Sistema de bloqueo automático para páginas web que incitan a la violencia a través de un algoritmo híbrido de aprendizaje computacional

Automatic locking system for websites that incite violence through a hybrid computational learning algorithm

Jorge Enrique Rodríguez*

Ángela Paola Herrera Domínguez**

Martha Liliana Rojas Olaya***

Fecha de recepción: 15 de abril 2013
Fecha de aceptación: 5 de mayo de 2013

Resumen

El artículo plasma un acercamiento al desarrollo de un proyecto de investigación orientado a la construcción de un algoritmo híbrido de aprendizaje computacional para el bloqueo automático de páginas web que incitan a la violencia a través de contenido snuff. En este, se hace una descripción de la situación actual del problema a resolver y se da a conocer un concepto de lo que es la minería y el aprendizaje computacional, a partir de ello se escogen tres algoritmos de trabajo similares al propuesto con el fin de analizar sus debilidades, fortalezas y aplicaciones.

Palabras clave: Sistema de bloqueo, aprendizaje computacional, minería web, violencia en internet.

* Ingeniería en Telemática – Universidad Distrital Francisco José de Caldas, Bogotá D.C, Colombia. Correo electrónico: jrodri@udistrital.edu.co

** Ingeniería en Telemática – Universidad Distrital Francisco José de Caldas, Bogotá D.C, Colombia. Correo electrónico: apherrerad@udistrital.edu.co

*** Ingeniería en Telemática – Universidad Distrital Francisco José de Caldas, Bogotá D.C, Colombia. Correo electrónico: mlrojaso@udistrital.edu.co

Abstract

In this paper we show the realization of a project that involves the creation of a hybrid learning algorithm for supervised computer automatically blocking websites that incite violence through snuff content. In this, there is a description of the current state of the problem to solve and provides a concept of what is mining and computational learning, on this basis, three algorithms are chosen similar to the proposed works, with the to analyze their weaknesses, strengths and applications.

Key words: Locking system, machine computational, web mining, Internet violence

1. Introducción

En países como Colombia las leyes que rigen la producción y comercialización de material audiovisual resultan insuficientes [1], razón por la cual las personas pueden acceder fácilmente al contenido violento, sobre todo a través de Internet donde se comparten recursos sin restricción alguna.

Aunque hoy en día las empresas disponen de políticas para el buen uso de los recursos corporativos por parte de los empleados, tener fácil acceso a páginas con contenido violento puede empeorar el consumo del ancho de banda existente y a su vez exponer la seguridad de la red ante diversos malware.

En este sentido es que para un administrador es de suma importancia mantener su red protegida de virus, espías y sobre todo limitar los recursos al uso corporativo, objeto sobre el cual fue diseñado. Es por ello que en el siguiente artículo se hará una revisión al desarrollo de un sistema de bloqueo automático como herramienta de apoyo al proceso de gestión en una red LAN, puesto que a través del análisis de un patrón de comportamiento con algoritmos de aprendizaje computacional supervisado se pueden detectar automáticamente y de manera constante nuevas páginas que, según su experiencia, indiquen contenido snuff.

2. Problema

Internet es una excelente herramienta de comunicación donde se puede adquirir información de diversas fuentes y con ello multiplicar el conocimiento, facilitando de esta manera que se creen nuevas tendencias hacia grupos que favorecen la investigación y el aprendizaje. Las fuentes generalmente se encuentran en diferentes ubicaciones geográficas, lo que es inadvertido para los cibernautas.

A su vez internet puede ser una tecnología peligrosa, ya que el acceder fácilmente a cualquier fuente de información puede conllevar a visitar páginas web de contenido que promocionan diferentes tendencias como el racismo, la xenofobia, terrorismo cibernético, grooming, ciberbullyng, sexting, pornografía infantil y trata de personas, entre otros. Además, en alguno de estos sitios web se hacen invitaciones al suicidio y al asesinato a

través del sadismo y el snuff (grabaciones de asesinatos reales).

Actualmente en Colombia las empresas proveedoras de telecomunicaciones ofrecen productos que bloquean contenido violento, por ejemplo la ETB (Empresa de Telecomunicaciones de Bogotá), ofrece el guardián de contenidos, donde los padres pueden administrar las páginas que podrán ser accesibles a sus hijos. Sin embargo cada día se crean nuevas páginas web de contenido violento, lo que implica ingresar cada una de estas url manualmente, tarea que resulta ser un poco tediosa.

Igualmente, en las redes LAN, los administradores deben hacer una verificación diaria de la creación de páginas web de contenido violento e ingresarlas manualmente en el squid para que sean bloqueadas a través de servidores proxy; al realizar esta labor algunas veces se carece de tiempo, lo que favorece la omisión de algunos sitios web cuyo contenido debería ser restringido.

3. Referentes sobre violencia

En [2], se señala que el desarrollo tecnológico ha creado una transformación de las respuestas culturales, políticas y sociales, de modo tal que la nueva cultura del acceso, la cibercultura, "está conectada, es instantánea, siempre está interactuando de alguna manera y su deseo básico no solo es conectarse sino crear un enlace inteligente, de manera que crea nuevas posibilidades" [2].

Los medios pueden contribuir a una cultura agresiva, las personas que ya son agresivas usan los medios como una confirmación adicional de sus creencias y actitudes, las que –a su vez– se ven reforzadas a través del contenido de los medios. Esta interacción es especialmente verdadera en los desarrollos a largo plazo [3].

La violencia presente en la web puede ser física, psicológica, sexual, económica, y social; todas estas modalidades se presentan en diferentes escenarios que se ven atacados por grupos o individuos que están manejando ventajosamente el anonimato y la inmediatez de compartir información, además de la comunicación en masa que ofrece la red. La violencia se ejerce en sectores tan diversos como el político, el social, el económico y el personal:

A. El sector social: en la red se pueden encontrar más de ochenta organizaciones raciales de diversos países que se alojan y protegen bajo el derecho a la libertad de expresión. Por ejemplo el Cyberhate (ciberodio), que se atestigua a través de banners con la imagen de los famosos martillos copiados de la película "El muro", la música de Pink Floyd y la foto de la chica skinhead que asegura ser "100% blanca".
La violencia social es ejercida principalmente por militantes y activistas radicales, fascistas, racistas, etcétera, quienes, a través del ciberespacio, envían propaganda, se organizan y multiplican. Pero esto solo es parte de lo que acontece en Internet.

B. El sector personal: en él se pueden destacar las mayores dificultades a enfrentar por las disciplinas de la salud, específicamente aquellas que conciernen al área de la psicología, pues en este escenario se vislumbran con más facilidad la complejidad e individualidad de cada ser. Aunado a lo anterior, el mundo virtual transforma y construye una realidad paralela de acuerdo a la disponibilidad de recursos y tiempo de cada usuario.

La nueva realidad de la que hablamos es el ciberespacio, en donde las amenazas virtuales son cosa diaria. No es raro encontrar portales que ofrecen dinero por laborar virtualmente para ellos en este tipo de actividades, lo que representa un riesgo para convertirse en adicto al Internet y desarrollador de estas prácticas de exclusión y violencia en la red.

Del mismo modo existen páginas que se especializan en la asistencia para el suicidio o en la orientación para continuar en un trastorno alimentario, como la anorexia o la bulimia. También la red ha hecho posible que negocios ilegales como la pornografía infantil, la pederastia y la trata de personas se encuentren al alcance de todos los cibernautas. Además de las páginas en donde se promocionan golpizas masivas, insultos o difamaciones para aquellos que consideran deben de desaparecer. A fin de cuentas, Internet se ha convertido en el medio perfecto de las venganzas anónimas, es así como los diversos ataques que puede uno recibir se manifiesten a través de correos electrónicos y spams (correos basura), o de páginas especiales para mandar amenazas a la integridad física a modo de broma (Jaramillo, 2006).

Internet es la única tecnología que alberga diversas personalidades, cada una de estas puede utilizarse a conveniencia, aun si esto representa ir en contra de los derechos humanos, tan solo depende de quién y para qué se utilice.

Con el crecimiento de Internet y su facilidad de acceso, se desarrolla igualmente una evolución convergente de contenidos violentos en la red. Con respecto a los foros de violentos la cuantía que llega a observar alguna de estas páginas son unas 18.000 personas al día. En cuanto a las páginas gore la cuantía de visitantes se calcula entre 80.000 y 150.000 al día por página. Y en cuanto a pornografía de violaciones la tasa de asistencia depende mucho del contenido de estas páginas y se calcula entre 2000 y 5000 visitantes al día en cada una de ellas [4].

4. Aprendizaje computacional

En el contexto de los sistemas artificiales el aprendizaje computacional se puede entender como un proceso por el cual los parámetros libres del sistema se adaptan a través de una estimulación continuada con el entorno para construir una cierta función de aplicación.

El aprendizaje computacional es un fenómeno que sucede a lo largo de un tiempo determinado, que puede corresponder a una cierta etapa dentro de la vida del sistema artificial o por el contrario que se pueda extender a lo largo de toda su vida. Habitualmente el tiempo en el que el sistema artificial aprende es limitado con relación a su tiempo de vida. Durante este intervalo, denominado fase de entrenamiento, el algoritmo de aprendizaje busca en su espacio de soluciones (o espacio de hipótesis) una solución compatible con un conjunto de muestras. Dicho conjunto se conoce con el nombre de conjunto de entrenamiento y corresponde a un número de ejemplos extraídos de un concepto c que se quiere modelar empíricamente. Este concepto corresponde a una función o comportamiento determinado del sistema artificial que se quiere construir de forma automática a través del algoritmo de aprendizaje.

Durante el periodo de aprendizaje el sistema buscará en el espacio de todas las posibles soluciones que sean capaces de ser construidas, una solución óptima con relación a alguna medida de coste de la que el propio sistema dispone, utilizando para ello recursos computacionales limitados [5].

4.1. Aprendizaje supervisado

El aprendizaje supervisado es aquel en el que el diseñador de redes neuronales ha de indicar a la red tanto las entradas como las salidas que desea obtener, es decir, el diseñador ha de mostrar a la red las entradas y corregir sus salidas para que coincidan con unas salidas deseadas. Los pesos de la red se regulan con el fin de obtener dicho resultado a través de un proceso que se denomina entrenamiento de la red [6].

Ejemplos de aplicación:

- Agrupación: obtención de grupos entre los datos.
- Extracción de características: obtención de características a partir de los datos de entrada.
- Reducción de dimensionalidad: los datos de entrada son agrupados en subespacios de una dimensión más baja que la inicial [7].

Con esta técnica de aprendizaje el entrenamiento consiste en presentarle a la red repetitivamente patrones de estímulos de entrada pertenecientes a un juego de ensayo. El juego de ensayo está formado por parejas "patrón de estímulos - respuesta correcta" y debe ser elegido cuidadosamente. Cada pareja se denomina hecho. En el juego de ensayo debe estar representada equilibradamente toda la información que la red necesite aprender.

Al realizar el entrenamiento la respuesta que da la red a cada patrón se compara con la respuesta correcta ante dicho patrón y, en virtud de esa comparación, se reajustan los pesos sinápticos. El reajuste de los pesos sinápticos está orientado a que, ante el patrón de entrada, la red se acerque cada vez más a la respuesta correcta.

Cuando ante un patrón de entrada la red de neuronas ya responde correctamente, se pasa al siguiente patrón del juego de ensayo y se procede de la misma manera.

Cuando se termina con el último patrón del juego de ensayo, se tiene que volver a empezar con el primero, ya que los pesos se han seguido modificando.

En casos sencillos, al cabo de unos pocos pasos de entrenamiento completos, con todos los elementos del juego de ensayo, los pesos sinápticos de todas las neuronas se estabilizan en torno a unos valores óptimos. Se dice entonces que el algoritmo de aprendizaje converge. Es decir, después de sucesivas presentaciones de todos los patrones estimulares del juego de ensayo, la red responderá correctamente a todos ellos, de esta manera se puede considerar entrenada y dar por terminada la fase de aprendizaje [8].

5. Minería web

La minería Web puede definirse como "descubrimiento y análisis de información útil procedente de la World Wide Web". Esta definición es bastante amplia e incluye tanto la búsqueda y recuperación de información en los millones de sitios web y bases de datos online, como el descubrimiento y análisis de patrones de acceso de los usuarios en uno o varios servidores web o servicios online (minería del uso de la web) pasando por el análisis de la propia organización de las páginas de un determinado portal o servidor web (minería de estructura).

Existen tres tipos de minería Web:

- Minería de uso: la minería de uso en la web (MUW) nace como una alternativa tecnológica a la personalización de la web. Su objetivo principal es modelar los patrones de comportamiento de

los usuarios que acceden a un sitio web determinado. De esta forma se logran caracterizar los diferentes segmentos de clientes que acceden al sitio web y explicar distintos fenómenos que pueden producirse relacionados con dicha segmentación; mejorar la organización y la estructura de los contenidos y servicios de un sitio web, de tal forma que cada cliente encuentre, de la manera más rápida posible, lo que necesita; y contribuir a la generación de visitas guiadas a los usuarios de tal forma que a cada usuario previamente caracterizado se le muestre realmente lo que necesita y se le proporcione una experiencia personalizada y fidelizadora.

- Minería de estructura: la minería de estructura web (WSM) trata de revelar cómo están relacionados los hipervínculos entre las distintas páginas para generar un informe estructural sobre la página y el sitio web. Además nos proporciona información acerca de si los usuarios encuentran la información, si la estructura del sitio es demasiado ancha o demasiado profunda, si los elementos están colocados en los lugares adecuados dentro de la página, si la navegación se entiende, cuáles son las secciones menos visitadas y su relación con el lugar que ocupan en la página principal.

  Típicamente tiene en cuenta dos tipos de enlaces: estáticos y dinámicos. La herramienta para realizar la WSM es la utilización de grafos, la cual nos permite reflejar el movimiento entre enlaces al navegar de una página a otra y así tener una mejor visión del conocimiento obtenido [9].
- Minería de contenidos: Este proceso se centra en la recogida de datos e identificación de patrones relativos a los contenidos de la web. Existen dos estrategias para la extracción del conocimiento; la minería de páginas web extrae patrones directamente de los contenidos existentes en las páginas. Estos documentos web pueden ser: texto libre, información procedente de bases de datos generadas en páginas con formato html, páginas escritas en xml, elementos multimedia y cualquier otro tipo de contenido presente en la web. La principal técnica de inteligencia artificial que se utiliza para realizar esta tarea es la utilización de técnicas de recuperación de información; la otra estrategia de extracción de conocimiento de contenidos de páginas web es la minería de resultados de búsqueda, la cual consiste en identificar patrones de comportamiento y características comunes en los archivos de sucesos de los servidores web.[10].

6. Algoritmos usados en problemas similares

6.1. Clasificador KNN (K-Nearest Neighbors)

El proyecto "Software para el filtrado de páginas web pornográficas basado en el clasificador KNN - UDwebporn", planteó el uso de un algoritmo para filtrar automáticamente páginas web, en este caso, páginas pornográficas. Para llevar a cabo dicha tarea se implementaron técnicas de minería de datos y algoritmos de aprendizaje incremental para el proceso de extracción, representación y clasificación de las páginas [11].

En este trabajo se realizó la selección del algoritmo KNN para la clasificación de las páginas con base a los resultados de las pruebas e implementaciones con otras técnicas para clasificación de hipertexto: Árboles de decisión C4.5 y NaiveBayes.

El algoritmo KNN ha sido ampliamente utilizado como un efectivo modelo de clasifica-

ción. Está basado en una función de distancia que calcula la diferencia o similitud entre instancias. Dada una instancia *x*, encierra sus *k* vecinos más cercanos: (*y1, y2,…,yk*) para asignarle la clase más común denotada por *c(x)* y determinada por la siguiente ecuación 1:

$$c(x) = \arg max_{c \in C} \sum_{i=1}^{k} \partial(c, c(y_i)) \qquad \text{Ecuación 1}$$

Donde $c\ (y_i)$ es la clase de y_i y ∂ es una función en donde $\partial\ (u, v) = 1$, si u = v. La función de distancia más utilizada es la distancia euclidiana, que se puede definir de la siguiente manera: la distancia euclidiana en medio de los puntos P= (P_1, P_2, …,P_n) y Q=(q_1, q_1, …, q_n); en un espacio n-dimensional se define la ecuación 2:

$$D(P, Q) = \sqrt{\sum_{i=1}^{n} (p_1 - q_1)^2} \qquad \text{Ecuación 2}$$

El algoritmo KNN tiene tres propiedades claves: es un método de aprendizaje perezoso (lazy), es decir que posterga la decisión de cómo generalizar los datos de entrenamiento hasta que una nueva instancia es observada; clasifica nuevas instancias analizando instancias similares e ignorando las diferentes; representa las instancias como puntos de valor real en un espacio euclidiano n-dimensional.

La complejidad computacional está dada por *O (np)* donde n es el número de instancias y p es el número de atributos. La implementación en la fase de clasificación de hipertexto hace referencia a la programación del algoritmo de aprendizaje computacional que permite determinar si una página web es pornográfica o no.

6.2. Clasificador basado en máquinas de soporte vectorial

El proyecto "POESIA (Public Open Source Environment for Safer Internet Access)" es financiado por la Unión Europea para una Internet más segura. Su objetivo es proveer a centros de educación un servicio de filtrado de contenidos inapropiados (páginas con pornografía o lenguaje obsceno, por ejemplo) evitando que menores de edad puedan acceder a este tipo de material.

Aunque el sistema incluye filtros para tratar 3 idiomas (inglés, italiano y español), a continuación se explica el módulo de filtrado para el castellano.

Este es un filtro ligero basado en aprendizaje estadístico que devuelve una respuesta en un tiempo corto, ya que el tiempo de respuesta es un factor crítico.

Usando esa representación se entrena un clasificador basado en Máquinas de Soporte Vectorial, un algoritmo de clasificación que selecciona de cada clase un pequeño número de instancias límite llamadas vectores soporte y construye una función lineal discriminante que las separa lo más posible.

Una vez que se tiene construido el clasificador, cada nueva instancia se clasifica aplicando el modelo, por ejemplo:

*-1.99 * sex – 0.35 * porn+ ...> 0 => Página segura*

Puesto que el filtro debe devolver un valor en forma de probabilidad (dato que utilizará el mecanismo decisor), y que las Máquinas de Soporte Vectorial no proporcionan ese tipo de resultados, se ajusta el anterior modelo mediante regresión lineal para poder obtener porcentajes [12].

La principal desventaja de SVM es la complejidad temporal del algoritmo. Siendo *m* el número de elementos del conjunto de entrenamiento, SVM resuelve un problema de programación cuadrática que implica ini-

cialmente complejidad $O(m^3)$. Múltiples investigaciones han propuesto métodos para mejorar esta complejidad llegando a que sea $O(m^2)$. [13]

6.3. Filtro Bayesiano

GFI MailEssentials™ es una galardonada solución de software de seguridad de correo y antispam para Exchange Server y otros servidores de correo que protege la red de virus y otras amenazas malware electrónicas. Proporciona un porcentaje de captura de spam de más del 99%, filtra el correo spam, las estafas phishing y los virus mediante varias capas de seguridad, incluyendo hasta cinco motores de antivirus y múltiples tecnologías de filtrado anti-spam, tal como dos motores anti-spam frecuentemente actualizados que no requieren ajustes, filtrado de reputación de IP, lista gris, protección de ataques de recolección de directorio y más [14].

El filtro bayesiano es una tecnología antispam utilizada en GFI MailEssential. Es una técnica adaptativa basada en algoritmos de inteligencia artificial, los cuales están diseñados para soportar la gama más amplia de técnicas de envío de correo no deseado disponible actualmente. El filtrado bayesiano se basa en el principio de que la mayoría de los eventos son dependientes; la probabilidad de que un evento ocurra en el futuro se puede deducir de las instancias anteriores de ese evento. GFI MailEssentials utiliza la misma técnica para identificar y clasificar el correo no deseado [15].

Antes de utilizar el filtrado bayesiano se debe crear una base de datos de palabras e indicios (por ejemplo, signo de $, direcciones IP y dominios, etc.). Esta información se puede recopilar a partir de una muestra de correos electrónicos no deseados y correos electrónicos válidos (denominados "HAM"). A continuación se asigna un valor de probabilidad a cada palabra o indicio basándose en cálculos que cuentan cuántas veces aparece una palabra en el correo no deseado en comparación con el HAM.

Lo anterior se hace analizando el correo electrónico saliente de los usuarios y el correo no deseado o desconocido: se analizan todas las palabras e indicios de ambos grupos de correo electrónico para generar el nivel de probabilidad de que una determinada palabra indique que el correo electrónico es no deseado. Esta probabilidad se calcula como en el ejemplo siguiente: Si la palabra 'hipoteca' aparece en 400 de 3.000 correos electrónicos no deseados y en 5 de 300 correos electrónicos legítimos, la probabilidad de que sea correo no deseado sería de 0,8889 (es decir [400/3000]/[5/300 + 400/3000]). Una vez creadas las bases de datos de HAM y de correo no deseado, se pueden calcular las probabilidades de las palabras y el filtro está listo para su uso [15].

La complejidad computacional en tiempo y espacio del clasificador bayesiano simple para el proceso de entrenamiento con n tuplas y k atributos es de $O(nk)$ y $O(k)$ respectivamente, mientras que el proceso de clasificación para m tuplas tiene un costo en tiempo de $O(mk)$. Esto hace que el método sea uno de los más eficientes en cuanto a complejidad se refiere [16].

Tabla 1. Comparación de algoritmos

	Fortalezas	**Debilidades**	**Aplicaciones**
Clasificador KNN	Las reglas de clasificación están basadas en la búsqueda de un conjunto de prototipos. No se necesita hacer ninguna suposición sobre los conceptos a aprender. Se pueden aprender conceptos complejos usando funciones sencillas como aproximaciones locales. Se puede extender el mecanismo para predecir un valor continuo (regresión). Es muy tolerante al ruido.	No hay un modelo global asociado a los conceptos a aprender El coste de encontrar los *k* mejores vecinos es alto. No hay un mecanismo para decidir el valor óptimo para *k* (depende de cada conjunto de datos). Su rendimiento baja si el número de descriptores crece. Su interpretabilidad es nula (no hay una descripción de los conceptos aprendidos).	Clasificador de datos con el fin de realizar filtraciones a una determinada información.
Clasificador basado en Maquinas de Soporte Vectorial	El entrenamiento es relativamente fácil. No hay óptimo local, como en las redes neuronales. Se escalan relativamente bien para datos en espacios dimensionales altos. El compromiso entre la complejidad del clasificador y el error puede ser controlado explícitamente. Datos no tradicionales como cadenas de caracteres y árboles pueden ser usados como entrada, en cambio de los vectores de características.	Se necesita una "buena" función *kernel,* es decir, se necesitan metodologías eficientes para sintonizar los parámetros de inicialización de la máquina de soporte vectorial.	Clasificador de datos con el fin de realizar filtraciones a una determinada información.
Filtro Bayesiano	Aprende mejor dado que examina todos los aspectos de un mensaje, en lugar de realizar el análisis de palabras clave. La auto-adaptación constante. El filtro Bayesiano evoluciona y se adapta a las nuevas técnicas de spam.	La mayoría de las listas de palabras clave solo están disponibles en inglés y son, por lo tanto, poco eficaces en regiones de habla diferente. Sensible al usuario.	Detección de correos spam y correos no deseados.

Fuente: elaboración propia

7. Conclusiones

El sistema de bloqueo automático se usa para controlar un flujo de información determinado a través de una restricción automática para el contenido no apropiado según requerimientos. En este caso la restricción automática es implementada por medio de un algoritmo híbrido de aprendizaje computacional; el contenido sobre el cual se hace la restricción es snuff.

En este artículo se hace una revisión al desarrollo de un sistema de apoyo para restringir automáticamente páginas web con contenido que incite a la violencia, planteando la viabilidad de un análisis futuro hacia la eficiencia del coste computacional de los cinco algoritmos con aprendizaje supervisado más utilizados actualmente y con ello conocer un comportamiento determinado para clasificar las páginas web con contenido snuff.

Este software se puede considerar como una novedosa herramienta telemática, ya que puede apoyar el proceso de restricción de páginas web cuyo contenido no es apto para una población en especial y los cuales pueden consumir recursos de la red para los cuales no fue diseñado.

8. Trabajos futuros

Construir un software de bloqueo automático para páginas web que incitan a la violencia a través de un algoritmo híbrido de aprendizaje computacional.

9. Referencias

[1] Especial – Snuff, el placer de lo real. [En línea]. La lupa, opinión al detalle. [Citado en septiembre del 2.012]. Disponible en internet <http://lalupaopinion.blogspot.com/2010/07/especial-snuff-el-placer-de-lo-real.html>

[2] TRUJANO RUIZ, Patricia, DORANTES SEGURA, Jessica y TOVILLA QUESADA, Vania. Violencia en Internet: nuevas víctimas, nuevos retos. liber., ene./jun. 2009, vol.15, no.1, p.7-19. ISSN 1729-4827. [Citado en Septiembre del 2.012]. Disponible en internet <http://pepsic.bvsalud.org/scielo.php?pid=S1729-48272009000100002&script=sci_arttext&tlng=en>

[3] UNESCO. Proyecto Principal de Educación en América Latina y el Caribe. Boletín 49. Publicaciones OREALC, 1999. 80p. ISSN 1014-5133.

[4] Violencia y Difusión [En línea]. Universidad Politécnica de Valencia. [Citado en Septiembre del 2.012]. Disponible en internet http://es.scribd.com/doc/21606538/VIOLENCIA-Y-DIFUSIONDarkRoom

[5] BERMEJO SANCHEZ, Sergi. Desarrollo de robots basados en comportamiento. 1 ed. Ediciones de la Universidad Politénica de Catalunya, 2003. 234p. ISBN 84-8301-721-1

[6] ZURRIETA, Asier. Aplicación de las técnicas de redes neuronales para el diagnóstico on-line del proceso de electroerosión por hilo[En línea]. [Citado en Septiembre del 2.012]. Disponible en internet. <http://www.disa.bi.ehu.es/spanish/profesores-etsibilbo/~jtpcaaxi/PFC/wwwANN/aprendizaje_de_las_ann.htm#_Toc136065875>

[7] FERNÁNDEZ REBOLLO, Fernando y BORRAJO MILLÁN, Daniel. Aprendizaje Automático [En línea]. Open CourseWare. [Citado en Septiembre del2.012]. Disponible en internet <http://ocw.uc3m.es/ingenieria-informatica/aprendizaje-automatico/material-de-clase-1/aa-ocwredes-no-supervisadas.pdf>

[8] Aprendizaje supervisado [En línea]. [Citado en Noviembre del 2.012]. Disponible en internet <http://sabia.tic.udc.es/mgestal/cv/RNAtutorial/node17.html />

[9] PANIAGUA ARIS, Enrique. La Gestión Tecnológica del Conocimiento. 1 ed. Servicio de Publicaciones, Universidad de Murcia, 2007. 321p. 978-84-9371-661-8

[10] Explotación de datos del Web Mining[En línea]. [Citado en Septiembre del 2.012]. Disponible en internet <http://gamoreno.wordpress.com/2007/08/24/explotacion-de-datos-del-webmining/>

[11] RODRÍGUZ, Jorge. BAUTISTA, Sandra. BARRERA, Harry. Software para el filtrado de páginas web pornográficas basado en el clasificador KNN - UDWEBPORN. Revista Avances en Sistemas e Informática – Universidad Nacional de Colombia sede Medellín. ISSN 1657-7663. Volumen 8 Número 1 de marzo de 2011.

[12] GARCÍA DÍAZ, Elkin. BoostingSupport Vector Machines [En línea]. Revista de Ingeniería SCielo. [Citado en Marzo del 2.013].Disponible en internet <http://www.iadis.net/dl/final_uploads/200405C024.pdf>

[13] Filtrado de contenidos web en español dentro del proyecto POESIA [En línea]. International Associationfordevelopment of theinformationsociety. [Citado en Septiembre del 2.012].Disponible en internet<http://www.iadis.net/dl/final_uploads/200405C024.pdf>

[14] Elimine el spam y proteja su red de virus y otras amenazas de correo. [En línea]. [Citado en Marzo de 2013]. Disponible en internet <http://www.gfihispana.com/exchange-server-antispamantivirus>

[15] Filtro bayesiano. [En línea]. [Citado en Marzo de 2013]. Disponible en internet <http://support.gfi.com/manuals/es/me2010/me2010acmanual_ES.1.54.html>

[16] RAMÍREZ ARELLANO, Aldo. Construcción y validación de unmodelo bayesiano para la clasificación de metas como apoyoa la planeación.Caso de estudio: Programa Operativo Anual

(POA) del Instituto Politécnico Nacional [En línea]. Instituto Politécnico Nacional. [Citado en Marzo del 2.013].Disponible en internet <http://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&ved=0CEUQFjAD&url=http%3A%2F%2Fitzamna.bnct.ipn.mx%3A8080%2Fdspace%2Fbitstream%2F123456789%2F9623%2F1%2F348.pdf&ei=TTZCUfHROKXq2QWq24CgBw&usg=AFQjCNGamPx0FXm1OI3MNvTCLfY43szaSw&sig2=HzcUQpLZotQ7YP3SjUyBYw>