Digital Images Analysis

Avid Roman-Gonzalez

Análisis de imágenes digitales

Digital images analysis

Avid Roman Gonzalez

TELECOM ParisTech, 46 rue Barrault, 75013 – Paris, Francia
German Aerospace Center – DLR, Remote Sensing Institute, Oberpfaffenhofen 82234 Wessling, Germany
Centre National d'Etudes Spatiales – CNES, Francia

RESUMEN

Un campo específico del procesamiento de imágenes se enfoca en la evaluación de la calidad de la imagen y en la evaluación de su autenticidad. Una pérdida de la calidad de la imagen puede deberse a los diferentes procesos por los cuales pasa. Dentro de la evaluación de la autenticidad de la imagen tenemos la detección de falsificaciones, detección de mensajes ocultos, etc.
En este trabajo mostraremos una vista general sobre estas áreas que tienen en común la necesidad de desarrollar teorías y técnicas para detectar cambios en la imagen que se notan muy poco o casi nada de manera visual.
La mayoría de estos métodos utiliza la información mutual como base para el análisis de la imagen. Las imágenes satelitales están afectadas por artefactos, el artefacto tiene una característica muy parecida a los comentados anteriormente, un artefacto es un desorden que casi no se puede observar visualmente.
Descriptores: *imágenes, marca de agua, información oculta, manipulación de imágenes, falsificación.*

ABSTRACT

A specific field of image processing focuses on the evaluation of image quality and assessment of their authenticity. A loss of image quality may be due to the various processes by which it passes. In assessing the authenticity of the image we detect forgeries, detection of hidden messages, etc.
In this work, we present an overview of these areas; these areas have in common the need to develop theories and techniques to detect changes in the image that it is not detectable of visual way. Most of these methods use mutual information as a basis for image analysis.
The satellite images are affected by artifacts, the artifact has a very similar characteristics to those mentioned above, an artifact is a disorder that almost cannot visually observe.
Keywords: *images, watermarking, hidden information, image manipulation, fakery.*

INTRODUCCIÓN

Cuando se trabaja con imágenes digitales, una tarea importante pero no muy fácil es conocer la calidad y autenticidad de dicha imagen. La calidad de una imagen se puede degradar debido a los diferentes procesos por el cual pasa antes de llegar al usuario final, estos procesos pueden ser la compresión, descompresión, redimensionamiento, filtrado, resaltado de colores, etc. Cada uno de estos procesos puede distorsionar la imagen y produce cambios en ella, estos cambios afectan la estadística y la información de la imagen.

Los cambios en una imagen no solo pueden ser de manera casual, sino también pueden ser cambios intencionados como por ejemplo para introducir datos de derecho de autor con técnicas de watermarking; o introducir información oculta con técnicas de esteganografia. En este punto existen varios grupos dedicados a la investigación en temas relacionados, existe el grupo de los que desarrollan métodos de watermarking, también está el grupo de los que desarrollan métodos para detectar watermarking, existe el grupo de los que desarrollan técnicas para poner información oculta en las imágenes y el grupo que desarrolla métodos para detectar la información oculta.

Por otro lado también tenemos la falsificación de imágenes donde por distintos motivos se aumentan o eliminan personas u objetos de una fotografía y existen grupos que se dedican a desarrollar métodos para la detección de imágenes falsificadas.

Dentro de todos estos campos descritos líneas arriba, lo más importante es poder detector los cambios en la imagen, esas alteraciones en la estadística u otros factores que pueden ser indicadores de distorsión o manipulación de la imagen.

Las imágenes satelitales de observación terrestre son afectadas por artefactos, estos artefactos producidos por procesos de pre-procesamiento o por condiciones del mismo sensor, son elementos estructurados que distorsionan la información de la imagen satelital, estos artefactos tienen las mismas características que las alteraciones descritas anteriormente por lo que se pueden utilizar técnicas de esteganalisis, detección de falsificación de imágenes o técnicas de evaluación de la calidad para la detección de dichos artefactos, es así que en la figura 1 mostramos un esquema de cómo todos estos campos pueden converger en la detección de artefactos.

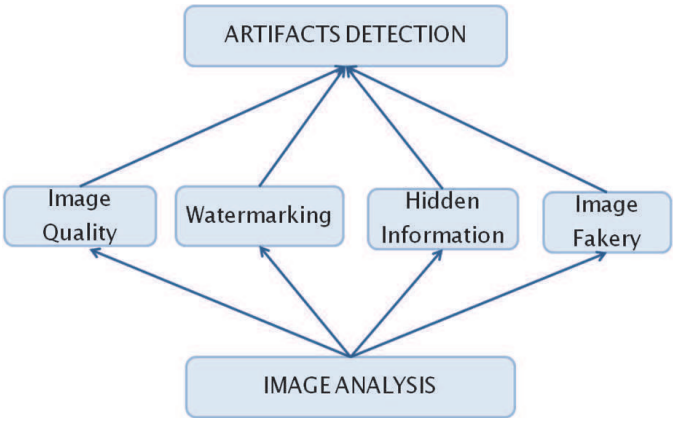


Figura 1 Esquema relacional entre los métodos de análisis de imágenes

CALIDAD DE LA IMAGEN

Las imágenes digitales están siempre sujetas a una variedad de distorsiones y modificaciones durante los procesos de compresión, transmisión, reproducción, etc.

Para tener el control y alguna posibilidad de mejorar la calidad de la imagen, es importante poder medir e identificar la calidad y la degradación de calidad en nuestros datos.

Los trabajos de investigación relacionados con la evaluación de la calidad de imágenes, tienen como objetivo el desarrollo de métodos y algoritmos que puedan evaluar de manera automática la calidad de una imagen [1][2][3][4]. Para lograr este propósito, algunos métodos utilizan medidas de comparación frente a una referencia. En ese sentido tenemos 3 enfoques: el enfoque “full-reference”(FR), el enfoque “non-reference”(NR) y el enfoque “reduced reference”(RR).

A. Full-Reference (FR)

Este método requiere acceder completamente a la imagen original como referencia. Se basa en la siguiente filosofía:

Señal Distorsionada = Señal de Referencia + Error

Asumimos que la señal de referencia tiene una calidad perfecta y lo que cuantificamos en el error de percepción visual.

B. Non-Reference (NR)

En este enfoque no se requiere ningún acceso a la imagen original, pero la evaluación de la calidad sin referencia es una tarea muy difícil, se han hecho algunos trabajos para la evaluación de distorsiones específicas.

Señal Distorsionada = Señal de Referencia + Error

Asumimos que la señal de referencia tiene una calidad perfecta y lo que cuantificamos en el error de percepción visual.

C. Reduced-Reference (RR)

Este enfoque no requiere un acceso total a la imagen original pero necesita de alguna información parcial de referencia como por ejemplo un juego de características extraídas.

D. Métricas para la evaluación de la calidad de la imagen

En la literatura se puede observar que se han desarrollado numerosas métricas para poder realizar la comparación y por ende una evaluación de la calidad entre una imagen y su referencia. Algunas medidas métricas para evaluar la calidad de una imagen utilizando el enfoque full-reference y que han sido evaluadas en [4] son las siguientes:

- PSNR: Trabaja solamente con la componente de luminancia.
- Samof JND Metrix: Trabaja con imágenes a color.
- DCTune: Diseñado originalmente para una optimización del JPEG. Trabaja con imágenes a color.
- PQS: Trabaja solamente con la componente de luminancia.
- NQM: Trabaja solamente con la componente de luminancia.
- Fuzzy S7: Trabaja solamente con la componente de luminancia.
- BSDM: Trabaja con imágenes a color.
- Multiscale SSIM: Trabaja solamente con la componente de luminancia.
- IFC: Trabaja solamente con la componente de luminancia.
- VIF: Trabaja solamente con la componente de luminancia.

Cada una de estas métricas trabaja de mejor o peor manera frente a distorsiones específicas, mientras algunas pueden ser mejores con algún tipo de distorsión, pues no son tan bueno frente a otras variaciones. Una de las métricas más conocidas es el PSNR (peak signal to noise ratio), esta medida puede mostrar algunos resultados no muy coherentes frente a un ejemplo simple: Si a una imagen le aumentamos una cantidad igual de ruido pero en diferentes secciones, tenemos resultados distintos con diferencia en la calidad de la imagen tras una evaluación visual tal como se muestran en la figura 2:

Figura 2 Dos imagines con el mismo PSNR. La misma cantidad de ruido ha sido agregada en las áreas rectangulares, en la parte de arriba (izquierda) y en la parte de abajo (derecha) de estas imágenes

Ambas imágenes tienen la misma cantidad de ruido, pero claramente se puede observar que de manera visual la imagen de la derecha es de mejor calidad que el de la izquierda, debido a que el ruido es más notorio en esta última.

E. Quality-Aware Images

Método propuesto en [1], es un método de evaluación de la calidad de la imagen reduced-reference (RR) basado en la extracción de ciertas características de la imagen original y embeberlo como información oculta dentro de la misma imagen para su posterior evaluación; se espera que estas características se mantengan después de los diferentes procesos por las cuales puede pasar la imagen como por ejemplo compresión, descompresión, filtrado, etc.

El proceso empieza en el transmisor, donde primero se extrae las características, luego estas características son embebidas dentro de la misma imagen. La imagen puede llegar al receptor después de algunos procesos de distorsión. En el lado del receptor se decodifica las características embebidas y se extrae las características de la imagen recibida para finalmente hacer una comparación entre ambos conjuntos de características. El proceso completo se puede observar en la figura 3.

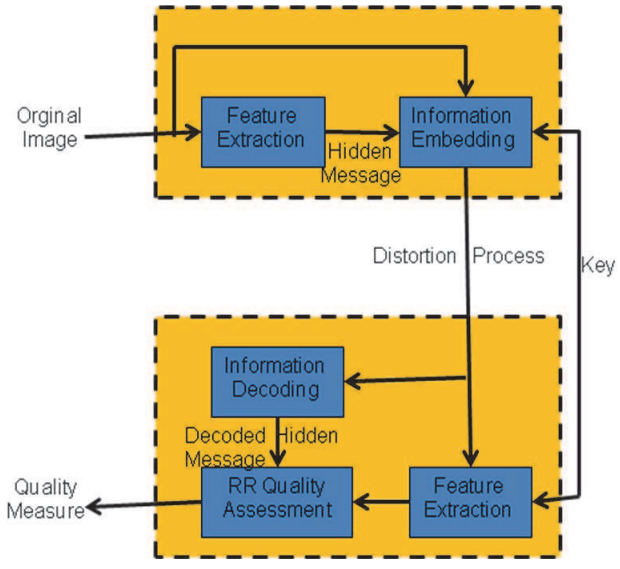


Figura 3 Proceso para Quality-Aware Images

El proceso de extracción de características empieza con la aplicación de la transformada wavelets, se selecciona algunos coeficientes wavelets, estimamos los parámetros y finalmente se realiza una cuantificación. El proceso de extracción de características se puede observar en la figura 4.

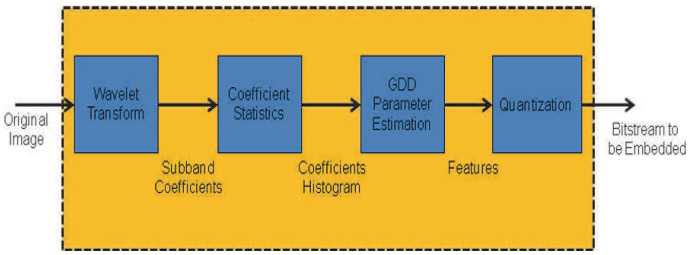


Figura 4 Extracción de características

Para embeber las características dentro de la misma imagen, primero aplicamos la transformada wavelet, seleccionamos algunos coeficientes para poder hacer una nueva cuantificación en función de las características extraídas para finalmente aplicar la transformada inversa. En la figura 5 se muestra el proceso de embebido de las características.

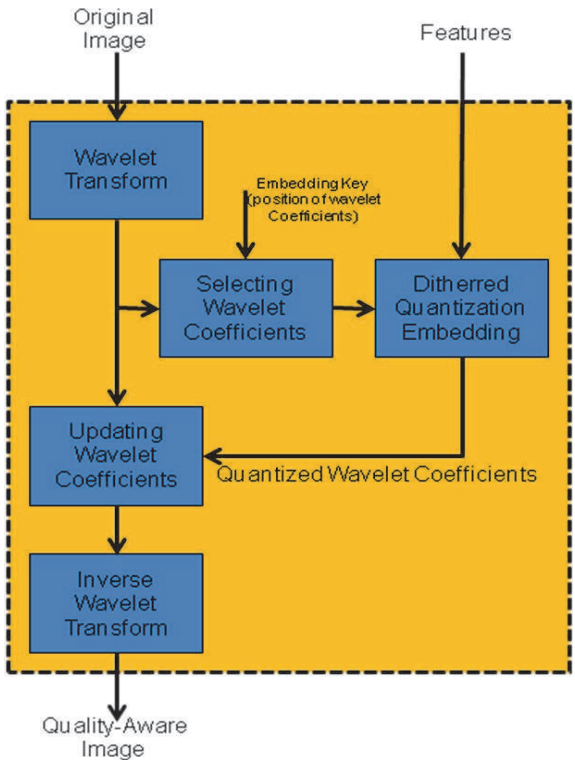


Figura 5 Proceso de embebido

WATERMARKING

Es una técnica cuyo objetivo principal es poner de manifiesto el uso ilícito de un cierto servicio digital por parte de un usuario no autorizado. Concretamente, esta técnica consiste en insertar un mensaje (oculto o no) en el interior de un objeto digital, como podrían ser imágenes, audio, vídeo, texto, software, etc. Dicho mensaje es un grupo de bits que contiene información sobre el autor o propietario intelectual del objeto digital tratado.

Existen varias técnicas de watermarking, se puede considerar marcas visibles y no visibles.

Para insertar una marca visible podemos seguir los siguientes pasos: denotamos a la imagen original como *f*, la marca como *w*, y la imagen marcada como f_w; finalmente aplicamos el siguiente proceso:

$$f_w = (1-\alpha) f + \alpha w$$

Dónde: α es una constante de visibilidad de la marca.

En la figura 6 podemos observar unos ejemplos de watermarking visible.

Figura 6 Marcas visibles

Si deseamos introducir una marca no visible, pues esta no será distinguible de manera visual, pero será posible detectarla o recuperarla utilizando códigos y algoritmos orientados a dicho fin. La invisibilidad es asegurada por la inserción de información redundante.

Por ejemplo podemos insertar la marca en los 2 últimos bits menos significativos de la imagen de acuerdo con:

$$f_w = 4(\frac{f}{4}) + \frac{w}{64}$$

Un esquema general de las técnicas de watermarking se muestra en la figura 7.

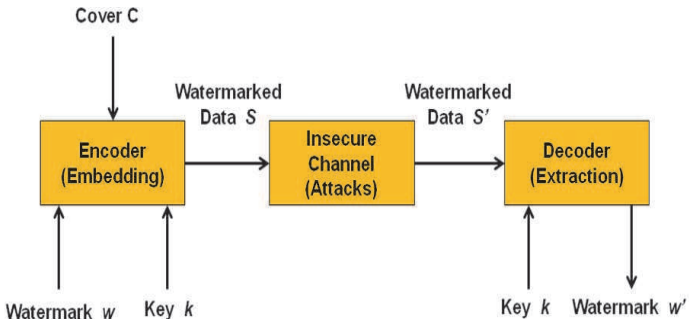


Figura 7 Técnica de watermarking

ESTEGANOGRAFIA

La estenografía consiste en técnicas de ocultamiento de información, existen muchos trabajos relacionados al ocultamiento de la información así como a la detección de información oculta [5][6][7][8][9]. El problema de la información oculta se traduce en lo siguiente: Tener un mensaje *M* que puede ser embebido en un dato *S* y como resultado dar *X*, este *X* puede ser sujeto a diversos procesos e intentos de ataque. Este proceso se muestra en la figura 8.

Un sistema de ocultamiento de información debe cumplir 2 requerimientos: *X* debe ser muy similar a *S*; y el mensaje *M* oculto debe sobrevivir a distintos procesos (compresión, redimensionamiento, etc.).

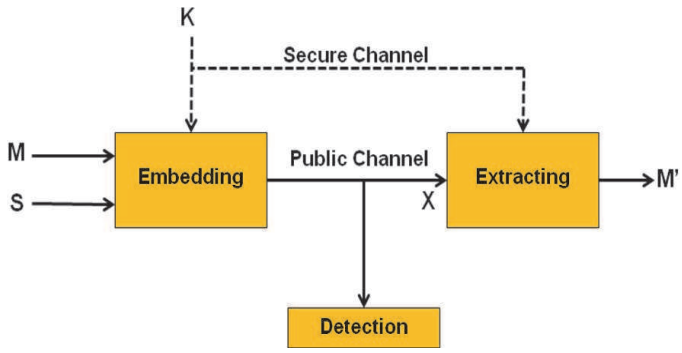


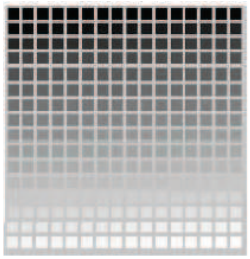
Figura 8 Esquema general para la estenografía

Si deseamos insertar información oculta en una imagen, pues debemos recordar que una imagen es una matriz de números, donde cada número codifica a un color:

- RGB 24 bits:
  00 00 00 00 00 00 00000000 00000000 00000000

  FF FF FF 255 255 255 11111111 11111111 11111111

- Escala de grises 8 bits:
  Numero de 0 a 256



Una técnica muy conocida para insertar mensajes en una imagen es la utilización del bit menos significativo LSB como portador de la información tal como se muestra en el siguiente ejemplo:

Si tenemos los siguientes pixeles originales:

(11101101 00100100 10100001)

(00001111 00101101 11101111)

(00001111 00100111 10000111)

Deseamos insertar el mensaje : ‘A’ (10010111)

Los nuevos pixeles serán:

(11101101 00100100 10100000)

(00001111 00101100 11101111)

(00001111 00100111 10000111)

A. Esteganalisis usando métricas de calidad de imagen

Esteganalisis es el proceso por el cual se analiza una imagen y se determina si contiene o no información oculta. Este método es propuesto en [5] es una técnica de esteganalisis basada en la comparación de una imagen con el resultado de aplicar a la misma imagen un filtro gaussiano, esta comparación se realiza utilizando métricas de calidad de imagen.

Para definir el proceso de análisis primero definimos la nomenclatura, Cover Signal es la imagen que no contiene información oculta, Stego Signal es la imagen que contiene información oculta. En la figura 9 podemos observar el proceso del método bajo descripción.

La extracción de características se realiza mediante la comparación de la imagen original y la imagen después de un filtro gaussiano, esta comparación se realiza mediante métricas de calidad de imagen, el conjunto de estas métricas viene a ser el vector de características. Finalmente con estos vectores de características tanto para imágenes con y sin información oculta, pues realizamos un entrenamiento para poder identificarlas.

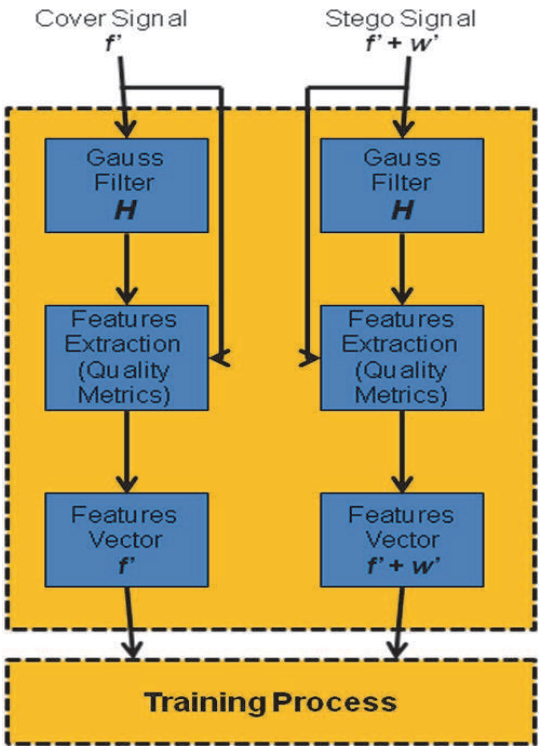


Figura 9 Esquema descriptivo del proceso de esteganalisis

Las métricas que se utilizan para la aplicación de este método son: Mean Absolute Error (*M1*), Mean Square Error (*M2*), Czekanowski Distance (*M3*), Angular Correlation (*M4*), Image Fidelity (*M5*), Normalized Cross-Correlation (*M6*) and Spectral Magnitude Distortion (*M7*).

$$M_1 = \frac{1}{K}\sum_{k=1}^{K}\left\{\frac{1}{N^2}\sum_{i,j=0}^{N-1}\left|C_k(i,j) - \bar{C}_k(i,j)\right|\right\}$$

$$M_2 = \frac{1}{K}\sum_{k=1}^{K}\left\{\frac{1}{N^2}\sum_{i,j=0}^{N-1}\left|C_k(i,j) - \bar{C}_k(i,j)\right|^2\right\}^{1/2}$$

$$M_3 = \frac{1}{N^2}\sum_{i,j=0}^{N-1}\left(1 - \frac{2\sum_{k=1}^{K}\min\left(C_k(i,j), \bar{C}_k(i,j)\right)}{\sum_{k=1}^{K}\left(C_k(i,j) + \bar{C}_k(i,j)\right)}\right)$$

$$M_4 = 1 - \frac{1}{N^2}\sum_{i,j=1}^{N}\frac{2}{\pi}\cos^{-1}\frac{C(i,j).\bar{C}(i,j)}{\left\|C(i,j)\right\|\left\|\bar{C}(i,j)\right\|}$$

$$M_5 = 1 - \left(\frac{1}{K}\sum_{k=1}^{K}\frac{\sum_{i,j=0}^{N-1}\left[C_k(i,j) - \bar{C}_k(i,j)\right]^2}{\sum_{i,j=0}^{N-1}C_k(i,j)^2}\right)$$

$$(u,v) = \sum_{m,n=0}^{N-1}C_k(m,n)\exp\left[-2\pi i m\frac{u}{N}\right]\exp\left[-2\pi i n\frac{v}{N}\right]$$

$$M_7 = \frac{1}{KN^2}\sum_{k=1}^{K}\sum_{u,v=0}^{N-1}\left\|\Gamma_k(u,v)\right| - \left|\bar{\Gamma}_k(u,v)\right\|^2$$

MANIPULACION DE IMAGENES

El arte de falsificar imágenes tiene una historia larga, y hoy en día que es la era digital es posible realizar cambios en la información representada de manera muy fácil sin dejar rastros de la manipulación. En las siguientes figuras podemos ver algunos ejemplos de falsificación de imágenes.

Figura 10 Algunos ejemplos de imágenes manipuladas [14]

Existen métodos para la detección de imágenes falsificadas como los descritos en [10][11][12][13][14]. Algunos de estos métodos se basan en los siguientes principios:

- Regiones duplicadas.
- Interpolación y remuestreo.
- Inconsistencias en el color.
- Inconsistencias en el ruido.
- Inconsistencias en el Color Filter Array (CFA).
- Inconsistencias en la iluminación.

La detección de inconsistencias en la iluminación es muy importante y permite detectar la manipulación de imágenes, algunos ejemplos de inconsistencias con la iluminación se muestran en la figura 11.

a) b)

Figura 11 Inconsistencias en la iluminación: a) fotografía manipulada, b) fotografía original

CONCLUSIONES

Todos estos enfoques para el análisis de imágenes pueden converger en la detección de artefactos, ya que la presencia de marcas de agua, la presencia de información oculta o la presencia de alteraciones en regiones de la imagen, produce cambios en la imagen original, estos cambios no son visible y son alteraciones en la estadística de la imagen o en otro factor.

La mayoría de los métodos dentro de estas áreas, utilizan la información mutual para poder hacer el análisis de la calidad y autenticidad de la imagen.

Por esta razón, se puede hacer la conjunción de estos métodos de evaluación y detección para poder implementar un método libre de parámetros para la detección de artefactos.

REFERENCIAS

[1] Z. Wang, G. Wu, H. R. Sheikh, E. P. Simoncelli, E. Yang, A. C. Bovik; “Quality-Aware Images”; IEEE Transaction on Image Processing.

[2] H. R. Sheikh, A.C. Bovik; “Image Information and Visual Quality”; IEEE Transaction on Image Processing, vol. 15, N°2, Feb. 2006, pp. 430-444.

[3] U. Rajashekar, A. C. Bovik, L. K. Cormack; “Visual Search in Noise: Revealing the Influence of Structural Cues by Gaze-contingent Classification Image Analysis”; Journal of Vision 2006.

[4] H. R. Sheikh, M. F. Sabir, A. C. Bovik; “A Statistical Evaluation of Recent Full Reference Image Quality assessment Algorithms”; IEEE Transaction on Image Processing, vol 15, N°11, Nov. 2006, pp. 3441-3452.

[5] I. Avcibas, N. Memon, B. Sankur; “Steganalysis Using Image Quality Metrics”; IEEE Transaction on Image Processing, vol. 12, N°2, Feb. 2003, pp. 221-229.

[6] P. Moulin, J. A. O’Sullivan; “Information-Theoretic Analysis of Information Hiding”; IEEE Transaction on Information Theory, vol. 49, N°3, Mar. 2003, pp. 563-593.

[7] C. Cachin; “An Information-Theoretic Model for Steganography”; Information and Computation, Mar. 2004.

[8] S. Lyu, H. Farid; “Steganalysis Using Higher-Order Image Statistics”; IEEE Transaction on Image Forensics and Security, vol. 1, N°1, Mar. 2006, pp. 111-119.

[9] K. Suvillan, U. Madhow, S. Chandrasekaran, B. S. Manjunath; “Steganalysis for Markov Cover Data with Applications to Images”; IEEE Transaction on Information Forensics and Security, vol. 1, N°2, Jun. 2006, pp. 275-287.

[10] H. Farid, “Image Forgery Detection”, IEEE Signal Processing Magazine, March 2009, pp. 16-25.

[11] J. Fridrich, “Digital Image Forensics”, IEEE Signal Processing Magazine, March 2009, pp. 26-37.

[12] B. Mahdian, S. Saic, “Blind Authentication Using Periodic Properties of Interpolation”, IEEE Transaction on Information Forensics and Security, vol. 3, N° 3, September 2008, pp. 529-538.

[13] B. Mahdian, S. Saic, “Detection of Resampling Supplement with Noise Inconsistencies Analysis for Image Forensics”, IEEE International Conference on Computational Sciences and Its Applications ICCSA 2008, pp. 546-556.

[14] B. Mahdian, S. Saic, “Blind Methods for Detecting Image Fakery”, IEEE Aerospace and Electronic Systems Magazine, vol. 25, N° 4, 2010, pp. 18-24.

E-mail: avid.roman-gonzalez@ieee.org