Artículo **Revista de Simulación Computacional**
Septiembre 2017 Vol.1 No.1 18-24

Método de esteganálisis adaptivo a las características de las imágenes

RAMÍREZ-RODRÍGUEZ, Ana Elena†, JUÁREZ-SANDOVAL, Ulises, NAKANO-MIYATAKE, Mariko*, CEDILLO-HERNÁNDEZ, Manuel

Universidad Politécnica de Pachuca

Recibido: 10 de Julio, 2017; Aceptado 09 de Septiembre,2017

Resumen

En este artículo se presenta un novedoso método de esteganálisis adaptivo. El método propuesto se basa en la Transformada Discreta Coseno para realizar una clasificación de las características de las imágenes, es decir, las imágenes son analizadas y sus características son clasificadas en tres categorías: regiones planas, semi-detalladas y detalladas; posteriormente un conjunto de vectores característicos son extraídos de las regiones previamente clasificadas mediante los algoritmos de Autocorrelación (AC), Medidas de Similitud Binaria (BSM) y Amplitud de los extremos locales (ALE), finalmente una Máquina de Soporte Vectorial (SVM) es utilizada en conjunto con los vectores característicos para determinar que imágenes contienen información oculta y cuáles no. Los resultados muestran que el algoritmo propuesto supera a los algoritmos convencionales y minimizando el error de detección.

Clasificador, Estegoanálisis, Esteganografía

Abstract

This paper presents an image adaptive steganalysis algorithm. In the proposed method, the Discret Cosine Transform is used as image charactetristics classifier, where the images characteristics are classified in three categories: texture, plain or edges regions. Taking advantage of these categories a setn of statistic feature vectors is obtained using different algorithms such as Autocorrelation (AC), Binary Similarity Measures (BSM), Amplitude of Local Extreme (ALE); finally the Support Vector Machine (SVM) claisfier is used in conjunction with the obtained vectors to determine if the images contain hidden information. The results show that the proposed algorithm overcomes the conventional algorithms and minimizes the detection error.

Classifier, Steganalysis, Steganography

Citación: RAMÍREZ-RODRÍGUEZ, Ana Elena†, JUÁREZ-SANDOVAL, Ulises, NAKANO-MIYATAKE, Mariko*, CEDILLO-HERNÁNDEZ, Manuel. Método de esteganálisis adaptivo a las características de las imágenes. Revista de Simulación Computacional. 2017. 1-1: 18–24

† Investigador contribuyendo como primer autor.
* Correspondencia al autor (email: mnakano@ipn.mx)

Introducción

Actualmente los métodos de intercambio de información han tenido un crecimiento significativo, en donde la información es transmitida de un emisor hacia un receptor por medio de un canal de comunicación; de esto que los métodos esteganográficos son utilizados para transmitir información de forma confidencial, Sin embargo, algunos de estos métodos pueden ser utilizados para trasmitir información sensible con fines ilícitos como terrorismo, trata de personas, etc.

Uno de los métodos esteganográficos más usados es el remplazo del bit menos significativo (LSB-R) [1], el cual consiste en remplazar el bit menos significativo de cada pixel de una imagen con la información que se desea transmitir, esto permite tener una gran capacidad de ocultar información, sin embargo, debido a sus características de inserción es uno de los métodos esteganográficos más vulnerables ante los métodos de detección de información oculta. Por otro lado, existe un método esteganográfico menos vulnerable y capaz de ocultar la misma cantidad de información que el método de LSB-R denominado comparación del bit menos significativo (LSB-M) [2][3], en este el valor de cada pixel de la imagen portadora incrementa o decrementa de forma aleatoria de acuerdo con la información que se desea ocultar. Esta forma de ocultar información hace que este método sea más robusto ante métodos de esteganálisis, en este sentido el diseño de un método que permita realizar la detección de los archivos generados por este tipo de esteganografia es de suma importancia.

El esteganálisis se entiende como una técnica capaza de identificar si un archivo posee o no información oculta, dicho de otra forma, es la contraparte de la esteganografia.

Recientemente se han propuestos diversos métodos de esteganálisis capaces de obtener características que permiten determinar si un archivo posee o no información oculta por medio del método esteganográfico LSB-Matching han sido propuestos, entre ellos destacan: el método de "Amplitud del Extremo Local" (ALE) [4], cuyo funcionamiento está basado en el análisis del histograma del archivo portador para determinar si posee o no información oculta; otro método basado en el análisis del histograma es el propuesto en [5], sin embargo este incorpora un Discriminador Lineal de Fisher (FLD) el cual clasifica las características y discrimina las imágenes que poseen información oculta de las que no; por otro lado, el método de Valores de los Pares (PoV) [6], es un método de esteganálisis que si bien ha sido utilizado para la detección de archivos esteganográficos generados por LSB-M, tiene mejores resultados para la detección de LSB-R.

Por otro lado, existen métodos de esteganálisis basados en la clasificación de vectores característicos, en [7] los autores proponen un método de esteganálisis denominado WAM, en este un conjunto de 27 momentos de ruido son extraídos de las bandas de frecuencia de la imagen en el dominio de la transformada wavelet, mismos que son finalmente clasificados mediante la construcción de un FLD. La autocorrelación (AC), consiste en obtener una relación entre pixeles, usando una matriz de autocorrelación de la imagen original y la estegoimagen [8].

El método de similitud binaria (BSM), intenta predecir si una imagen contiene o no información analizando la correlación entre los mapas de bits de la imagen, así como la textura de cada uno de ellos [9].

ISSN: 2523-6865

Actualmente son pocos los algoritmos de esteganálisis reportados en la literatura que consideran las características de las imágenes como áreas texturizadas[10][11], planas o con bordes, en este sentido al hacer uso de este tipo de características durante el proceso de detección métodos como AC, BSM y ALE generan una fuerte variación de falsos positivos y falsos negativos, para reducir estas variaciones en los errores de detección e incrementar el porcentaje de detección es posible utilizar un clasificador entrenado para cada una de las características antes mencionadas.

En este artículo se presenta un novedoso algoritmo de esteganálisis para imágenes digitales, en el cual un clasificador de texturas [12] y un conjunto de tres métodos de extracción de características (AC, BSM y ALE) que obtiene vectores característicos los cuales son tratados mediante el uso de una Maquina de Soporte Vectorial con el fin de indicar que imagen es un archivo con información oculta.

El resto de este trabajo se encuentra organizado mediante el siguiente orden: en la primera sección se describe el algoritmo propuesto, los Resultados obtenidos son descritos en la segunda sección, finalmente las conclusiones son mostradas.

Algoritmo propuesto

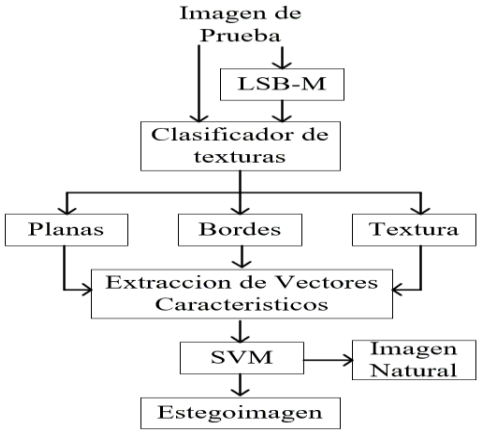

Figura 1 Diagrama a bloques del algoritmo propuesto.

En esta sección el método propuesto de esteganálisis adaptivo es descrito de forma general mediante el diagrama de la Fig.1. Una descripción detallada del método propuesto es explicada mediante los siguientes pasos:

1. Imagen de Prueba: la imagen de prueba corresponde a un conjunto de imágenes naturales.
2. LSB-M: en este bloque el método esteganográfico de LSB-M es utilizado para ocultar información en el 25%, 50%, 75% y 100% de la imagen de prueba.
3. Clasificación de texturas: en este artículo un clasificador de texturas basado en el dominio de la transformada discreta coseno (DCT) propuesto en [9] es implementado. En este la imagen es dividida en bloques de 8x8 y la DCT es implementada en cada uno de ellos. Las características de textura de cada bloque son definidas por la suma del valor absoluto de cada región del bloque transformado denotadas como: "DCT", altas frecuencias (H), bajas frecuencias (L) y semiplano (E), como se muestra en la Fig.2.

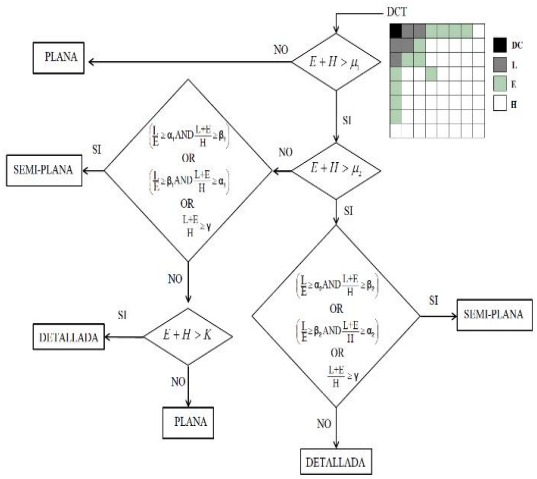

Figura 2 Clasificador de Textura.

ISSN: 2523-6865

Finalmente, para la obtención de los resultados experimentales los parámetros utilizados son los mismos que los sugeridos en [12] bajo las siguientes consideraciones:

– Si tiene más de 80% de detección de los bloques planos se considera plana. Si es entre 40% y 79.9% se considera que es una imagen con bordes.
– Si la imagen tiene menos del 40% de bloques planos se considera una imagen con textura.

4. Extracción de Vectores característicos: en este proceso un conjunto de métodos de extracción de características es implementado para obtener un conjunto de vectores que permitan identificar si una imagen posee o no información oculta.

La Autocorrelación

La autocorrelación [8] en LSB presenta eficientes resultados para imágenes planas, pero no tan eficiente para imágenes detalladas y puede representada como se observa en (1).

$$AC_{x,y} = \sum_{i,j} S_{i,j} \cdot S_{i+x,j+y} \quad (1)$$

Donde $S_{i,j}$ es (i, j)-ésimo valor del plano LSB. Si la autocorrelación es 0, los datos no muestran una ninguna relación entre ellos, entonces la imagen probablemente contiene un mensaje oculto.

En el presente artículo se utilizan las siguientes autocorrelaciones: $AC_{0,1}$, $AC_{0,2}$, $AC_{1,0}$, $AC_{2,0}$, $AC_{1,1}$, $AC_{1,2}$, $AC_{2,1}$, $AC_{2,2}$., después de calcular las autocorrelaciones anteriores el radio entre las imágenes es calculado de acuerdo con (2).

$$R = \frac{AC_{prueba}}{AC_{estegoimagen}} \quad (2)$$

Donde AC_{prueba} es $AC_{x,y}$ de la imagen de prueba, mientras $AC_{estegoimagen}$ corresponde a la imagen obtenida después de someter intencionalmente la imagen de prueba al método esteganográfico de LSB-M.

Las Medidas de Similitud Binarias

Si la imagen tiene un mensaje oculto, las características de los vecinos cercanos se alteran en el LSB [9], considerando imagines de tamaño MxN la similitud binaria puede ser representada como:

$$x_{i,j} = \begin{cases} 1 \text{ si } x_i = 0 \text{ y } x_i^s = 0 \\ 2 \text{ si } x_i = 0 \text{ y } x_i^s = 1 \\ 3 \text{ si } x_i = 1 \text{ y } x_i^s = 0 \\ 4 \text{ si } x_i = 1 \text{ y } x_i^s = 1 \end{cases} \quad (3)$$

Donde x_i representa el pixel en la posición i, y x_i^s los vecinos del pixel i. Consecuentemente un conjunto de 10 características son obtenidas mediante (4-13), para formar un vector característico de 10 elementos.

$$m_1 = \frac{2(a+d)}{2(a+d)+b+c} \quad (4)$$

$$m_2 = \frac{a}{a+2(b+c)'} \quad (5)$$

$$m_3 = \frac{a}{b+c'} \quad (6)$$

$$m_4 = \frac{a+d}{b+c'} \quad (7)$$

$$m_5 = \frac{1}{4}\left(\frac{a}{a+b} + \frac{a}{a+c} + \frac{d}{b+d} + \frac{d}{c+b}\right) \quad (8)$$

$$m_6 = \frac{ad}{\sqrt{(a+b)(a+c)(b+d)(c+b)}} \quad (9)$$

$$m_7 = \sqrt{\frac{a}{a+b} + \frac{a}{a+c'}} \quad (10)$$

$$m_8 = \frac{b+c}{2a+b+c'} \quad (11)$$

$$m_9 = \frac{bc}{(a+b+c+d)^2} \quad (12)$$

$$m_{10} = \frac{b+c}{4(a+b+c+d)} \quad (13)$$

Los valores de a, b, c, d son obtenidos mediante:

$$a = \frac{1}{MN}\sum_I \alpha_1^1 \quad (14)$$

$$b = \frac{1}{MN}\sum_I \alpha_1^2 \quad (15)$$

$$c = \frac{1}{MN}\sum_I \alpha_1^3 \quad (16)$$

$$d = \frac{1}{MN}\sum_I \alpha_1^4 \quad (17)$$

Donde α_i^j denota la función de transición de los píxeles vecinos del píxel central.

Amplitud del Extremo Local

Es un método para detectar archivos tratados con el algoritmo LSB-Matching [4]. En donde la posición del extremo local consiste en las posiciones mínimas y máximas del histograma, así como el uso de una matriz de coocurrencia para las obtener las direcciones horizontal o vertical, 45° y 135° [13], en el cual es realizado el análisis.

Mediante este método un conjunto de 10 valores característicos es obtenido del histograma y las matrices de coocurrencia. Las primeras dos características son obtenidas del histograma mediante (18) y (19).

$$A = \sum_{x\in\varepsilon\cap\{3,4,\dots 252\}} |2h(x) - h(x-1) - h(x+1 \quad (18)$$

Donde $h(x)$ es el número de pixeles con valor x.

$$d_1 = \sum_{x\in\varepsilon\cap\{1,2,253,\}} |2h(x) - h(x-1) - h(x+1) \quad (19)$$

Las características obtenidas mediante la matriz de coocurrencia son calculadas mediante (20).

$$A_2(M) = \sum_{p\in\varepsilon'} |4M(p) - \sum_{n\in N} M(p+n)| \quad (20)$$

Finalmente, los valores diagonales de las dichas matrices son obtenidos mediante (21).

$$d_2(M) = \sum_{k=0}^{255} M(k,k) \quad (21)$$

Donde $N = \{(0,1),(1,0),(-1,0),(0,-1)\}$, las diez características se presentan en la tabla 1:

1	A_1
2	d_1
3	A_2
4	$A_2(M_{vertical})$
5	$A_2(M_{45°})$
6	$A_2(M_{135°})$
7	$d_2(M_{horizontal})$
8	$d_2(M_{vertical})$
9	$d_2(M_{45°})$
10	$d_2(M_{135°})$

Tabla 1 Características obtenidas con el método ALE.

Finalmente, una máquina de soporte vectorial con un kernel Gaussiano [14] es implementada como clasificador, en este el conjunto de vectores característicos son tratados con el objetivo de indicar si la imagen pose o no información oculta.

Resultados

Para evaluar el método propuesto es utilizada una base de imágenes BOWS-2 [15], la cual contiene 10,000 imágenes en escala de grises de tamaño 512x512 píxeles. Inicialmente en el conjunto de imágenes se oculta información en el 25%, 50%, 75% y 100% de la imagen mediante el método esteganográfico LB-M, posteriormente mediante el uso de clasificador de texturas las imágenes son clasificadas en tres categorías: planas (A), semiplana o medianamente texturizada (B) y texturizada (C) en donde la categoría A tiene un total de 2482 imágenes planas, la categoría B tiene 5650 imágenes y la categoría C tiene 1868 imágenes.

ISSN: 2523-6865

Las imágenes contenidas en cada una de estas categorías son tratadas mediante los algoritmos de Autocorrelación, Medidas de Similitud Binarias y Amplitud del Extremo Local. En la tabla 2 se muestra la dimensión de los elementos de cada vector, los cuales son clasificados mediante una máquina de soporte vectorial y un kernel Gaussiano, el cual indicara si las imágenes contienen información oculta o no.

	AC	BSM	ALE
Dimensión del vector	8	10	10

Tabla 2 Dimensión cada vector característico, correspondiente a cada método de extracción de características.

En el método propuesto se usaron 4 diferentes porcentajes de información oculta: 25%, 50%, 75% y 100% los cuales son analizados mediante diferentes métodos de extracción de características (AC), (BSM) y (ALE), cuyos porcentajes de detección comparados con métodos convencionales se muestran en la Tabla 3, Tabla 4 y Tabla 5 respectivamente.

	25%	50%	75%	100%
Convencional	57.71	72.47	85.55	86.28
A	57.86	73.49	86.49	86.70
B	58.06	72.86	86.42	86.45
C	57.97	72.64	86.53	86.42

Tabla 3 Porcentaje de detección del método propuesto usando el método de extracción de características de Auto Correlación.

	25%	50%	75%	100%
Convencional	64.92	79.99	90.00	90.20
A	65.21	80.52	90.76	90.79
B	65.15	79.96	90.44	90.76
C	65.08	80.91	91.04	90.30

Tabla 4 Porcentaje de detección del método propuesto usando el método de extracción de características de Medidas de Similitud Binarias.

	25%	50%	75%	100%
Convencional	73.23	87.19	92.51	92.50
A	73.42	87.74	92.50	92.49
B	73.05	87.70	92.61	92.67
C	73.23	87.19	92.51	92.50

Tabla 5 Porcentaje de detección del método propuesto usando el método de extracción de características de Amplitud del Extremo Local.

En las tablas se puede observar que en general el método propuesto presenta un mejor rendimiento que el método convencional.

Conclusiones

En este artículo se propone un nuevo algoritmo de esteganálisis adaptivo para imágenes digitales en el cual gracias a la incorporación de un algoritmo capaz de realizar una clasificación de cada imagen de acuerdo con sus características de textura es posible reducir el error de detección que se presenta en los algoritmos convencionales, obteniendo así una mejor detección de estegoimagenes generadas por el método de LSB-M. El uso de una máquina de soporte vectorial como clasificador para discriminar las estegoimagenes de las imágenes naturales ayuda a incrementar el porcentaje de detección del método propuesto ante diferentes porcentajes de información oculta, siendo capaz de realizar detecciones superiores al 55% para un porcentaje de información oculta del 25%.

Agradecimiento

Los autores agradecen el apoyo del Instituto Politécnico Nacional y CONACYT para la realización de este trabajo.

Nombre de los Autores:
Ana Elena Ramírez Rodríguez
O. Ulises Juárez Sandoval
Mariko Nakano Miyatake
Manuel Cedillo Hernández

ISSN: 2523-6865

Referencias

[1] Shruti Sekra, Smata Balpande and Karishma Mulani, ¨Steganography Using Genetic Encryption Along With Visual Cryptography", SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE), vol. 2, issue 1, 2015.

[2] Pevný Tomáš, Bas Patrick, Fridrich Jessica, "Steganalysis by Substractive Pixel Adjacency Matrix", IEEE Transactions on information forensics and security, volume 5, no. 2, 2010.

[3] Zhang J., Cox I., Doërr G., "Steganalysis for LSB matching in images with high-frequency noise", IEEE Int. Workshop on Multimedia Signal Processing (MMSP), 2007.

[4] Cancelli G., Doërr G., Cox I. y Barni M., "Detection of ± steganography based on the amplitude of histogram local extrema". Proc. IEEE Int. Conf. On Image Processing (ICIP), 2008.

[5] Ker A. D., "Steganalysis of LSB matching in grayscale images", IEEE Signal Processing Lett. Vol. 12, pp. 441-444, 2005.

[6] A. Westfeld y A. Pfitmann, "Attacks on Steganographic Systems: Breaking the Steganographic Utilities EZStego, Jsteg, Steganos and S-Tools – and Some Lessons Learned", Information hiding, Lecture Note vol. 1768, 2000.

[7] M. Golijan J. Fridich T. Holotyak "New Blind Stegoanalysis and its implications", SPIE Security, S Steganography and watermarking of Multimedia contents, vol 6072, pp 1-13, 2006.

[8] Yadollapour A., Naimi H. M., "Attack on LSB steganography in color and grayscale images using autocorrelation coefficients", European Journal of Scientific Reasearch, Volume 31, no. 2, pp.172-183, 2009.

[9] Avcibas Ísmail, Kharrazi Mehdi, Memon Nasir, Sankur Bülent, "Image steganalysis with Binary Similarity Measures", EURASIP Journal on Applied Signal Processing, pp. 2749-2757, 2005.

[10] Juarez-Sandoval Oswaldo, Cedillo-Hernández Manuel, Nakano-Miyatake Mariko, Pérez-Meana Héctor, Toscano-Medina, Karina, "Image-Adaptive Steganalysis for LSB Matching Steganography". Proc IEEE Int. Conf. on Telecommunications and Signal Processing (TSP), 2016.

[11] Juarez-Sandoval Oswaldo, Cedillo-Hernández Manuel, Sánchez-Pérez Gabriel, Toscano-Medina, Karina, Pérez-Meana Héctor, Nakano-Miyatake Mariko, "Compact Image Steganalysis for LSB-Matching Steganography". Proc IEEE Int. Workshop Biometrics and Forensics (IWBF), 2017.

[12] Tong Henry, N. Venetsanopoulos Anastasios, "A perceptual model for jpeg applications based on block classification. Texture masking and luminance masking", Proc. IEEE Int. Conf. On Image Processing (ICIP), 1998.

[13] Robert M. Haralick, K. Shanmugam, and Its'hak Dinstein." Textural Features for Image Classification", IEEE Transactions on Systems, Man, and Cybernetics, Vol. Smc-3, No. 6, November 1973.

[14] Schaathung, Hans Georg., "Machine learning in image steganalysis", 1st ed., United Kingdom, John Wiley & Sons Ltd, chapter 5, 2012.

[15] Bas, P., Furon, T.: BOWS-2, July 2007, disponible en: http://bows2.gipsa-lab.inpg.fr

ISSN: 2523-6865