Sistema inmune artificial para estegoanálisis de imágenes JPEG

José de Jesús Serrano-Pérez, Moisés Salinas-Rosales, Nareli Cruz-Cortés

Instituto Politécnico Nacional,
Centro de Investigación en Computación,
Laboratorio de Ciberseguridad, Ciudad de México,
México

Resumen. La esteganografía es la técnica de ocultar la información digital quizás más utilizada en la actualidad. Existen numerosos reportes sobre su uso exitoso para ocultar código malicioso dentro de objetos multimedia que infiltran software dañino (malware) en diversos dispositivos electrónicos, evitando su detección por los controles correspondientes. Una vez que el malware ha alcanzado su destino, otro software extrae el código incrustado y ejecuta un ataque. Este tipo de malware es llamado *estegomalware*. El estegoanálisis es la contramedida de la esteganografía, que se refiere al estudio de las técnicas que permite la detección de *esteganogramas*. En el estegoanálisis moderno se han utilizado diversas técnicas de la Inteligencia Artificial. En este trabajo exploramos el uso de un paradigma con inspiración biológica llamado Sistema Inmune Artificial (SIA) para detectar imágenes en formato JPGE alteradas con esteganografía. Además, proponemos el uso de la ondeleta de Haar para la definición del vector de características que mejor describa a la imagen bajo análisis. Los experimentos ejecutados arrojaron resultados prometedores que prueban que la detección realizada por nuestra propuesta son comparables, y ocasiones mejores, que otros trabajos representativos del estado del arte.

Palabras clave: Esteganografía, estegoanálisis, sistemas inmunes artificiales, clasificación, reconocimiento de patrones.

Steganalysis Based on an Artificial Immune System for JPEG Images

Abstract. Steganography is one of the most used hiding information techniques today.Recently, the use of steganography techniques has been reported very successful to hide malicious code inside, apparently innocuous, multimedia objects, in order to infiltrate malware into organizations and personal devices, avoiding malware detection controls. Once the embedded malware has reached its destination, another software extracts the embedded code and performs the attack. This new kind of malware is called *stegomalware*. Steganalysis is the countermeasure to steganography, and it is a set of techniques that allows the detection of

these *steganograms*. In modern steganalysis different Artificial Intelligence techniques have been employed, but very few have proposed solutions based on Bio-inspired and Evolutionary Computing. In this work we present a steganography detection method based on an Artificial Immune System (AIS) to detect JPEG images altered with steganography. We propose the use of Haar Wavelets in order to extract a characteristic feature vector that best describe the analyzed image. The experiments performed shown promising results that could prove that a classification system made with AIS could perform same and in some cases better.

Keywords: Steganography, steganalysis, artificial immune systems, wavelets, classification, pattern recognition.

1. Introducción

La esteganografía es una rama de las técnicas de ocultamiento de la información, cuyo uso permite establecer un canal de comunicación encubierto y seguro, donde solo las entidades involucradas son conscientes de él, para eso se selecciona un elemento inocuo y común que pasará fácilmente desapercibido, ademas de que incluso a una inspección superficial no se le encontrara rareza alguna. Si bien el uso de estas tecnicas remota a las primeras civilizaciones. En la actualidad su uso sigue vigente y tiene una presencia muy fuerte y dominante en el mundo digital, donde es utilizado para burlar sistemas de censura en países totalitarios para poder comunicarse con el mundo exterior, así como para la exfiltración de información sensible, etc. En la figura 1 podemos ver de que se compone un sistema esteganografico, el emisor genera una llave que codificara el mensaje en un objeto por medio de una función embeber, el resultado es un objeto encubierto o esteganograma, al llegar al receptor, este utiliza la misma llave con la que se codifico el mensaje con una función extracción. Ejemplo de una herramienta esteganográfica, es Outguess [7]

Ejemplo de esto se ve en la figura 1, donde el mensaje a enviar se codifica con una llave y el objeto que servia como encubrimiento, cuando viaje por un canal de comunicación, se le conocerá como esteganograma, una vez que llegue a su destino el receptor, con la misma llave con la que se codifico el mensaje, se extrae y obtiene la información oculta en ese esteganograma.

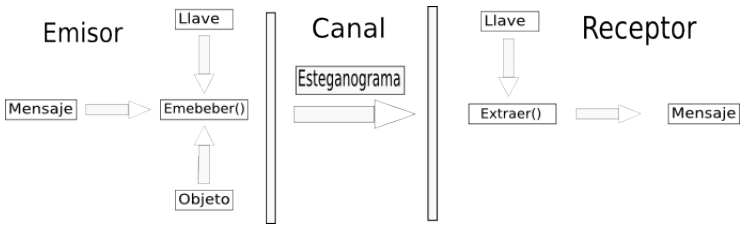

Fig. 1. Modelo un sistema esteganográfico

Sin embargo se le ha encontrado un nuevo uso a la esteganografía, donde aprovechando las propiedades de ocultamiento, se ha comenzado a utilizar para ocultar código malicioso o virus informáticos, donde una vez que el estganograma ha llegado a su destino final, son extraídos del objeto donde se ocultaban vulnerando así los controles antimalware y de control de contenido. A este nueva forma de implementar *malware* se le conoce como *stegomalware*; ejemplos de esto han sido Lurk [10], Stegosploit [8] y ataques de filtración al sistema operativo Android [11].

El estegoanálisis es la contraparte de la esteganografía y se encarga de la detección de información oculta en un un grupo de objetos dados, para eso emplea diversas técnicas de disciplinas computaciones como análisis de imágenes y señales, inteligencia artificial y reconocimiento de patrones, entre otras. Se han propuesto varias técnicas para poder detectar este tipo de objetos.

Utilizando distintas técnicas de las diferentes disciplinas mencionadas. En este trabajo se propone un sistema inmune artificial (SIA) para la detección de esteganogramas, la información se utiliza para entrenar el sistema se extrae por medio del análisis de ondeletas de Harr en imágenes.

Las principales aportaciones en este trabajo son las siguientes:

1. La adaptación de un SIA para detectar esteganogramas.
2. El uso de ondeletas de Harr para caracterizar las imagenes y se pueda identificar aquellas que son esteganogramas.

Una de las principales ventajas del uso de esta ondeleta es que son de cálculo rápido y permiten obtener una representación compacta de las imágenes a caracterizar. Los resultados obtenidos en los experimentos muestran que la propuesta es factible y competitiva.

En la sección 2 se describe lo que es el estegoanalisis, los diferentes tipos y métodos existentes, en la sección 3 se menciona lo que es el sistema inmune artificial y como se desarrolla una aplicación utilizando este paradigma computacional, en la sección 4 se describe la propuesta del SIA como clasificador de esteganogramas, en la sección 5 se detalla la metodología que se sigue para desarrollar el sistema y los resultados obtenidos, posteriormente en la sección 6 se discuten los resultados obtenidos y se menciona el posible trabajo a futuro para realizar

2. Estegoanálisis

No hay un método único y formal para crear un *esteganograma* por lo que el estegoanálisis requiere de múltiples técnicas de diferentes áreas para poder reconocer aquellos objetos que pudieran ser esteganogramas [1]. Esto hace el problema de detección interesante y complejo por las implicaciones practicas que conlleva, partiendo de la experimentación, hallar el método para poder encontrar la o las características que permiten la detección de los objetos. Seguido de esto es necesario escoger un método de clasificación que en base a la información obtenida de la imagen pueda clasificar de manera correcta estos objetos y determine si contienen información oculta o no.

2.1. Técnicas de estegoanálisis

Dentro del estegoanálisis se definen 2 tipos de detectores, los dedicados y los universales, el primero es un tipo de detector especifico para un tipo de técnica en particular, su ventaja es el de un porcentaje detección mayor comparado con los detectores universales, pero con la desventaja de que debe de saber *a priori* que tipo de técnica fue utilizada en el objeto a analizar. Por otra parte, los detectores universales son aquellos que detectan mas de 2 tipos de técnicas esteganográficas, su desventaja es que tienden a tener una tasa de detección menor que la de los detectores dedicados, pero no requieren saber que técnica esteganográficas fue empleada en el objeto a analizar.

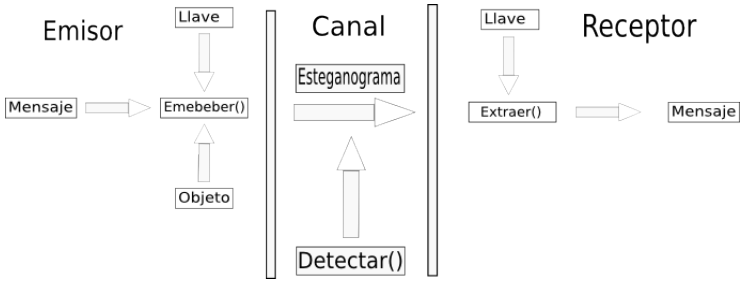

Fig. 2. Detector con enfoque de guardia pasivo

A su vez cualquiera de los dos tipos se divide en dos enfoques, activo y pasivo, el primer enfoque consiste en modificar todos los elementos que viajan en el canal de comunicación, de manera que no afecte su uso legitimo (ejemplo la visualización de una imagen) pero cuando se requiera recuperar la información, esto no sea posible. Aunque supone una solución final al problema de la detección de la esteganografía su implementación es meramente teórica. Para el enfoque pasivo representado en la figura 2 este se encarga de analizar cada objeto por medio de una función de detección, tal que dada una probabilidad se determina si, un objeto es un esteganograma o no. Este trabajo se enfoca en los detectores de tipo dedicados con enfoque pasivo.

2.2. Estado del arte

El trabajo realizado por Dumitrescu,2003 [4] realiza un trabajo de detección con enfoque dedicado, detectando en los bits menos significativos variaciones anormales en elementos multimedia como audio y vídeo, los clasifica usando analisis estadistico obteniendo resultados de detección entre el 87 % y 99 %. Un trabajo mas reciente realizado por Chen, 2009 detectando la herramienta esteganográfica JPEG-Steg [3] donde usa modelos mixtos lineares como método de extracción de características en imágenes JPEG y como método de clasificación utiliza redes neuronales, obteniendo asi resultados de detección del 98 % al 100 %,

el trabajo de Sindhu, 2008 [9] extrae las características de imágenes BMP por medio de análisis estadísticos en los bits menos significativos y por medio de análisis estadísticos de primer orden detecta las variaciones en el conjunto de características, obteniendo resultados de clasificación entre el 92 % y 99 %

3. Sistemas inmunes artificial

El sistema inmune artificial (SIA) son un nuevo paradigma computacional donde se busca emular el sistema inmune humano, de modo que se pueda adaptar como un método de clasificación, estos sistemas tienen la propiedad de adaptabilidad y auto-mantenimiento. A pesar de ser un reciente paradigma computación comparado con otros métodos de clasificación como maquinas de soporte vectorial, aprendizaje maquina o redes neuronales, ha demostrado obtener resultados similares a los métodos con mayor tiempo de desarrollo e investigación. De manera formal un SIA se define de la siguiente manera: Ün sistema adaptativo, inspirado por la teoría de inmunología y la observación de funciones inmunes, principios y modelos, que son aplicados a la solución de problemas"[12].

Sus usos principales son para la solución de problemas de clasificación y optimización, las áreas donde mas son utilizados por mencionar algunas:

- Seguridad computacional,
- Optimización de funciones numéricas,
- Aprendizaje maquina,
- Bio-informatica,
- Detección de virus,
- Minería de datos.

3.1. Desarrollando una arquitectura de SIA

Hasta la fecha no se ha desarrollado una metodología general para los SIA, pero Castro y Timmis [2] sugieren una arquitectura para su desarrollo, donde se definen los siguientes puntos:

- Primero definir la representación para los componentes del sistema,
- Un conjunto de mecanismos para evaluar la interacción entre los individuos,
- Un conjunto de procedimientos de adaptación que gobiernen las dinámicas del sistema.

Para la representación de los componentes del sistema se han empleado representaciones como cadenas binarias y vectores de valores reales, para nuestro caso emplearemos los vectores de valores reales que obtuvimos del análisis por medio de las ondeletas de Harr. Para poder realizar la interacción, un método de evaluación debe ser definido para poder determinar la afinidad de los elementos que componen el sistema, ya que estaremos usando vectores de valores reales, vamos a usar distancia euclidiana para dicho fin:

$$A = \sqrt{\sum_{i=1}^{L} (Ab_i - Ag_i)^2}. \quad (1)$$

Para definir el conjunto de procedimientos que gobernaran el sistema usaremos el algoritmo de seleccion negativa, que menciona los siguientes pasos:

1. Definir el *self* y el no *non-self*,
2. Crear anticuerpos que sean diferentes del *self*,
3. Entrenar y probar los anticuerpos con un conjunto de patógenos de entrenamiento,
4. Una vez que se tiene un numero definido de anticuerpos maduros, probar el sistema contra un conjunto de pruebas.

Para que se pueda cumplir el algoritmo se tiene que cumplir la siguiente definición formal sobre los conjuntos *self* y *non-self*: Dado el espacio $\sum^L$ y el conjunto que define *self* $S \subset \sum^L$ definimos el conjunto *non-self* $N \subset \sum^L$ ser el complemento $N = \sum^L \backslash S$ tal que $\sum^L = S \cup N$ y $S \cap N = \emptyset$.

De manera practica puede ser que dicha definición no pueda cumplirse, así que se tiene que buscar que la representación de los elementos del sistema corresponda a la definición previamente descrita

4. Propuesta

El trabajo propuesto es desarrollar un sistema de detección de esteganogramas usando un clasificador que utilice un SIA en imágenes JPEG alterados con la herramienta Outguess, utilizando un sistema inmune artificial usando un algoritmo de clasificación negativa, así como la identificación de los rasgos que mejor describen a las imágenes alteradas con Outguess, para eso usaremos los coeficientes obtenidos del análisis por ondeletas de Harr. El desarrollo se describe de la siguiente manera:

1. Crear dos repositorios con las mismas imágenes, uno alterarlo con una herramienta esteganográfica y el otro dejarlo intacto, estos serán nuestros repositorios de entrenamiento.
2. Realizar la extracción de características por medio del análisis de ondeletas de Harr para cada uno de los repositorios creados.
3. Utilizando el algoritmo de selección negativa del sistema inmune artificial , desarrollar el clasificador y entrenarlo con los datos de los repositorios de entrenamiento.
4. Probar el clasificador contra un repositorio de imagenes de prueba.

A continuacion de describira cada uno de los puntos mencionados en el desarrollo empezando por la extracción de características:

4.1. Extracción de características

Para poder desarrollar un detector de esteganogramas JPEG se requiere primero obtener un vector de rasgos que nos permita caracterizar bien el esteganograma que queremos identificar, ya que nuestro interés está en las imágenes

JPEG, escogeremos una técnica que nos permita obtener la información más relevante de la imagen, para ello existen varias formas de obtener esta información, dentro de las más utilizadas está el uso de análisis por ondeletas, cuya ventaja es su rápido cálculo y un conjunto de coeficientes que describen la imagen de manera precisa, existen dentro de la familia de ondeletas varios tipos de ellas, como por ejemplo Daubechies y Harr. Las ondeletas de Harr en particular se caracterizan por su rapidez de cálculo y uso para describir imágenes [6]. Para esto se usa la segunda transformada de ondeletas de Harr la cual se describe de la siguiente manera [5]:

$$\overline{f} = \begin{pmatrix} f_{0,0} & f_{0,\frac{1}{2}} \\ f_{\frac{1}{2},0} & f_{\frac{1}{2},\frac{1}{2}} \end{pmatrix} = \begin{pmatrix} s_{0,0} & s_{0,1} \\ s_{1,0} & s_{1,1} \end{pmatrix}. \tag{2}$$

Considerar la función $\overline{f}$ que es la aproximación de una función f y s_0, s_1 los valores de la señal a analizar (siendo la amplitud y longitud de la señal respectivamente).

$$\begin{pmatrix} s_{0,0} & s_{0,1} \\ s_{1,0} & s_{1,1} \end{pmatrix} \rightrightarrows \begin{pmatrix} \frac{s_{0,0}+s_{0,1}}{2} & \frac{s_{0,0}-s_{0,1}}{2} \\ \frac{s_{1,0}+s_{1,1}}{2} & \frac{s_{1,0}-s_{1,1}}{2} \end{pmatrix}. \tag{3}$$

Después de que se hayan aplicado un número de iteraciones exitosas (usualmente n cuando el tamaño de la señal es 2^n) obtenemos la siguiente matriz

$$\begin{pmatrix} CA & CH \\ CV & CD \end{pmatrix}, \tag{4}$$

donde cada coeficiente describe lo siguiente:

- **Cambios Ponderados** (CA) : Incluye las propiedades globales de la señal/imagen analizada.
- **Cambios Horizontales** (CH) : Incluye la información sobre las lineas horizontales ocultas en la señal/imagen.
- **Cambios Verticales** (CV): Incluye la información sobre las lineas verticales ocultas en la señal/imagen.
- **Cambios Diagonales** (CD): Incluye la información sobre las lineas diagonales ocultas en la señal/imagen.

Cuando se realiza el analisis en una imagen a color se obtienen 48 valores en total, 12 corresponden a los coeficientes en CA, 12 en CH, 12 en CV y 12 en CD, esto por que es una imagen a color, nosotros solo utilizaremos los 3 últimos coeficientes que son CH, CD y CD, siendo un total de 36 coeficientes que forman nuestro vector de caracterización, el cual representamos en la tabla 1.

En la figura 3, se muestra un análisis de dos imágenes iguales en sus cuatro coeficientes, las imágenes del primer renglón corresponden a un esteganograma, las imágenes correspondientes al segundo renglón son la misma imagen pero sin contenido oculto, visualmente hay diferencias notorias cuando comparamos ambas imágenes en el coeficiente horizontal, vertical, diagonal y el ponderado. De esta manera se ejemplifica que es posible crear un vector de características significativamente descriptivo usando los coeficientes obtenidos por la ondeleta de Harr.

Tabla 1. Vector de caracterización

CH			CV			CD		
C_0	...	C_{11}	C_{12}	...	C_{23}	C_{24}	...	C_{36}

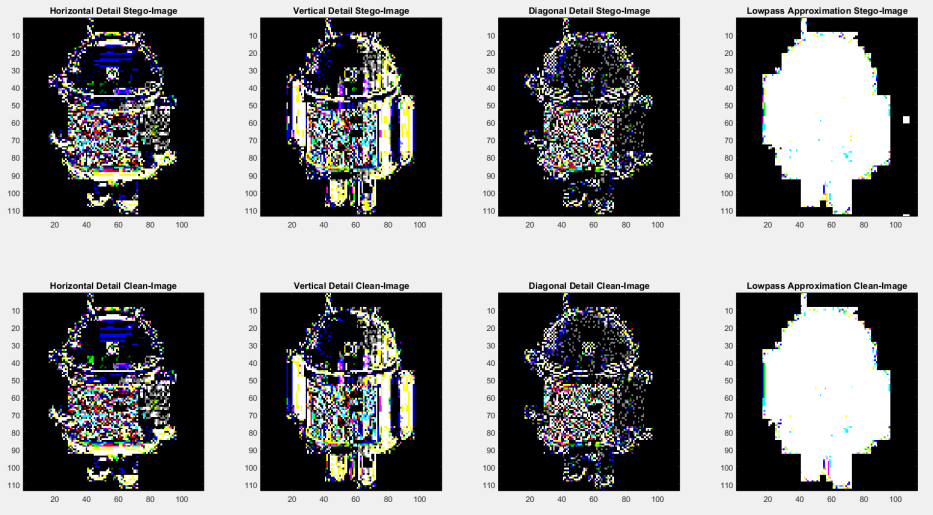

Fig. 3. Análisis visual de una imagen limpia y la misma con contenido oculto usando ondeletas de Harr

4.2. Clasificador SIA para esteganogramas

Siguiendo la arquitectura de desarrollo mostrada en la sección 3.1, se describe lo siguiente:

1. Para la representación de los componentes en el sistema se tienen 3 entidades, el conjunto del *self* que son todas aquellas imágenes que no tienen contenido oculto, el conjunto del *non-self* que son las imágenes con contenido oculto y los detectores que identificaran a los invasores, que serán todos aquellos elementos que no estén definidos en los conjuntos anteriores, cada uno está representado por un vector de características , es decir por un vector formado por 36 valores numéricos.
2. El mecanismo que evalúa la interacción entre estos componentes es la medida de afinidad que se haya seleccionado, en este caso la medida esta dada por la ecuación (1) de distancia euclidiana
3. El procedimiento de gobernará la dinámica del sistema sera el algoritmo de selección negativa también definido en la sección 3.1

4.3. Definiendo el SIA

Procedemos a definir el *self* y *non-self*:

Tabla 2. Composición del anticuerpo

CH			CV			CD			Afinidad con *non-self*	Afinidad con *self*
C_0	...	C_{11}	C_{12}	...	C_{23}	C_{24}	...	C_{36}	$A(Ab_i, NS_i)$	$A(Ab_i, S_i)$

- El *self* serán todos los vectores de características que correspondan al repositorio de imágenes limpias
- El *non-self* serán todos los vectores de características que correspondan al repositorio de imágenes con contenido oculto.
- Una vez definidos los repositorios inicializamos los anticuerpos, que tendrán las mismas características que los vectores antes mencionados, estarán compuestos por 36 valores aleatorios reales en un rango máximo y mínimo definido por los valores del conjunto de entrenamiento, tendrá ademas dos valores adicionales, uno que determine su afinidad con el repositorio de *self* y *non-self*, esta afinidad es la distancia euclidiana entre el anticuerpo y el elemento del repositorio, esto esta representado en la tabla 2.

4.4. Entrenamiento del SIA

Una vez que estén inicializados los repositorios, seguimos a la fase de entrenamiento, donde cada nuevo anticuerpo creado ,al que le llamaremos inmaduro, se le calcula su afinidad con el elemento correspondiente en el conjunto *self* y *non-self*, esto es con la premisa de que para cada elemento en el repositorio del *self* y *non-self* se tiene un anticuerpo. Cada anticuerpo pasa por la siguiente prueba:

- Mientras $numAbM < n$
  - Si $A(Ab_i, NS_i) < A(Ab_i, S_i)$
    - Destruir y crear un nuevo anticuerpo.
  - Si $A(Ab_i, NS_i) > A(Ab_i, S_i)$
    - Agregar el anticuerpo al conjunto de anticuerpos maduros,
    - $numAbM = numAbM + 1$.

$A(Ab_i, NS_i)$ es la afinidad entre el anticuerpo con el elemento correspondiente en *non-self* y $A(Ab_i, S_i)$ es la afinidad con el elemento correspondiente en el *self*. Este proceso se repite hasta haya n anticuerpos maduros($numAbM$), a cada iteración se le denomina ciclo de vida, de manera adicional este entrenamiento evita que los anticuerpos sean auto-reactivos y detecten elementos que no deben identificar.

4.5. Probando el SIA

Una vez que todos los detectores hayan madurado, procedemos a probar el sistema, todos los anticuerpos analizan todos los elementos de prueba y se define la siguiente regla de solución:

- Si $A(Ab_i, In_j) \geq A(Ab_i, NS_i)$ y $A(Ab_i, In_j) > A(Ab_i, S_i)$

- Clasificar como esteganograma.

donde $A(Ab_i, In_j)$ es la afinidad entre un anticuerpo contra un elemento de prueba, el conjunto In es el repositorio de pruebas representado de la misma manera que los conjuntos del $self$ y *non-self.*

5. Experimentos

Para comprobar la funcionalidad del sistema se siguio la metodologia descrita, inciando con la creación del repositorio inicial, donde se utilizaron 1000 imágenes JPEG en RGB, todas las imagenes tienen un tamaño fijo de 512x512 pixeles con una profundidad de color de 24 bits y una tasa de compresión de aproximadamente 26.2313, al tener los 2 repositorios se obtuvieron 2000 imágenes en total, el archivo embebido en el repositorio de imágenes alteradas con Outguess fue un código malicioso en Javascript, los vectores de características fueron almacenados en archivos CSV y gráficados para su primer análisis como se puede ver en la figura 4.

Tabla 3. Resultados obtenidos del SIA en la detección de Outguess

Detección Outguess				
Coeficiente Utilizado	Exhaustividad	Mejor Precisión	Peor Precisión	Precisión en Promedio
CH	100 %	94 %	77 %	86.24 %
CV	100 %	87 %	72 %	80.7 %
CD	100 %	84 %	65 %	75.82 %

Si nosotros utilizáramos los todos los coeficientes como un solo vector de características, difícilmente podríamos diferenciar entre lo que queremos identificar, en nuestro caso al querer implementar el SIA, no se cumpliría la caracterización del *self* y *non-self*, por lo que hemos decidido dividir el vector de características en 3 vectores que contienen los CH, CV y CD por separado, cada uno de estos grupos esta representado en la figura 4, cada vector se compone de 12 coeficientes en total. Para el SIA utilizamos 1000 detectores. Observamos que conforme se va a acercando al numero de detectores deseados, requiere mas ciclos de vida. Una vez que maduraron los 1000 detectores se procedió a probar el sistema, para eso empleamos un nuevo repositorio de 200 imágenes distintas a las utilizadas en la fase de entrenamiento, este repositorio se compone de 100 imágenes limpias y 100 alteradas con Outguess, nuevamente se les extrae los coeficientes para su clasificación en el sistema.

Es importante mencionar que el sistema se probo para los tres casos, cuando usamos los datos de CH, CV y CD. Se ejecuto el programa 50 veces y los resultados obtenidos para cuando se utiliza el sistema usando los 3 coeficientes por separado se muestran en la tabla 5, la linea negra, denotada por los puntos (+), representa los resultados obtenidos de usar CH, la linea roja, denotada por

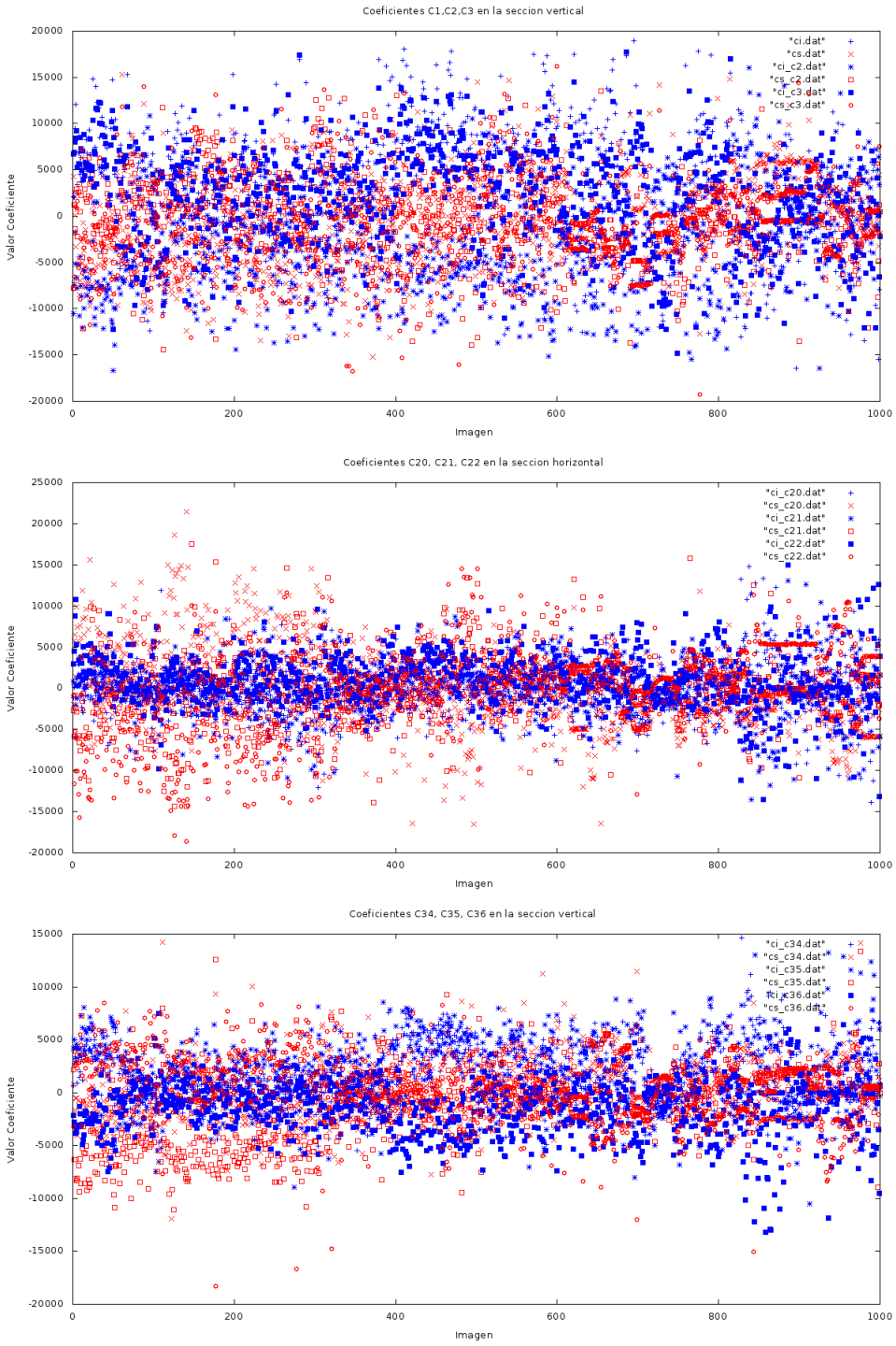

Fig. 4. Representación gráfica de los coeficientes

los puntos(■), de usar CV y la linea azul, denotada por los puntos (•), de usar CD. En la tabla 3 mostramos los resultados obtenidos. Con los coeficientes ya extraidos de las imagenes, el tiempo promedio del sistema en realizar un corrida es de 15 segundos.

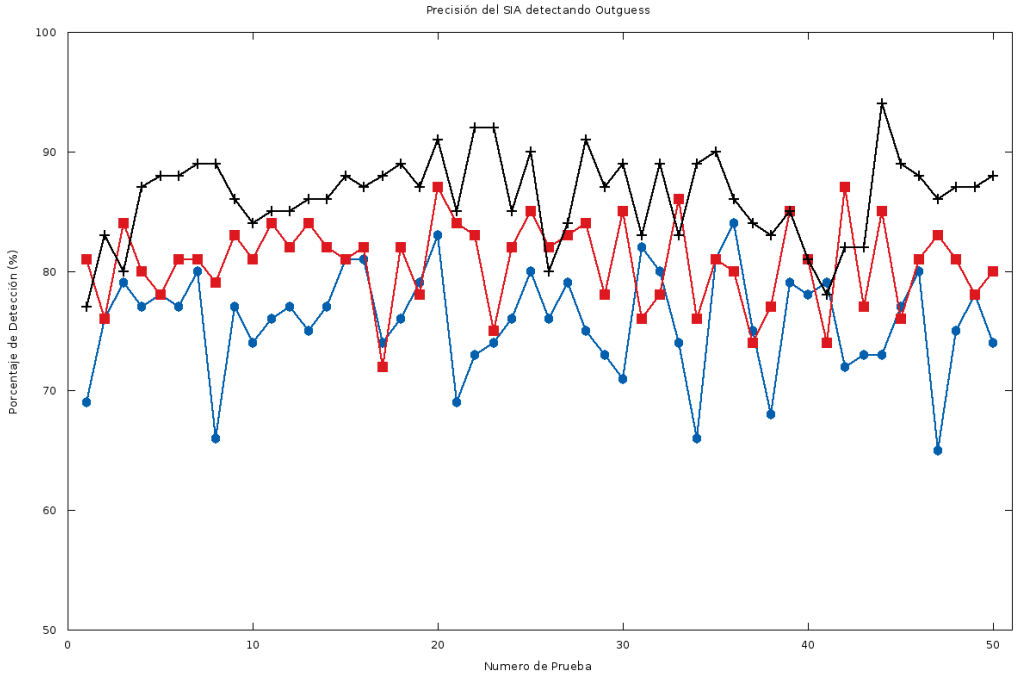

Fig. 5. Evolución de los detectores respecto a cada uno de los coeficientes utilizados

6. Discusión y conclusiones

Con los resultados en la tabla 3 y con los coeficientes gráficados en la figura 5, nos damos cuenta que si influye mucho la selección del vector de características que mejor caracterice a Outguess, vemos que el mejor coeficiente para la caracterización es CH, ya que se obtuvo una precisión del 94 % como mejor y una ponderada del 86.24 %. Comparándolos con los trabajos mencionados en el estado del arte, los resultados son competitivos. De esta manera demostramos que un clasificador de esteganogramas para Outguess basado en un sistema inmune artificial obtiene resultados competitivos iguales o mejores que los trabajos reportados en la literatura y que tiene un gran potencial como herramienta

de estegoanálisis, así como el uso de ondeletas de Harr para la caracterización de estos objetos con contenido oculto. Trabajo a futuro sería el probar este sistema para otras técnicas esteganográficas como F5 y Steghide, así como su implementación con un enfoque de detector universal, así como un análisis de sensibilidad de los parámetros del algoritmo.

Agradecimientos. Se agradece el apoyo del Instituto Politécnico Nacional a través de los proyectos de investigación SIP-20161234 y SIP-20160314.

Referencias

1. Böhme, R.: Advanced Statistical Steganalysis. Information Security and Cryptography, Springer Berlin Heidelberg (2010)
2. Castro, L.: Artificial immune systems : a new computational intelligence approach. Springer, London New York (2002)
3. Chen, M.C., Roy, A., Rodriguez, B.M., Agaian, S.S., Chen, C.L.P.: An application of linear mixed effects model to steganography detection. In: Systems, Man and Cybernetics, 2009. SMC 2009. IEEE International Conference on. pp. 1782–1786 (Oct 2009)
4. Dumitrescu, S., Wu, X., Wang, Z.: Detection of lsb steganography via sample pair analysis. IEEE Transactions on Signal Processing 51(7), 1995–2007 (July 2003)
5. Nievergelt, Y.: Wavelets made easy. Birkhauser, New York (2013)
6. Piotr Porwik, A.L.: The haar–wavelet transform in digital image processing:its status and achievements. MG&V 13(3) (2004)
7. Provos, N.: Defending against statistical steganalysis. In: Proceedings of the 10th Conference on USENIX Security Symposium - Volume 10. SSYM'01, USENIX Association, Berkeley, CA, USA (2001), http://dl.acm.org/citation.cfm?id=1251327.1251351
8. Sha, S.: Stegosploit: Hacking With Pictures (May 2015), https://conference.hitb.org/hitbsecconf2015ams/sessions/stegosploit-hacking-with-pictures/
9. Sindhu, S.S.S., Renganathan, R., Raman, P.J., Kamaraj, N.: Stegohunter: Steganalysis of lsb embedded images based on stego-sensitive threshold close color pair signature. In: Computer Vision, Graphics Image Processing, 2008. ICVGIP '08. Sixth Indian Conference on. pp. 281–288 (Dec 2008)
10. Stone-Gross, B.: Malware Analysis of the Lurk Downloader (Agust 2014), http://www.secureworks.com/cyber-threat-intelligence/threats/malware-analysis-of-the-lurk-downloader/
11. ThreatSolutions: Android malware employs steganography? Not quite... (January 2012), https://www.f-secure.com/weblog/archives/00002305.html
12. Timmis, J., Hone, A., Stibor, T., Clark, E.: Theoretical advances in artificial immune systems. Theoretical Computer Science 403(1), 11–32 (2008), http://www.sciencedirect.com/science/article/pii/S0304397508001059