ARBOR Ciencia, Pensamiento y Cultura
Vol. 189-760, marzo-abril 2013, a021 | ISSN-L: 0210-1963
doi: http://dx.doi.org/10.3989/arbor.2013.760n2007

LINGÜÍSTICA COMPUTACIONAL Y ESTEGANOGRAFÍA LINGÜÍSTICA. DISTRIBUYENDO INFORMACIÓN OCULTA CON RECURSOS MÍNIMOS

COMPUTATIONAL LINGUISTICS AND LINGUISTIC STEGANOGRAPHY. DISTRIBUTING HIDDEN INFORMATION WITH MINIMAL RESOURCES

Alfonso Muñoz Muñoz
Universidad Politécnica de Madrid
Departamento de Ingeniería y Arquitecturas Telemáticas
Escuela Universitaria de Ingeniería Técnica de Telecomunicación
amunoz@diatel.upm.es

Irina Argüelles Álvarez
Universidad Politécnica de Madrid
Departamento de Lingüística Aplicada a la Ciencia y a la Tecnología
Escuela Universitaria de Ingeniería Técnica de Telecomunicación
irina@euitt.upm.es

Cómo citar este artículo/ Citation: Muñoz, A.; Argüelles, I. (2013). Lingüística computacional y esteganografía lingüística. Distribuyendo información oculta con recursos mínimos. *Arbor*, 189(760):a021. doi: http://dx.doi.org/10.3989/arbor.2013.760n2007

Recibido: 18 julio 2012; Aceptado: 3 diciembre 2012.

RESUMEN: La lingüística computacional puede ser aprovechada junto a la ciencia de la esteganografía lingüística para diseñar sistemas útiles en la protección/privacidad de las comunicaciones digitales y en el marcado digital de textos. No obstante, para poder llevar a cabo tal tarea se requiere de una serie de condiciones que no siempre se dan. En este artículo se investiga si es posible diseñar procedimientos que permitan ocultar información en lenguaje natural utilizando la mínima cantidad de recursos tanto lingüísticos como computacionales. Se propone un algoritmo y se implementa, razonando posteriormente a favor de la utilidad y la seguridad de propuestas de este tipo.

PALABRAS CLAVE: Esteganografía lingüística; marcado digital; NLW; algoritmo.

ABSTRACT: Computational linguistics and linguistic steganography could allow to design useful systems in the protection / privacy of digital communications and digital language watermarking. However, building these systems is not always possible provided a series of conditions are not met. This article investigates whether it is possible to design procedures to hide information in natural language using minimal linguistic and computational resources. An algorithm is proposed and implemented, arguing for the usefulness and security of such proposals.

KEYWORDS: Linguistic steganography; watermarking; NLW; algorithm

1. LINGÜÍSTICA COMPUTACIONAL Y ESTEGANOGRAFÍA LINGÜÍSTICA. OCULTANDO INFORMACIÓN EN EL LENGUAJE NATURAL

El advenimiento de los sistemas informáticos y especialmente de la interconexión de las redes de telecomunicaciones ha dado a la información textual un protagonismo notorio. Aunque vivimos en un mundo multimedia, es cierto que la información textual está presente en todos los sitios e Internet y las redes de telefonía es buena muestra de ello: periódicos online, páginas web, correos electrónicos, mensajería instantánea, blogs, redes sociales, SMS, voz transcrita automáticamente a texto, etc. Procesar adecuadamente la información textual repercute en una gran variedad de aplicaciones con utilidad real.

En la última década, bajo el paraguas de la lingüística computacional se ha aprovechado el conocimiento disponible en áreas como el análisis del discurso, la lingüística de corpus, la lexicografía o la estadística de palabras, para su aplicación a tecnologías muy diversas como los algoritmos de reconocimiento del habla, los sistemas de traducción automática, sistemas de minería de datos, algoritmos de análisis ortográficos, resumen automático de textos, compresión de datos, recopilación y sintetización de información en tareas de inteligencia (Raskin, Nirenburg, Atallah, Hempelmann y Triezenberg, 2002), etc.

Aunque los trabajos más significativos son de la primera década del siglo XXI, más recientes son las propuestas que aprovechándose de todo este conocimiento proponen nuevos mecanismos de protección y anonimato en comunicaciones digitales. Un ejemplo puede ser el diseño de sistemas que mediante el uso del lenguaje natural permiten crear sistemas de memorización de claves de acceso (*password*) más seguros, claves más difíciles de deducir por un atacante pero fáciles de memorizar para el usuario legítimo (Atallah, McDonough, Raskin y Nirenburg, 2000).

En el campo de la protección de comunicaciones digitales la lingüística computacional tenía, en principio, poca utilidad. A menudo la ciencia de la criptografía que se define como el arte y ciencia de hacer una información ilegible a un tercero que no disponga de una clave, cubría la mayor parte de las necesidades de protección en servicios y protocolos telemáticos, minimizando ataques de revelación, anulación o alteración de información intercambiada (Kahn, 1996). No obstante, la criptografía tiene un problema destacable, su visibilidad. Cuando alguien protege (cifra) una información mediante criptografía puede detectarse esa comunicación cifrada, una comunicación no legible, aunque no por ello se pueda recuperar el contenido original sin la clave criptográfica. Existen escenarios donde detectar el uso de criptografía puede ser un problema y los atacantes pueden actuar en consecuencia, por ejemplo, en un estado censor prohibiendo la comunicación entre las entidades que se comunican de esta forma. Dado la necesidad de complementar la ciencia de la criptografía en estos escenarios, surge históricamente el interés en el uso de la esteganografía (ocultar información) y el estegoanálisis (detectar información oculta).

La ciencia de la esteganografía puede definirse como la ciencia y el arte de ocultar una información dentro de otra, que haría la función de tapadera o cubierta, con la intención de que no se perciba ni siquiera la existencia de dicha información (Kahn, 1996; Cox, 2007). La ciencia de la esteganografía es complementaria a la ciencia de la criptografía; esta última si bien no oculta la existencia de un mensaje, sí lo hace ilegible para quien no esté al tanto de un determinado secreto, una clave. En la práctica ambas ciencias pueden combinarse para mejorar la autenticidad y privacidad de las comunicaciones.

A lo largo de la historia se han propuesto múltiples formas de cubiertas para no levantar sospechas y que no se detecte la información ocultada (Kahn, 1996; Cox, 2008). Cuando la cubierta o tapadera es un texto en lenguaje natural se habla de un tipo concreto de esteganografía, la esteganografía textual. Cuando un texto se modifica o se genera basándose en una información a ocultar al resultado de tal operación se le denomina estegotexto, estegotexto que debe ser legible.

La ocultación de información utilizando mensajes en lenguaje natural no es ni mucho nueva, a lo largo de la historia se han documentado diversos métodos y tapaderas para hacerlo: en cartas, libros, telegramas, poemas, canciones, artículos de periódicos, etc. Por ejemplo, el *newspaper code* en la época victoriana o la reja de Cardano en el siglo XVI (Kahn, 1996). Hoy día, estas técnicas son comúnmente clasificadas bajo códigos abiertos[1] *o* semagramas textuales[2] dentro de la esteganografía textual (Kahn, 1996).

En nuestros días, parece interesante recuperar estas ideas para utilizar mensajes en lenguaje natural para ocultar información. Este tipo de técnicas podrían dificultar en gran medida la detección de información oculta dado el gran volumen de información textual que se intercambia en las redes. Adicionalmente, al volumen de información que debería ser capaz de procesar un potencial analista, se suma el perfeccionamiento de la esteganografía textual mediante el uso de diversos principios de la lingüística computacional, dando lugar a la ciencia de la esteganografía lingüística (Bergmair, 2007).

Una vez introducidos los conceptos básicos utilizados en el presente artículo, el apartado 2 incluye una breve introducción a la ciencia de la estegano-

grafía lingüística que permitirá comprender y acotar los resultados expuestos posteriormente. El apartado 3 plantea la problemática de las propuestas de esteganografía lingüística actual y se realiza una hipótesis sobre la posibilidad de diseñar sistemas que utilicen un conjunto de recursos lingüísticos mínimos. Este apartado da lugar a una propuesta de algoritmo. El apartado 4 recoge la experimentación al implementar el algoritmo. Se razonan aspectos relativos a la seguridad estadística y a la calidad lingüística de los estegotextos producidos. El apartado 5 concluye el artículo destacando los resultados más significativos de la tendencia investigada.

2. INTRODUCCIÓN A LA ESTEGANOGRAFÍA LINGÜÍSTICA

En la última década, las ideas clásicas agrupadas en torno a la esteganografía textual han dejado paso a nuevas propuestas más robustas y seguras agrupadas bajo la ciencia de la esteganografía lingüística (Bergmair, 2007). La ciencia de la esteganografía lingüística puede definirse como aquel conjunto de algoritmos robustos que permiten la ocultación de información, típicamente binaria, utilizando textos en lenguaje natural como tapadera. Esta ciencia utiliza principios de la ciencia de la esteganografía e incorpora recursos y métodos de la lingüística computacional como análisis automático del contenido textual, generación automática de texto, análisis morfosintácticos, lexicografía computacional, descripciones ontológicas, etc., para crear procedimientos públicos no triviales según los principios de Kerckhoffs (Kerckhoffs, 1883). Es decir, la seguridad de estos algoritmos dependerá exclusivamente de una pequeña información secreta, una clave, compartida por el emisor y el receptor. El algoritmo de ocultación será público, es decir, conocido por todos, incluso el potencial analista, y los estegotextos resultantes deberán ser resistentes a ataques estadísticos y lingüísticos (coherencia, estructura gramatical, etc.) tanto por software automatizado como por analistas humanos. Como se puede deducir, y queda demostrado en la literatura (Lingyun, 2007, 2011; Lingjun, 2008; Zhi-li, 2008a, 2008b; Chen, 2008; Meng, 2008, 2009, 2010; Zhenshan, 2009), esta tarea no es nada sencilla y depende mucho de la cantidad de información que se quiere ocultar y del texto modificado o generado para producir el estegotexto resultante.

El interés en esta ciencia se debe a que puede dar solución a dos problemas comunes: privacidad/anonimato y marcado digital de textos. Para ello se utilizan dos grandes familias de algoritmos clasificados en técnicas de generación automática de estegotextos y técnicas de modificación de textos existentes.

a) Técnicas de generación automática de estegotextos

Este tipo de técnicas permite generar automáticamente textos en lenguaje natural que ya ocultan la información deseada. Los dos procedimientos típicos documentados para generarlos, en ocasiones combinados, consisten en imitación gramatical de textos de referencia, por ejemplo el uso de *Probabilistic Context-Free Grammars* (PCFG) (Chapman, 1997, 2001; Zuxu, 2007; Blasco, 2008), o la imitación estadística de textos de referencia, como por ejemplo el método de Peter Wayner o variantes (Wayner, 1992, 1995; Tenembaum, 2002; Muñoz, 2010).

Esta línea de investigación es útil para la creación de canales ocultos de información y por tanto útil en el ámbito de la privacidad y el anonimato en comunicaciones. No obstante, aunque suena excitante, este tipo de propuestas son de enorme complejidad en la práctica, ya que si bien es posible conseguir textos con validez léxica y sintáctica no se conoce una propuesta que dé estegotextos de calidad si se analizan aspectos semánticos o de coherencia global del estegotexto generado (Bergmair, 2007).

Independientemente del estado actual de la tecnología en este aspecto, las propuestas de este tipo requieren de modelos estadísticos del lenguaje utilizado o textos de entrenamiento de los cuales "calcularlos". A estos modelos se les une la necesidad, al menos, de analizadores morfosintácticos, recursos léxicos y etiquetadores.

Por desgracia, no se conocen trabajos rigurosos que analicen el potencial de esta línea de investigación en lengua española. El único conocido fue desarrollado por los autores de esta investigación en 2010, evolucionando la propuesta del método de Peter Wayner, publicando la herramienta Stelin (Muñoz, 2010). Esta herramienta de libre disposición permite generar automáticamente textos en español que ocultan información. El procedimiento de ocultación se basa en la imitación estadística de textos de referencia y en el uso de modelos N-Gram. Adicionalmente, la herramienta permite manualmente mejorar la calidad del estegotexto generado sin necesidad que el receptor de dicho mensaje conozca los cambios introducidos manualmente. Actualmente esta tecnología permite generar estegotextos de gran calidad en textos de tamaño medio, centenas de palabras, donde se consigue ocultar pocas centenas de bits.

b) Técnicas de modificación de textos existentes

Las técnicas más tradicionales de ocultación de información consisten en utilizar un texto existente y ocultar la información mediante la modificación de elementos del mismo. En la última década se han propuesto multitud de técnicas (Bergmair, 2007), no

exentas de problemas, para lenguajes de todo tipo: inglés, español, japonés, chino, árabe, ruso, etc. Aunque este tipo de técnicas se pueden utilizar para la protección y anonimato de comunicaciones la comunidad científica tiene más interés en su aplicación como marcado digital de textos, *Natural Language Watermarking (*NLW) (Bergmair, 2007).

En la actualidad, la integridad y autenticidad de un mensaje puede ser garantizada mediante una firma digital. En general, las firmas digitales son procedimientos que generan una información extra, basada en la información que se desea proteger y añadida a ella. Por lo tanto, estos procedimientos tienen la desventaja de que la información generada no está autocontenida, lo cual significa que podría ser separada y provocar un error de verificación. La ocultación de información en un texto en lenguaje natural, si la modificación no supone alteraciones notables, facilitaría la incorporación de firmas autocontenidas. Estas firmas en un artículo podrían garantizar que el texto es exactamente el que el autor escribió, demostrar la autoría (*authorship proof*) o facilitar la medición de la difusión de una obra. Independientemente del objetivo perseguido existen 5 tendencias a la hora de modificar textos existentes para ocultar información.

b1. Modificaciones léxicas

Estos procedimientos consisten en la ocultación de información mediante la sustitución/modificación de palabras. El método más analizado es la sustitución basada en el uso de sinónimos. Desde que esta idea fuera trabajada por Chapman y Davida (Chapman, 1997) es considerada como una excelente opción y estudiada en diversas lenguas (Bergmair, 2007). El mayor problema con esta técnica es que, o no existen, o son muy pocos los sinónimos puros en una lengua, es decir, dos palabras que signifiquen exactamente lo mismo en cualquier contexto. Por este motivo, conseguir herramientas prácticas con estos principios, ya sea para ocultación de información en general o para el marcado digital de textos, requiere de sofisticados mecanismos para determinar cuál es la ambigüedad de una palabra en un contexto determinado y para saber si puede ser reemplazada o no por otra palabra (Chen, 2008; Meng, 2008; Zhenshan, 2009). Para ello, se requieren procedimientos WSD (*Word Sense Disambiguation*) y estudios estadísticos que indiquen cuáles son los más aconsejados de entre los sinónimos disponibles para una palabra.

b2. Modificaciones Sintácticas-Semánticas

Estos procedimientos se basan en alterar la estructura sintáctico-semántica de un texto para ocultar información. Ejemplos de este tipo de modificación en lenguas tan dispares como el inglés, chino, coreano, turco, ruso o persa son: el cambio de voz activa/pasiva, el movimiento de los adverbios dentro de la oración, el cambio de orden de los términos unidos por conjunciones como en listo y guapo o guapo y listo, etc. La literatura demuestra que este tipo de soluciones son más resistentes a ataques activos, ataques que modifican una palabra por otra, ya que ocultan la información a nivel de estructura no exclusivamente a nivel léxico (Bergmair, 2007).

Los únicos estudios significativos que se conocen de la aplicación de estos procedimientos en lengua española están publicados en (Muñoz, 2009, 2012). En estos, se profundiza en la posibilidad de utilizar la sintaxis en lengua española para enmascarar información, en concreto se analizan transformaciones sintácticas basadas en el cambio de activa a pasiva, transformaciones basadas en el movimiento de los adjetivos y otros complementos dentro del sintagma nominal y transformaciones basadas en la reordenación de complementos del verbo.

b3. Traducción de una lengua a otra

El objetivo de estos procedimientos es ocultar información aprovechándose de la existencia de más de una frase o enunciado equivalente de un idioma origen a un idioma destino. La elección de una de las frases posibles entre las disponibles permite crear un sistema binario de ocultación (Grothoff, 2005; Meng, 2010).

b4. Errores ortográficos y tipográficos. Abreviaturas y signos de puntuación

Los procedimientos que utilizan las "comodidades" en la forma del habla o de la escritura (errores, abreviaturas, signos de puntuación indebidos) son muy útiles desde el punto de vista esteganográfico (Topkara, 2007), especialmente si las modificaciones generan un texto que se distribuye en un canal donde dichas modificaciones sean frecuentes, por ejemplo, errores ortográficos en foros de internet. Si bien es cierto que pueden aplicarse tecnologías existentes para detectar la presencia masiva de tales errores o características: por ejemplo, software detector de errores ortográficos, análisis gramaticales, etc.

b5. Ocultación basada en la estructura y el formato de un texto

Este tipo de técnicas son las más antiguas que han sido documentadas (Kahn, 1996). Típicamente se utilizan caracteres invisibles, la separación entre líneas o entre palabras, o la codificación basada en cambios sucesivos del formato del texto**.** Estos mecanismos facilitan la ocultación de grandes cantidades de bits pero no están exentos de problemas. Es común ver cómo ataques activos como reemplazar una palabra por otra, pueden anular la información oculta de forma sencilla. En los últimos años, especialmente por el

ARBOR Vol. 189-760, marzo-abril 2013, a021. ISSN-L: 0210-1963 doi: http://dx.doi.org/10.3989/arbor.2013.760n2007

interés de la comunidad científica china en estegoanálisis de estegotextos, múltiples propuestas se han publicado para la detección de este tipo de técnicas (Lingyun 2007; Huang 2007a, 2007b; Huang 2007; Lingjun 2008).

Independientemente de la técnica concreta, la tendencia en las técnicas de modificación de textos existentes es hacia propuestas basadas en modificaciones léxico-semánticas y sintáctico-semánticas (Bergmair, 2007), centrándose especialmente en aspectos semánticos y ontologías. Los nuevos sistemas del futuro deberían permitir construir sistemas software automatizados más realistas frente a ataques estadísticos y lingüísticos, generando estegotextos con una apariencia adecuada y que respeten las normas básicas de cohesión y coherencia para que no puedan ser detectados ni siquiera por un analista humano.

3. DISTRIBUYENDO INFORMACIÓN OCULTA CON RECURSOS MÍNIMOS. HIPÓTESIS

Los procedimientos y referencias documentadas en el apartado anterior reflejan el estado actual de la tecnología aplicada a la ciencia de la esteganografía en diferentes idiomas (en menor caso para lengua española al no estar tan estudiada). Estos trabajos permiten concluir que son necesarios multitud de recursos específicos para un lenguaje dado para llevar este tipo de algoritmos a buen puerto, algoritmos que no generan, a día de hoy, estegotextos "humanamente perfectos" y que sólo permiten ocultar unas pocas centenas de bits para textos de una cierta calidad. Entre los recursos comúnmente utilizados se encuentran: etiquetadores, traductores, analizadores morfosintácticos, modelos estadísticos, ontologías, desambiguadores, diccionarios de palabras, etc.

En función de la lengua en cuestión, será más o menos difícil encontrar los recursos necesarios para desarrollar nuestro algoritmo esteganográfico. Nuestras investigaciones en lengua española demuestran cómo se han tenido que desarrollar recursos propios no disponibles o existentes pero licenciados/patentados. Este tipo de esfuerzos, dificultan y ralentizan la investigación en propuestas de este tipo.

Por este motivo, en este trabajo, se analiza la posibilidad de desarrollar algoritmos que utilicen un mínimo de recursos lingüísticos y computacionales. Tan mínimo como alcanzar la ausencia de los mismos. La limitación de estos recursos podría estar debida al entorno o "canal hostil" donde se desee realizar la comunicación o a limitaciones de los dispositivos (software o hardware) utilizados para comunicaciones entre emisor y receptor. Si este tipo de algoritmos fuera factible se analizaría su capacidad para ocultar información y si realmente son prácticos.

3.1 Hipótesis. Algoritmo de esteganografía lingüística basado en la ausencia de recursos lingüísticos y tecnologías de lingüística computacional.

La creación de un algoritmo de esteganografía lingüística, con una cierta "robustez", basado en la ausencia de recursos lingüísticos y tecnologías de lingüística computacional tiene varios problemas. El más destacable es la generación de estegotextos de la mayor calidad posible de forma automatizada. Las investigaciones de detección de información oculta en textos demuestran que a menudo se detecta su presencia porque existen palabras que no encajan en un contexto dado desde un punto de vista semántico o gramatical. Habitualmente los algoritmos de detección se basan en textos escritos por humanos para entrenar sistemas que permitan diferenciar textos escritos por humanos y estegotextos escritos por algoritmos específicos. Sin duda, el reto actual consiste en conseguir textos con apariencia humana para una variedad de temáticas. Por tanto, si no tenemos recursos ni tecnologías ampliamente utilizadas en la lingüística computacional para conseguir engañar a un potencial analista, resulta en principio "imposible" hacer una propuesta seria en este sentido. No obstante, todavía es posible, al menos, pensar en una solución, con ciertos inconvenientes.

Supongamos la siguiente hipótesis: Un estegotexto es habitualmente detectado porque no fue escrito por una persona sino por una máquina (algoritmos de momento imperfectos). ¿Es posible que un humano escriba "a mano" un estegotexto y por tanto no pueda ser detectado? Si un humano escribe el estegotexto no necesitamos la mayor parte de los recursos lingüísticos y tecnologías de la lingüística computacional. Esta hipótesis puede ser llevada a la práctica, pero con una serie de inconvenientes en los que se profundizará en adelante, la más destacable, el tiempo de generación de estegotextos (automatización).

Para analizar la viabilidad de la hipótesis planteada se diseña un algoritmo basado en dos procedimientos: esteganografía basada en diccionario[3] y edición manual. La idea es sencilla:

> 1. Uno o más textos de referencia o fuente son seleccionados. Conocidos sólo por emisor y receptor. El texto fuente es divido en S_i grupos de W palabras en función de un clave secreta compartida entre emisor y receptor. Es decir, formamos grupos de palabras extrayéndolas de los textos seleccionados. La selección de qué palabras forman parte de cada grupo es pseudoaleatoria (para evitar patrones) y se hace en función de una clave criptográfica. Recuérdese que todo el algoritmo es público (principios de *Kerckhoffs*) y la seguridad depende sólo de una clave. Sin esta clave no se podrán formar los grupos de palabras.

2. De cada grupo se selecciona una palabra WS_i. El criterio de selección de la palabra, según los principios de esteganografía basada en diccionario, permitirá ocultar información.

3. El resultado final será una lista de palabras sin sentido aparente (sintáctico ni semántico).

4. El algoritmo permite añadir nuevas palabras (una o más) para ir conectando las palabras extraídas, de esta forma dar "validez lingüística" al estegotexto. El receptor de la información no necesita conocer las palabras introducidas manualmente por el emisor. El receptor tiene algún procedimiento para reconocer la posición exacta de las palabras que enmascaran información.

5. La única limitación para añadir nuevas palabras antes de cada palabra extraída es que la palabra elegida (manualmente) no se encuentre entre las W palabras posibles del grupo S_i del cual se ha extraído la palabra WS_i.

La idea es clara, automatizar la ocultación de la información y dejar al usuario libertad para crear manualmente el estegotexto que desee y conseguir que el receptor decodifique sin considerar las incorporaciones destinadas a mejorar la calidad del estegotexto. Se presupone que propuestas de este tipo harán muy difícil la detección de información oculta ya que será difícil la detección incluso para un analista humano (y no sólo para software de detección creado para tal fin).

4. DISTRIBUYENDO INFORMACIÓN OCULTA CON RECURSOS MÍNIMOS. MEDIDAS Y EXPERIMENTACIÓN

4.1 Decisiones de diseño. Implementación del algoritmo

En este apartado se destacan algunas decisiones de diseño consideradas para la implementación del algoritmo y la realización de medidas.

En general, el esquema de comunicación y todos los elementos involucrados quedan reflejados en la Figura 1.

El proceso para ocultar una información creando un estegotexto será el siguiente:

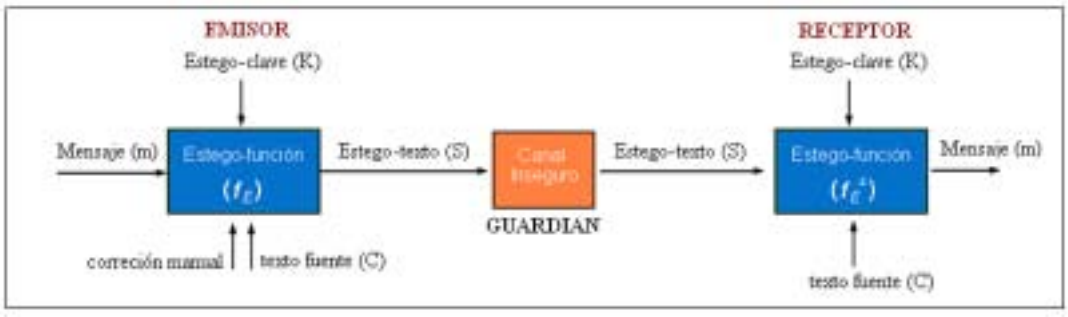
1. Seleccionar uno o más textos fuente (C). Este texto se toma como referencia para extraer palabras que formarán parte del estegotexto creado.

2. Seleccionar el mensaje m a ocultar. Se convierte a información binaria.

3. Seleccionar una clave criptográfica, compartida con el receptor. Desde un punto de vista lingüístico la clave criptográfica no es tan importante, pero sí lo es desde un punto de vista de la seguridad general. La clave es útil para cifrar la información a ocultar (una medida adicional de seguridad), en la creación de conjuntos de palabras desde el texto fuente y en la asignación de una codificación binaria a cada palabra dentro de cada grupo. Es interesante destacar este último aspecto. Por ejemplo, si tenemos ocho palabras dentro de un grupo, éstas se numerarán en binario desde 000 a 111 (las 8 posibilidades), como la información a ocultar, que está en binario, se recorre secuencialmente de principio a fin para ocultar toda la información se selecciona los 3 bits que correspondan, se compara con la codificación de las palabras del grupo y se extrae la que corresponde. Por ejemplo, m=111 y las palabras del grupo son "hola=000, árbol=001 … casa=110, rojo=111" se extraería la palabra "rojo". La decisión sobre qué codificación de las disponibles asignar a cada palabra del grupo se toma también en función de la clave. En la implementación realizada se ha utilizado el algoritmo criptográfico *Rijndael*, estándar AES (Daemen y Rijmen, 2002), de clave 256 bits y un generador pseudoaleatorio (*PRNG – Pseudo-Random Number Generator* -) basado en el mismo (AES en modo contador). Estos algoritmos son los recomendados actualmente en la protección de comunicaciones digitales.

4. Se corrige manualmente el estegotexto creado. La implementación genera una plantilla creada con las palabras presentes en cada grupo extraído del texto fuente (C).

Figura 1. Esquema de funcionamiento del algoritmo implementado



ARBOR Vol. 189-760, marzo-abril 2013, a021. ISSN-L: 0210-1963 doi: http://dx.doi.org/10.3989/arbor.2013.760n2007

5. Enviar/almacenar el estegotexto.

El proceso para recuperar la información oculta de un potencial estegotexto sería el siguiente:

1. Seleccionar el estegotexto que se supone tiene información oculta.

2. Seleccionar la misma clave criptográfica y texto fuente que el emisor.

3. Se construyen los grupos del texto fuente, al igual que lo hacía el emisor.

4. El software receptor (se podría hacer a mano) analiza el estegotexto esperando una de las palabras existentes en el primer grupo creado. Si no la encuentra va descartando palabras hasta que encuentre una palabra de las posibles de ese grupo, cuando encuentra una palabra anota su codificación binaria y selecciona el siguiente grupo. Este proceso lo repite hasta finalizar el estegotexto.

5. Si todo es correcto se extrae la información enmascarada por el emisor (la descifra también). Si no es así, lo más probable es que se recupere información sin sentido.

Una vez comprendido el funcionamiento general de la propuesta investigada es importante resaltar algunas decisiones realizadas en la implementación. La más significativa es la consideración, siempre, de grupos del mismo número de palabras (W) y que sea potencia de 2. Este criterio podría haber sido diferente pero de esta forma la implementación se simplifica y es más fácil manejar información binaria.

De esta forma, el proceso de ocultación consistirá en la selección de una palabra de cada grupo, de tal forma que cada segmento ocultará $\log_2 W$ bits. Según esto el número mínimo de palabras presentes en el estegotexto serán:

$$(1)\ N_{minW} = I_H / \log_2 W$$

donde N_{minW} es la información, número de bits, a ocultar (I_H) divido por el número de bits que representa cada palabra seleccionada para el estegotexto. Según esto el texto fuente de referencia deberá tener un tamaño mínimo de palabras de al menos:

$$(2)\ \text{Fuente Texto}_{min} = N_{minW} * W$$

Dadas estas condiciones, sería interesante ver qué número W de palabras es el más interesante por grupo. Si se analizan las formulas (1) y (2) cuanto mayor sea W el número de palabras aportadas al estegotexto será menor, lo cual es interesante para crear estegotextos pequeños, mientras que el texto fuente necesario será mayor. Además, si W es alto el número de palabras por grupo hará más difícil la posterior inclusión de palabras manualmente anteponiéndose a las palabras generadas y añadidas al estegotexto. Analizando las siguientes figuras (Figura 2 y Figura 3) para volúmenes de información de por ejemplo 60, 90, 128 y 256 bits, serían adecuados en una primera aproximación tamaños de W=4, W=8 o W=16 (balance entre tamaño y edición). Lógicamente, cuanto menor sea la información a ocultar más fácil será construir mensajes con una elevada seguridad. El valor de 128 a 256 bits, siendo reducido, permitiría ocultar alguna información con utilidad práctica como la distribución de claves criptográficas, urls, mensajes de movilización, coordenadas GPS, citas, etc.

Nuestras pruebas indican que W=8 es una buena decisión al equilibrar el número de bits que ocultará cada palabra seleccionada ($N_{bits\text{-}pal}=\log_2 8=3$ bits) con la facilidad de incorporar nuevas palabras para crear estegotextos con aceptabilidad lingüística (por cada grupo no se pueden seleccionar las 8 palabras presentes). Por tanto, con W=8 el texto de referencia se dividiría en grupos de 8 palabras no repetidas (W=8) elegidas pseudoaleatoriamente, palabras a las cuales se les asignaría una codificación en función de la clave configurada.

Figura 2. Numero de palabras añadidas al estegotexto ($N_{min}W$) para ocultar 60, 90, 128 y 256 bits (I_H) con diferentes números de palabras por segmento ($\log_2 W$)

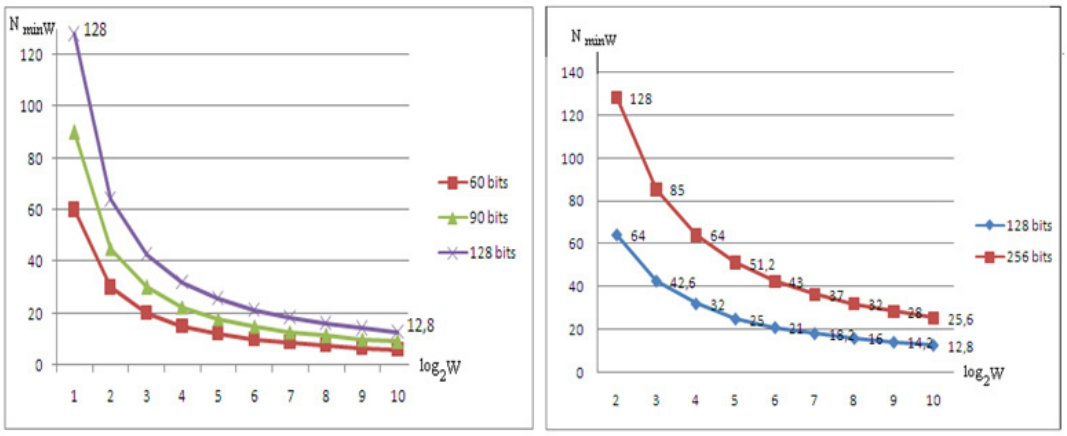
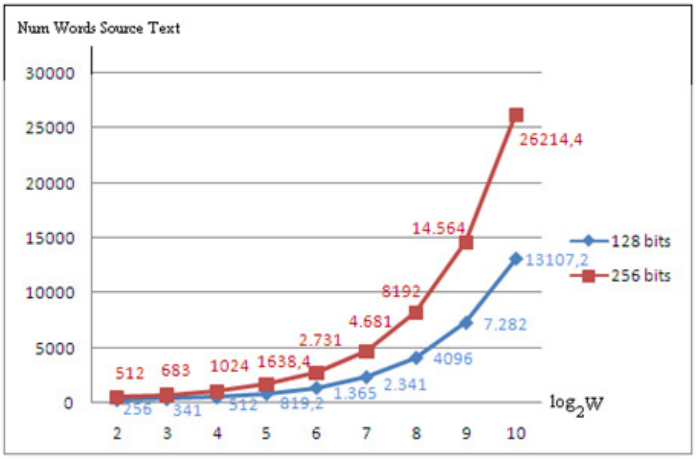


Figura 3. Número de palabras mínimas en texto de referencia para ocultar 128 o 245 bits. Fuente Textomin= (I_H/ $\log_2 W$)*W



Con este criterio, por ejemplo, si añadiéramos manualmente 2 palabras más por palabra añadida automáticamente al estegotexto tendríamos una media de capacidad de ocultación de 1 PALABRA-BIT en el total del estegotexto. En el mejor de los casos una frase con sentido en lengua española tendría un mínimo de tres palabras (nombre+verbo+complemento). Esta capacidad de ocultación es razonable comparada con otras propuestas publicadas (Bergmair, 2007)).

La capacidad de ocultación final dependerá de la capacidad editora del emisor y del tiempo de edición dedicado. La capacidad de ocultación media por palabra del estegotexto final puede ser descrita por tanto como:

$$N_{total\text{-}palabras\text{-}stegotexto} = P_{añadidas} + N_{palabras\text{-}generadas}$$

$$\text{Capacidad media} = N_{palabras\text{-}generadas} * O_{palabra\text{-}generada} / N_{total\text{-}palabras\text{-}stegote}$$

siendo $P_{añadidas}$ el número total de palabras añadidas manualmente, $N_{palabras\text{-}generadas}$ el número total de palabras generadas automáticamente y $O_{palabra\text{-}generada}$ representa el número de bits que se oculta por palabra generada ($\log_2 N$).

Para facilitar la edición al emisor, y por tanto la mejora de la calidad del estegotexto sin afectar significativamente al tamaño del estegotexto final, las palabras añadidas a cada grupo se ponen en minúsculas, sin signos de puntuación ni tildes (las palabras no pueden ser signos de puntuación), este hecho permite adaptar las palabras del estegotexto resultante en la manera deseada. Por ejemplo, añadir tres palabras manualmente, añadir un punto y a continuación poner la primera letra de una palabra seleccionada por el algoritmo en mayúscula. El receptor simplemente descarta los símbolos de puntuación, mayúsculas y tildes.

4.2 Experimentación. Ejemplo de estegotexto en español

En este apartado se propone un ejemplo del resultado de la aplicación del algoritmo propuesto. Para ello seleccionamos un texto en lengua española como referencia, el artículo de Derechos Humanos publicado en Wikipedia (Wikipedia_es, 2012), y ocultamos 42 bits de información (por ejemplo, una dirección IP de un servidor en el cual alguien quiere compartir información ilícita). Al aplicar el algoritmo tenemos las siguientes palabras y plantillas a modo de ejemplo, Figura 4 y Figura 5.

Figura 4. 14 palabras que ocultan 42 bits de información

> *"espacio idea intimidad colectivo sucedio distinguen caracteristicas entonces cierta plasman serie fe capacidad solidaridad"*

Una vez conocida la plantilla sólo es necesario invertir tiempo en la edición manual. El siguiente ejemplo fue realizado en unos 2 minutos, Figura 6. En negrita se destacan las palabras extraídas automáticamente, el resto es edición manual. En este caso la calidad resultante depende de la calidad de la escritura del emisor más que de las limitaciones del algoritmo. Puede observarse como el estegotexto producido no tiene nada que ver con el texto de referencia.

Analizando la Figura 6 y suponiendo una capacidad de ocultación (capacidad editora) de unos 0,3 bits/palabra observamos para W=8 y el mismo texto fuente lo siguiente, Figura 7.

En este punto ya se pueden destacar las ventajas e inconvenientes de propuestas de este tipo.

ARBOR Vol. 189-760, marzo-abril 2013, a021. ISSN-L: 0210-1963 doi: http://dx.doi.org/10.3989/arbor.2013.760n2007

Figura 5. Palabras presentes en cada segmento para el ejemplo seleccionado

espacio	aprehendidos|america|espacio|fernandezgaliano|virtualidad|legal|consagracion|correspondiente
idea	humanista|decidir|materia|religioso|experimento|idea|1287|precarias
intimidad	introdujo|realizado|sólo|6|ambas|retoma|intimidad|23
colectivo	colectivo|efectividad|cooperaciones|iusracionalista|cabida|iusnaturalismo[63]|xxiv|tendencias
sucedio	trabajos|objeciones|reconocimiento|monarca|otras|colectiva|decadencia|sucedió
distinguen	ningun|distinguen|entre|anarquismo|individual|muy|viene|gesto
caracteristicas	recogerlos|realizar|adecuado|recogia|mil|caracteristicas|que|recurrir
entonces	nociones|miembro|entonces|libertartum|relacionados|heredo|seno|reconocidos
cierta	agosto|sujeto|descolonizacion|cierta|apelan|emancipacion|perez|dio
plasman	plasman|sociedad|eficacia|encuentra|the|respuesta|pronuncian|posee
serie	detencion|pertenecen|integran|estatalmente[9]|plano|serie|durante|relaciona
fe	autores|conciliacion|contra|concreta|fe|evolucion|articulada|ramon|
capacidad	defensa|producido|capacidad|unifica|medieval|libre|cultura|consideraban
solidaridad	solidaridad|en|ideales|mitad|segun|simple|motivos|ultimos|

Figura 6. Ejemplo de estegotexto de 142 palabras y 42 bits ocultos. la capacidad medida de ocultación es de 0,2957 bits/palabra

Tu **espacio** virtual en Internet da una **idea** de cómo proteges tu **intimidad**. El **colectivo** stegoHACK y el colectivo rootedUp, que **sucedió** al grupo firstStego, **distinguen** diferentes **características** de los nuevos ataques a la privacidad que deberían ser considerados. Hace 10 años, **entonces** la seguridad informática era incipiente, los ataques eran muy minoritarios. Hoy día, es **cierta** la tendencia que afirma que los ataques se **plasman** especialmente hacia las redes sociales. Las redes sociales se componen de una **serie** de tecnologías que facilitan el intercambio de información y que se apoyan en la **fe** de los usuarios en que los datos intercambiados serán debidamente protegidos por el proveedor del servicio, aunque no siempre sea así. La **capacidad** de distribución de estas redes y la **solidaridad** de los internautas en el intercambio de archivos de todo tipo simplificará el trabajo de los atacantes.

Figura 7. Relación tamaño estegotexto final y tamaño de información a ocultar para el ejemplo dado

Tamaño información a ocultar	0,3 bits/palabras
16 bits	54 palabras totales
32 bits	107 palabras totales
64 bits	214 palabras totales
128 bits	427 palabras totales
256 bits	854 palabras totales

ARBOR Vol. 189-760, marzo-abril 2013, a021. ISSN-L: 0210-1963 doi: http://dx.doi.org/10.3989/arbor.2013.760n2007

Inconvenientes

El principal inconveniente viene del tiempo necesario para editar/perfeccionar el texto manualmente. No obstante, esto fue definido como una característica en el caso que no se disponga de otra alternativa. Es decir, hasta cierto punto esto no puede ser considerado un inconveniente e introduce una serie de ventajas que se verán a continuación.

La capacidad de ocultación aunque baja, nuestras pruebas reflejan márgenes de 0,2 bits/palabra hasta 1 bit/palabra, es comparable a otras propuestas que utilizan recursos varios (Bergmair, 2007).

Quizás el principal inconveniente sea la formalización de los resultados, ya que depende mucho de la capacidad editora del emisor, no tanto del texto de referencia. Las pruebas realizadas indican que es común necesitar entre 5 a 10 minutos para dejar un texto en forma "humana". Esta propuesta podría ser interesante para ocultar pocas decenas de bits hasta unos 128 bits si no se desea invertir mucho tiempo (pocos minutos), generando textos de pocas centenas de palabras. En unas decenas de bits se pueden ocultar información con utilidad práctica: como una localización por una coordenada GPS, un mensaje breve, una URL, una dirección IP, una clave criptográfica, etc.

Ventajas

El algoritmo puede funcionar sin la existencia de recursos y tecnologías tales como etiquetadores, desambiguadores, etc. La calidad del estegotexto depende de la edición manual del emisor creando stegotextos indistinguibles para las técnicas actuales de estegoanálisis. Recuérdese que las investigaciones previas detectaban información oculta comparando potenciales estegotextos con textos escritos por humanos y detectando anomalías (Lingyun 2007; Lingjun 2008; Huang 2007a, 2007b; Huang 2007; Meng, 2010; Chen, 2008; Meng, 2008; Zhenshan, 2009). Es interesante, además, que aunque esta investigación se centra en la lengua española, este algoritmo podría ser adaptado a otras lenguas. Por ejemplo, si utilizamos la versión en inglés del artículo de Derechos Humanos de la Wikipedia (Wikpedia_en, 2012) pueden crearse estegotextos como el siguiente, Figura 8, Figura 9 y Figura 10.

4.3 Seguridad del algoritmo implementado

Los ejemplos reflejados anteriormente permiten observar como es posible construir estegotextos completamente legibles. En este apartado se va a razonar sobre una serie de cuestiones adicionales de seguridad partiendo del siguiente escenario: el algoritmo de esteganografía propuesto es público (lo conoce el

Figura 8. Ocultamos 42 bits en 14 palabras necesitando un mínimo de 112 palabras del texto de referencia

intended decides societies number of hemisphere abusing and is expand invoked so name exercise

Figura 9. Lista de palabras disponibles en cada segmento de los 14 necesitados

intended	S_1:brought|questions|intended|respond|amendments|with|nature|removal
decides	S_2:new|decides|around|law[55]|liberator|critique|more|often
societies	S_3:vietnam|determined|generation|became|property[65][66]|wars|societies| Customary
number	S_4:number|saarc|contractualist|purposes|criticism|help|economical|term
of	S_5:manifestly|father|principal|successfully|of|reason|chief|main
hemisphere	S_6:say|hemisphere|assert[74]|distance|conceptions|quasijudicial|germany| York
abusing	S_7:by|enforcing|real|priorities|scholars|strong|terms|abusing
and	S_8:christianity|secure|absence|us|judge|natural|and|sanctions|
is	S_9: is|want|abstention|headquartered|once|adherence|free|west|
expand	S_{10}:expand|sovereignty|welfare|marx|achieved|supranational|really| Participation
invoked	S_{11}:illogical|march|sake|invoked|africas|discovered|six|classical
so	S_{12}:emancipation|principal|hypothetical|eighteen|proceeded|year|so|laws
name	S_{13}:directly|structures|name|marx[citation|keeping|divisions|citizens|unanimously
exercise	S_{14}:signed|ironic|occurred|19th|interpretations|universalist|europe|exercise

ARBOR Vol. 189-760, marzo-abril 2013, a021. ISSN-L: 0210-1963 doi: http://dx.doi.org/10.3989/arbor.2013.760n2007

Figura 10. Uno de los posibles estegotextos basado en la Figura 9. Un estegotexto de 138 palabras (capacidad de ocultación 0,3043 bits/palabra)

> Does anyone know what is going on? What is **intended**? If the Government **decides** to cut salaries we must cope with it but, please, let me doubt that the action will have any positive results. Different **societies** behave differently and react depending on their background so the economic plans that worked for Germany do not necessarily have to work here. First consequence: the **number of** countries that have announced strikes at this side of the **hemisphere** grow. Governments are clearly **abusing** of workers **and** it **is** a fact that the crisis will **expand**. Then, what is next? Loyalty and a sense of community have been **invoked** to make people think there is nothing else to do. **So**, let´s cooperate! In **name** of solidarity! But, please cut also half YOUR salary - that could be a very good **exercise**.

atacante), emisor y receptor comparten de forma secreta, una clave y uno o más texto de referencia con utilidad esteganográfica.

Ataques activos

Un ataque activo es aquel cuyo objetivo principal es eliminar la información potencialmente enmascarada en una cubierta dada, por ejemplo, en un tipo de textos. Dado que el atacante en principio no sabe qué texto es válido y cuál tiene información oculta debería actuar sobre todos, por tanto las modificaciones/eliminaciones no deberían superar un cierto límite de deterioro del portador al que se aplican. Es común que este tipo de ataques no se realice de forma indiscriminada dado que podría introducir diversos problemas. Por ejemplo, imagínese que un proveedor de Internet realizara esto de manera sistemática y por ejemplo un usuario envía un documento legítimo como un contrato, firmado digitalmente. Si el proveedor altera el texto, el documento, la firma no será válida y ello podría repercutir en la imagen que los usuarios tienen de cierto proveedor a la hora de procesar la información intercambiada.

Supongamos, por tanto, que de alguna forma un atacante ha sido capaz de detectar la presencia de información oculta en una serie de textos, hasta donde se conoce esto no sería posible automáticamente pero sirve como ejercicio intelectual (imagínese un traidor de una organización que da un soplo a la policía). Si el atacante supiera sobre qué texto atacar podría actuar de forma que desincronizara al receptor. Es decir, intentando añadir, adivinar, palabras de forma que se fuerce a que el receptor se confunda a la hora de seleccionar una palabra en un grupo dado y por tanto no ser capaz de recuperar la información enmascarada.

En muchas situaciones prácticas los ataques activos no tienen repercusiones importantes. Por ejemplo, un receptor podría confirmar por un canal público que ha recibido correctamente "el mensaje" de un emisor. Si no es así se generaría un nuevo estegotexto o se buscaría otra forma de comunicación.

Ataques pasivos – detección

En este apartado se razona sobre la posibilidad de detectar la presencia de información ocultada con algoritmos como el diseñado. Recuérdese que todo el procedimiento de ocultación es público y conocido por el atacante.

Antes de avanzar, es importante destacar que el texto de referencia utilizado no tiene restricciones destacables, únicamente necesita tener un número suficiente de palabras para crear los grupos de palabras. Si el texto de referencia es más grande existirán más palabras entre las cuales elegir para construir los grupos. Si el texto de referencia es comprometido puede reemplazarse por otro fácilmente y basar las nuevas comunicaciones en él.

Conocido esto, un atacante intentaría detectar información oculta relacionando una serie de estegotextos bajo sospecha y extraer algún tipo de patrón. En principio, el algoritmo propuesto no introduce anomalías detectadas por los algoritmos de estegoanálisis actuales, luego parece factible que un atacante intentara relación estegotextos con la forma de escribir del emisor y con el texto de referencia seleccionado para intentar extraer alguna conclusión. A día de hoy, no se conoce la forma de hacer esto, no obstante se razonan los dos escenarios más negativos:

Escenario 1. El emisor siempre usa el mismo texto de entrenamiento y la misma clave criptográfica para generar todos sus estegotextos, esto lo conoce el atacante.

Las palabras que formarán el estegotexto final dependerán, al menos, de la información a ocultar y de la habilidad del emisor al redactar el estegotexto. El atacante podría intentar estudiar, al menos, la ocurrencia de las palabras en posibles textos de referencia pero las palabras añadidas manualmente generarían muchos falsos positivos ya que es difícil predecir que palabras forman parte del texto de referencia y cuáles no. De hecho, el emisor podría utilizar palabras en su edición que pertenecen al texto de referencia pero que no se han utilizado en la ocultación de infor-

mación o en la construcción de los grupos utilizados. En este sentido, no parece sencillo generar un método de ataque que explote de manera efectiva este conocimiento.

Escenario 2. El atacante conoce el texto de referencia utilizado

En el caso que un atacante conociera esta información privada (es privado no el texto en sí, sino el hecho que se está utilizando en esteganografía) intentaría estimar y detectar información oculta en potenciales estegotextos que podrían estar generados usando ese texto de referencia. Por ejemplo, si suponemos un W=8, se extrae un palabra por cada 3 bits a ocultar, podríamos conjeturar que en lengua española es probable que para que una frase tenga sentido sea necesario al menos 3 o 4 palabras (nombre+verbo+complemento). Es decir, una estimación tosca podría ser de 1/3 o 1/4 del número total de palabras debería aparecer en el texto de referencia. Aunque propuestas de este tipo permitirían descartar algunos textos sin información oculta, de nuevo dependería de la forma de escribir del emisor y del tamaño del texto de entrenamiento, si es este es grande (cientos de palabras o más) muchos textos serían clasificados como que presentan información oculta cuando no es así.

En general, la ciencia del estegoanálisis tiene 3 fases: la primera es la detección, la segunda es la estimación de la cantidad de bits ocultados y la tercera es la recuperación. En el caso hipotético que un atacante pudiera detectar la presencia de la información, no podría recuperar la información sin la clave criptográfica. Recuérdese que para recuperar la información es necesario formar grupos de palabras y estos se hacen aleatoriamente en función de una clave, además la información ocultada es previamente cifrada.

5. CONCLUSIÓN

Este artículo ha analizado la posibilidad de usar algoritmos de esteganografía lingüística que generen estegotextos de calidad con un mínimo número de recursos lingüísticos y tecnologías de lingüística computacional (analizadores morfosintácticos, diccionarios de sinónimos, etiquetadores, algoritmos de desambiguación del significado de las palabras, ontologías, etc.). Estos algoritmos deberían ser resistentes a los ataques publicados e incluso a analistas humanos que idealmente serían incapaces de detectar anomalías en los estegotextos.

Solventar los problemas derivados de la falta de tecnologías para la automatización de la generación de estegotextos con validez lingüística (sintáctica, semántica y textual) no es nada sencillo y en principio es difícil encontrar una alternativa. En esta investigación se propone un algoritmo basado en la posibilidad de que un humano escriba “manualmente” la mayor parte del texto a enviar, sólo una pequeña parte del texto será generado automáticamente con la información que se desea enmascarar. Es decir, en ausencia de otros recursos, una persona puede dar la calidad deseada a un texto manualmente y todavía ocultar información mediante un algoritmo público, conocido por todos. El receptor del estegotexto no necesitará conocer las palabras introducidas manualmente por el emisor. Esta característica permite al emisor dedicar todo el tiempo que desee en la calidad final del estegotexto que enviará. Esto tiene ventajas e inconvenientes como se ha tratado ampliamente en el desarrollo de esta exposición.

De la investigación, puede concluirse que es posible diseñar algoritmos que generen textos de alta calidad lingüística con pocos recursos, aunque no sin una serie de inconvenientes destacables. La fortaleza de algoritmos como el diseñado recae en la edición manual, pero esto supone un problema a la hora de ocultar grandes volúmenes de información ya que obligaría a la edición manual de mucho texto. No obstante, las pruebas realizadas hasta el momento concluyen una capacidad de ocultación del orden de las propuestas “automatizadas” de esteganografía lingüística más serias, de 0,2 a 1 bit/palabra. Es decir, para una calidad aceptable del estegotexto una media de decenas de bits ocultos en unas pocas centenas de palabras. Esto limita su uso a escenarios muy concretos, como pueda ser el envío oculto de una localización (coordenada GPS), una dirección de internet, un mensaje de movilización, un número de teléfono, mensajes cortos en redes sociales, una clave criptográfica, etc.

A día de hoy no se conocen ataques a este tipo de propuestas. Los ataques de estegoanálisis actuales publicados no pueden detectar este tipo de estegotextos, ya que los ataques publicados se basan en la detección de anomalías entre estegotextos creados por “software” en su comparación con textos creados por personas. Los estegotextos generados con el algoritmo diseñado están “escritos por personas”. Un trabajo en curso consiste en formalizar de la mejor manera posible las características de este tipo de algoritmos especialmente en lo que tiene relación con el impacto de que una persona edite manualmente textos y si es posible o no que ello introduzca algún tipo de patrón que permita detectar la presencia de información oculta.

Mientras la comunidad científica sigue avanzando en procedimientos automatizados de calidad en su aplicación a la esteganografía lingüística, en ciertos entornos, propuestas como la analizada aquí puede tener una gran utilidad y no deberían ser olvidadas para el enmascarado de información de tamaño pequeño o mediano (decenas a centenas de bits).

ARBOR Vol. 189-760, marzo-abril 2013, a021. ISSN-L: 0210-1963 doi: http://dx.doi.org/10.3989/arbor.2013.760n2007

NOTAS

1 Ocultación basada en la selección de ciertas letras, palabras o frases en un texto. En terminología inglesa, *Cues, Null Ciphers, Jargon Code* y *Grilles*.

2 Modificaciones de la estructura y formato de elementos presentes en un texto.

3 La esteganografía basada en diccionario consiste en ocultar información basado en el hecho de seleccionar un elemento entre los disponibles de un diccionario o conjunto.

BIBLIOGRAFÍA

Atallah, M; McDonough, C; Raskin, V. y Nirenburg, S. (2000): *Natural language processing for information assurance and security: an overview and implementations.* Proceeding NSPW '00 Proceedings of the 2000 workshop on New security paradigms Pages 51 - 65 ISBN:1-58113-260-3 doi>10.1145/366173.366190

Bergmair, R. (2007): *A comprehensive bibliography of linguistic steganography.* Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents. Doi: 10.1.1.99.2615

Blasco, J; Hernandez-Castro, J; Tapiador, J. y Ribagorda, A. (2008): *Csteg: Talking in C code*. Vols. In Proceedings of SECRYPT International Conference, pp. 399–406. INSTICC. Oporto. July 2008.

Chapman, M. y Davida, G. (1997): *Hiding the hidden: A software system for concealing ciphertext as innocuous text.* Proceedings of the International Conference on Information and Communication Security. Lecture Notes in Computer Sciences 1334. Doi: 10.1.1.22.1193.

Chapman, M; Davida, G. y Rennhard, M. (2001): *A practical and effective approach to large-scale automated linguistic steganography.* ISC '01 Proceedings of the 4th International Conference on Information . ISBN:3-540-42662-0.

Chen, Z; Liu-sheng, H; Zhen-shan, Y; Xin-xin, Z. y Xue-ling, Z. (2008): *Effective Linguistic Steganography Detection*. Vol. 2008 IEEE 8th International Conference on Computer and Information Technology Workshops. ISBN: 978-0-7695-3242-4.

Cox, I; Miller, M; Bloom, J; Fridrich, J. y Kalker, T. (2007): *Digital Watermarking and Steganography*. Morgan Kaufmann; 2 edition (Nov 13 2007). ISBN-13: 978-0123725851.

Daemen, J. y Rijmen, V. (2002): *The Design of RijndaeL: AES - The Advanced Encryption Standard*. Springer; 1 edition (March 22, 2002). ISBN-10: 3540425802

Dai, W; Yu, Y. y Deng, B (2009): *BinText steganography based on Markov state transferring probability*. ACM International Conference Proceeding Series; Vol. 403, 2009. Vols. Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human. ISBN:978-1-60558-710-3.

Grothoff, C; Grothoff, K; Alkhutova, L; Stutsman, R. y Atallah, M. (2005): *Translation-Based Steganography*. Computer Science Information Hiding Lecture Notes in Computer Science, 2005, Volume 3727/2005, 219-233, DOI: 10.1007/11558859_17

Huang, H; Sun, X; Li, Z. y Sun, G. (2007a): *Detection of Hidden Information in Webpage*. Fuzzy Systems and Knowledge Discovery. 2007. Vols. Fourth International Conference, pp. 317-321. ISBN 978-0-7695-2874-8.

Huang, H; Xingming, S; Guang, S. y Junwei, H. (2007b): *Detection of Steganographic Information in Tags of Webpage Based on Tag-Mismatch*. Intelligent Information Hiding and Multimedia Signal Processing. IIHMSP 2007. Third International Conference on Volume 1, pp. 257-260. Doi: 10.1109/IIHMSP.2007.4457539

Huang, J; Sun, X; Huang, H. y Luo, G. (2007): *Detection of Hidden Information in Webpages Based on Randomness.* Information Assurance and Security, 2007. Doi: 10.1109/IAS.2007.74

Kahn, D. (1996): *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet.* Publisher: Scribner; Rev Sub edition (December 5, 1996). ISBN-10: 0684831309. Hardcover: 1200 pages.

Kerckhoffs, A. (1883): La cryptographie militaire. *Journal des sciences militaires*, vol. IX. http://www.petitcolas.net/fabien/kerckhoffs [Mayo 2012]

Lingjun, L; Liusheng, H. y Xinxin, Z. (2008): *A statistical attack on Kind of Word-Shift Text-Steganography.* Vols. IIH-MSP 2008, pp. 1503-1507. ISBN:978-0-7695-3278-3.

Lingyun, X; Xingming, S; Gang, L. y Can, G. (2007): *Research on Steganalysis fort text steganography based on font format*. Vols. IAS 2007, pp. 490-495. ISBN: 0-7695-2876-7.

Lingyun, X; Xingming, S. y Gang, L. (2011): *Bin X, Steganalysis of Syntactic Transformation based Steganography. JDCTA: International Journal of Digital Content Technology and its Applications*, Vol. 5, No. 5, pp. 320 - 330, 2011.

Meng, P; Huang, L; Chen, Z; Yang, W. y Li, D. (2008): *Linguistic Steganography Detection Based on Perplexity.* Vol. 2008 International Conference on MultiMedia and Information Technology. ISBN: 978-0-7695-3556-2.

Meng, P; Hang, L; Yang, W; Chen, Z. y Zheng, H. (2009): *Linguistic Steganography Detection Algorithm Using Statistical Language Model*. International Conference on Information Technology and Computer Science, 2009. ISBN: 978-0-7695-3688-0.

Meng, P; Liusheng, H; Zhili, C; Yuchong, H. y W, Y. (2010): *STBS: A Statistical Algorithm for Steganalysis of Translation-Based Steganography.* Lecture Notes in Computer Science, 2010, Volume 6387/2010, pp. 208-220. Doi: 10.1007/978-3-642-16435-4_16

Muñoz, A; Argüelles, I. y Carracedo, J. (2009): *Modificaciones sintácticas en lengua española con utilidad en esteganografía lingüística.* Revista Electrónica de Lingüística Aplicada (ISSN 1885-9089). RAEL Nº8, páginas 229-247.

Muñoz, A; Argüelles, I. y Carracedo, J. (2010): *Improving N-Gram linguistic steganography based on templates.* International Conference on Security and Cryptography. Secrypt 2010. July 26-28 Athens, Greece. http://stelin.sourceforge.net [Mayo 2012]

Muñoz, A. y Argüelles, I. (2012): *Modificaciones Sintácticas basadas en la reorde-*

nación de complementos del verbo con utilidad en esteganografía lingüística. Revista Electrónica de Lingüística Aplicada (ISSN 1885-9089). RAEL Nº10, páginas. 31-54.

Raskin, V; Nirenburg, S; Atallah, M; Hempelmann, C. y Triezenberg, Katrina. (2002): *Why NLP should move into IAS.* International Conference On Computational Linguistics. Proceeding COLING-Roadmap '02 Proceedings of the 2002 COLING workshop: A roadmap for computational linguistics - Volume 13 Pages 1-7. doi>10.3115/1118754.1118757

Tenenbaum, A. (2002): *Linguistic steganography: Passing covert data using text-based mimicry.* Vols. Final year thesis, April 2002. submitted in partial fulfillment of the requirements for the degree of "Bachelor of Applied Science" to the University of Toronto.

Topkara, M; Topkara, U. y Atallah, M. (2007): *Information Hiding through Errors: A Confusing Approach.* Vols. Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents, January 29- February 1, 2007, San Jose.

Wayner, P. (1992): *Mimic functions.* Vols. Cryptologia XVI, pp. 193–214, July 1992.

Wayner, P. (1995): *Strong theoretical steganography*. Vols. Cryptologia XIX, pp. 285–299, July 1995.

Wikipedia_es. (2012): *Derechos Humanos.* https://es.wikipedia.org/wiki/Derechos_ humanos [Mayo 2012].

Wikipedia_en. (2012): *Human Rights.* https://en.wikipedia.org/wiki/Human_ rights. [Mayo 2012]

Zhenshan, Y; Liusheng, H; Zhili, C; Lingjun, L; Xinxin, Z. y Youwen, Z. (2009): *Steganalysis of Synonym-Substitution Based Natural Language Watermarking*. Vols. International Journal of Multimedia and Ubiquitous Engineering. Vol. 4, No. 2, April, 2009.

Zhi-li, C; Liu-sheng, H; Zhen-shan, Y; Lingjun, Li. y Wei, Y. (2008a): *A Statistical Algorithm for Linguistic Steganography Detection Based on Distribution of Words.* IEEE Computer Society. Vols. Proceedings of the 2008 Third International Conference on Availability, Reliability and Security. pp. 558-563. ISBN: 978-0-7695-3102-1.

Zhili, C; Liusheng, H; Zhenshan, Y; Wei, Y; Lingjun, L; Xueling, Z. y Xinxin, Z. (2008b): *Linguistic Steganography Detection Using Statistical Characteristics of Correlations between Words*. Lecture Notes In Computer Science. Information Hiding, 2008. ISBN: 978-3-540-88960-1. Doi>10.1007/978-3-540-88961-8_16

Zuxu, D; Fan, H; Muxiang, Y. y Guohua, C. (2007): *Text Information Hiding Based on Part of Speech Grammar*. Proceedings of the 2007 International Conference on Computational Intelligence and Security Workshops, pp. 632-635. ISBN: 0-7695-3073-7.