based Intelligent Information and Engineering Systems, Volume: 2773/2003, 2003, Page(s): 1427-1434.
- Mirza, H.H.; Thai, H.D.; Nagata, Y.; et al. Digital VideoWatermarking Based on Principal Component Analysis, IEEE, Second International Conference on Innovative Computing, Information and Control, 2007. ICICIC '07. 5-7 Sep-2007, Page(s): 290 – 290.
- Erkan Yavuz; Ziya Telatar. Digital Watermarking with PCA Based Reference Images, SpringerLink, Advanced Concepts for Intelligent Vision Systems, Volume: 4678/2007, 2007, Page(s): 1014-1023.

UNIVERSIDAD DE CÓRDOBA

ESCUELA POLITÉCNICA SUPERIOR
INGENIERÍA TÉCNICA EN INFORMÁTICA DE SISTEMAS
PROYECTO FIN DE CARRERA

MARCAS DE AGUA EN IMÁGENES DIGITALES

AUTOR: RAÚL PÉRULA MARTÍNEZ

DIRECTORA: ÁNGELA ROJAS MATAS