Esteganografía y canales encubiertos

Esteganografía lingüística

Dr. Alfonso Muñoz (@mindcrypt)
alfonso@criptored.com

Reconocimiento-NoComercial-SinObraDerivada
Bajo licencia CC BY-NC-ND
https://creativecommons.org/licenses/by-nc-nd/4.0/

Si no puedo mover el cielo, agitaré el mundo subterráneo

Sigmund Freud

Motivación de este documento

Estimado lector, el presente documento incluye parte de la documentación que consulté y procesé hace más de 10 años (2000-2009) para el desarrollo de sistemas y canales encubiertos basados en esteganografía lingüística (ocultación de información en textos en lenguaje natural) para la protección frente a sistemas masivos de interceptación de comunicaciones. Este documento incluye extractos de una documentación más amplia.

Una vez pasado este tiempo, he pensado en liberar esta información, quizás parte del contenido todavía pueda serle de utilidad. Algunas propuestas han sido mejoradas pero muchas otras todavía son actuales y le ayudarán a meditar y desarrollar sistemas de protección. Hasta mi conocimiento, en lengua española, este documento sigue siendo el mejor documento existente para formarse en la ocultación de información en lenguaje natural.

El documento resume algunas de las técnicas y herramientas más famosas, así como se incluye una amplia bibliografía con referencias de interés.

Espero que lo disfrute.

Un saludo

Mayo 2019 - @mindcrypt

15/05/2019 – Versión 1

Índice de Contenidos

1. DESDE LA CRIPTOGRAFÍA CLÁSICA A LA ESTEGANOGRAFÍA LINGÜÍSTICA

Las tres cosas más difíciles en este mundo son:
guardar un secreto, perdonar un agravio
y aprovechar el tiempo
Benjamín Franklin

El ser humano siempre ha tenido secretos de muy diversa índole, y ha buscado mecanismos para mantenerlos fuera del alcance de miradas indiscretas, especialmente si la información se transmite por un canal inseguro en el cual la información puede ser curioseada y modificada. De hecho, el espionaje de las comunicaciones ha constituido, tanto en la guerra como en la paz, un valioso instrumento para conocer las actividades e intenciones de otros grupos de personas.

La evolución de todos los mecanismos y técnicas que intentan solucionar este problema es lo que se conoce hoy día como la ciencia de la criptología, compuesta por sus dos ramas, criptografía y criptoanálisis. La ciencia de la criptología se puede englobar en dos grandes épocas: criptología clásica y criptología moderna. La criptología clásica comprende todas aquellas técnicas de escritura secreta hasta mediados del siglo XX. Estas técnicas de cifra se agrupaban en métodos de transposición y métodos de sustitución. La transposición consiste en colocar-combinar-reordenar la información de un mensaje de formas distintas a la original, mientras que la sustitución establece mecanismos que consisten en la sustitución de caracteres del alfabeto empleado por otros símbolos, típicamente mediante sustitución monoalfabética o polialfabética.

Con el paso de los siglos la ciencia de la criptología fue adquiriendo consistencia. Se conocían multitud de algoritmos de cifrado y métodos de criptoanálisis. Una nueva criptografía estaba a punto de saltar a escena, con los mejores avances de los siglos anteriores, y con una idea revolucionaria, la planteada en 1883 por el lingüista holandés Augusto Kerckhoffs von Nieuwenhof (1835-1903) en su libro *La cryptographie militaire* [1]:

"La seguridad de un criptosistema no debe depender de mantener secreto el algoritmo de cifrado. La seguridad sólo debe depender de mantener la clave de cifrado en secreto".

El camino hacia una nueva filosofía criptográfica ya había comenzado, y se fue robusteciendo con una serie de artículos que establecieron definitivamente la base de la nueva criptografía, la criptografía moderna, y que se extiende hasta nuestros días. Existen dos momentos claves en el siglo XX para la evolución futura de la criptografía y la protección de comunicaciones. Una de ellas fue en la década de los 40 del siglo XX con la publicación de dos artículos fundamentales que sentarían las bases de la teoría de la información: *A Mathematical Theory of Communication*, en 1948 [2], y *Communication Theory of Secrecy Systems*, en 1949 [3], desarrollados por Claude Shannon (1916-2001). Los artículos de Shannon propusieron dos técnicas de cifrado en criptosistemas de clave secreta, que resumían los mecanismos anteriores de la historia, a las que llamó difusión y confusión. Por un lado, la difusión sería la técnica que permitiría dispersar las propiedades estadísticas inherentes al lenguaje en el texto en claro sobre el criptograma, por ejemplo, mediante permutaciones o transposiciones. Por

otro lado, la técnica de confusión, permitiría generar caos, mezcla en el resultado cifrado, de tal forma que la dependencia entre texto en claro, clave y criptograma sería lo más compleja posible e impediría romper el algoritmo (propone aplicar la técnica de sustitución). Ahora más que nunca la criptografía se convertiría en el refugio de los matemáticos, el lugar perfecto en el cuál aplicar numerosas teorías, teniendo en cuenta los principios de Kerckhoffs. Todos estos avances contribuirían al desarrollo de cifradores de flujo y cifradores de bloque.

A finales de la década de los 70 y en la década de los 80 se producirían los avances conceptuales más notorios que marcarían muchas de las tendencias criptográficas en las décadas posteriores. Posiblemente, el salto cualitativo más importante en la historia de la criptografía fue gracias al artículo *New directions in cryptography*, publicado en 1976 por Whiteld Diffie y Martin Hellman, que establecía el concepto de criptografía asimétrica o clave pública, en la que cada participante en una comunicación secreta disponía de dos claves, una pública y otra privada. Cualquier emisor podía comunicarse con un destinatario conociendo exclusivamente su clave pública, sólo el destinatario podía descifrar la comunicación cifrada, dado que sólo él conocía su clave privada. Fue en esta época cuando se abrió el camino al uso de funciones unidireccionales fáciles de computar en una dirección, pero muy complejas computacionalmente de invertir sin una trampa, una pista a modo de clave de sistema. Esto abrió un gran potencial para el desarrollo de protocolos criptográficos en las redes de comunicación, y para dar una solución práctica al problema de la distribución de claves. En la década de los 80, el avance en los principios de los algoritmos de curvas elípticas y en las ideas de la actual criptografía cuántica marcarían los sistemas actuales de protección de comunicaciones digitales.

Es cierto, en toda esta evolución, que la criptografía ha mostrado una gran utilidad en conflictos militares y en defensa de libertades civiles, véase el caso del *software PGP*. No obstante, adolece de un problema intrínseco: en todo momento la comunicación que tiene lugar puede ser detectada, aunque esto no implique necesariamente el conocimiento de la información intercambiada. En muchas situaciones reales, la detección de una comunicación cifrada podría alentar a potenciales enemigos a tomar decisiones concretas, localizar y atacar las fuentes de donde proviene la información, anular la comunicación, etc.

En el interés de proteger mejor las comunicaciones surgió, históricamente, el concepto de esteganografía. Este arte, actualmente toda una ciencia, se centraba en todo tipo de procedimientos para crear comunicaciones enmascaradas, comunicaciones que pasarían desapercibidas para un potencial atacante. Como puede suponerse este hecho establece un doble mecanismo de seguridad, criptografía-esteganografía, y es de gran utilidad en entornos hostiles. La evolución de la escritura oculta ha sido paralela a la criptografía, del mismo modo hoy día podemos hablar de esteganografía clásica y moderna (simétrica, asimétrica y cuántica). Para ello es importante remontarse después de la II Guerra Mundial donde muchas ramas de la ciencia experimentaron un avance significativo.

Los nuevos conocimientos en teoría de códigos (matemáticas), telecomunicaciones e informática, química, física, biología, procesamiento digital de contenido multimedia, etc., tuvieron su reflejo notorio en la ciencia de la esteganografía. Estos nuevos

procedimientos ya no se restringen a los clásicos conflictos bélicos, sino a todas aquellas facetas que requieren ocultar una información a un grupo de individuos. Tiene aplicación directa en: política, comunicaciones militares, diplomacia, mecanismos de protección de propiedad intelectual, defensa de libertades civiles, secretos industriales, intrusión en sistemas informáticos (por ejemplo, espionaje industrial), ocultación de virus, etc. Es en esta nueva época cuando se empieza hablar de la ciencia de la esteganografía moderna. Esta nueva vertiente consiste en que la seguridad de los procedimientos esteganográficos no depende de mantener en secreto el algoritmo de ocultación, principios de Kerckhoffs [1], e incluso tampoco del tipo de la tapadera/cubierta utilizada, la seguridad recae exclusivamente en mantener una pequeña información secreta entre los intervinientes de la comunicación enmascarada, típicamente una clave.

El interés concreto de un sistema esteganográfico dependerá de 3 características: capacidad (cantidad de información que puede ser ocultada), seguridad/invisibilidad (probabilidad de detección por un estegoanalista) y robustez (cantidad de alteraciones dañinas que el medio puede soportar antes de que se pierda la información oculta) [12].

Conocidas estas características, una buena pregunta a responder es qué principios deben seguirse para analizar si es posible ocultar información en un estegomedio concreto y qué estegomedio concreto es más interesante (seguro) para ocultar un mensaje. La segunda cuestión es fácil de responder, el mejor estegomedio es uno completamente desconocido para el estegoanalista, una idea similar al uso del lenguaje navajo en la II Guerra Mundial [8], o, más recomendable en la actualidad, un estegomedio muy común (por ejemplo, imágenes JPEG), que permita ocultar un volumen razonable de información y permita ser distribuido sin levantar sospechas. Si existen muchos estegomedios el estegoanalista se enfrentará a la difícil tarea de "separar el grano de la paja", es decir, de recolectar el mayor número posible de muestras de ese estegomedio concreto y estegoanalizar todas esas muestras en busca de información oculta.

La búsqueda de un procedimiento concreto de ocultación en un medio puede ayudarse teniendo en cuenta estas 3 grandes líneas de creación de algoritmos esteganográficos: 1) la cubierta existe y la ocultación de información no la modifica, 2) la cubierta existe y la ocultación produce alteraciones y 3) la generación automática de la cubierta incluye la información a ocultar [12].

En el proceso de generación de estegosistemas seguros sin duda, por tanto, es necesario añadir el factor del tipo de cubierta. El siglo XX ha destacado sin duda por la publicación de un número enorme de estegomedios que tienen utilidad esteganográfica. Aunque se han publicado procedimientos esteganográfico-criptográfico más "analógicos" como emisoras de números [36] o espionaje enmascarado basado en tecnologías RFID [37], sin duda la irrupción de las telecomunicaciones e informática ha decantado los procedimientos esteganográficos modernos hacia canales y formatos digitales. Así, en los últimos años se han publicado propuestas de ocultación de información utilizando imágenes, audio y vídeo digital [12], tecnologías web como cabeceras http o cookies [38], utilización de la redundancia de las instrucciones máquina en ficheros ejecutables (véase por ejemplo la herramienta *Hydan*) [39] [40], lenguajes de marcado web como HTML–XML (ocultación basada en caracteres

invisibles[1], modificación de los caracteres de las etiquetas alternando mayúsculas y minúsculas al ser éstas *insensitive* y ocultación basada en el orden de los atributos de una etiqueta[2]) [41] [42] [43] [44] [45], utilización esteganográfica de diferentes protocolos de comunicación (SOAP, HTTP, TCP, UDP, Ipv4, IPv6, DHCP, ICMP, IPSEC, IGMP, FTP, DNS, 802.2, 802.3, redes inalámbricas, "accesorios" de mails, etc.) para establecer canales encubiertos para saltarse protecciones corporativas [46] [47] [48] [49] [50] [51] [52], como por ejemplo cortafuegos (típicamente utilizando campos reservados, campos redundantes o el reordenamiento de paquetes), ocultación de información en sistemas ficheros y soportes de almacenamiento como *StegFs* [53], Slack Space [11] o Alternate Data Stream [54], malware en hardware y puertas traseras en microchips [55] [56], etc.

Sin embargo, en la actualidad, las imágenes, los ficheros de audio y los vídeos digitales son probablemente el medio más utilizado por su cuantiosa presencia en las redes de comunicaciones. En los últimos años, se han publicado múltiples técnicas esteganográficas y estegoanalíticas centradas en este tipo de contenidos. A continuación, se va a hacer una breve descripción, fuertemente documentada, con alguno de los avances más significativos relacionados con estas cubiertas.

En primer lugar, una opción interesante para ocultar información son los formatos digitales de vídeo y su capacidad para almacenar mensajes de información de un volumen considerable sin alterar significativamente su aspecto externo. En 1998, A. Westfeld y G. Wolf [57] demostraron cómo un sistema real, en concreto de vídeoconferencia, se podía utilizar para establecer un canal oculto de información sin que la señal sufriera una degradación grande. En general, un vídeo puede definirse como un conjunto de *frames* individuales formado por imágenes y audio (y en ocasiones también texto). Los procedimientos de ocultación de información en un vídeo se pueden aprovechar de las distintas técnicas esteganográficas sobre cada uno de esos elementos individuales (estegomedios) que configuran cada *frame*, aunque algunos de los procedimientos específicos documentados en vídeos han sido: codificación de información a partir del cálculo de los vectores de movimiento entre una colección de frames, técnicas basadas en corrección de errores, etc [58] [59]. A pesar del gran interés que pueda presentar este estegomedio, se han publicado pocas herramientas que faciliten la aplicación real de estos procedimientos para un público amplio. Quizás una de las más conocidas es *MSU StegoVideo*, de Dimitry Vatolin y Oleg Petrov, que permite la ocultación de archivos en secuencias de un vídeo, aplicando la corrección de errores adecuada para que la información pase desapercibida [60].

En segundo lugar, otro estegomedio de especial interés es el audio, especialmente en estos últimos años con el auge del audio-streaming, las radios-online personales, el podcasting, etc. El estudio de las limitaciones del sistema de audición humano es el punto de partida para el diseño correcto de un algoritmo esteganográfico que oculte información en señales de audio. El sistema de audición humano es bastante más difícil de engañar que el sistema de visión. Por ejemplo, el oído presenta una sensibilidad alta

[1] Aplicación de procedimientos similares a la esteganografía textual clásica pero aplicados a páginas web. Por ejemplo, añadir texto con color del fondo de la página web, usar espacios y tabuladores para codificar una información binaria, etc. Ejemplo de herramientas de este tipo son *WebStego* e *Invisible Secret*.

[2] Un ejemplo de herramienta que facilita esta ocultación es la herramienta *Deogol* de Stephen Forrest. La capacidad de ocultación por etiqueta depende del número de atributos (1 o más) y es de $\log_2(\text{nºatributos!})$

a la presencia de un ruido blanco gaussiano añadido a una señal de audio. Esta detección puede ser incluso de unos 70dB por debajo del nivel de ruido ambiente [61]. Sin embargo, a pesar de estas propiedades, existen diversas situaciones en las que el sistema puede ser engañado, es decir, es impreciso en la detección. Una de estas situaciones consiste en que ante la presencia de "sonidos fuertes" y "sonidos más débiles" los primeros tienden a enmascarar a los segundos. Otra es que el sistema de audición humano es poco sensible a ciertos cambios de fase en una señal de audio, o a la supresión de ciertas frecuencias en la señal de audio, modificaciones en las que se basa el estándar MPEG-1 audio Layer III (mp3). Sin embargo, la introducción de modificaciones puede crear patrones no comunes que pueden ser detectados, por ejemplo, mediante estudios estadísticos de las propiedades de la señal empleada. En los últimos años se han publicado múltiples procedimientos esteganográficos y estegoanalíticos en señales de audio: técnicas basadas en LSB (Least Significant Bit) en muestras de audio, como la herramienta *stegowav* [62], técnicas de ocultación en la fase de una señal (modulación de la fase de una señal y codificación en la fase, *phase coding*), técnicas de ocultación en el eco de una señal, ocultación aprovechando las características estadísticas de las señales de audio (por ejemplo, segmentación de la señal de audio de forma adaptativa), ocultación basada en algoritmos de compresión (MP3, WMA, OGG Vorbis), etc [61][63]. Un ejemplo significativo de este último caso, puede ser la herramienta *Mp3stego* que facilita la ocultación de información en ficheros mp3 [64]. Fabien A. Petitcolas, su creador, destacó que el único ataque real conocido contra la ocultación de información en un fichero mp3 consistiría en que un atacante descomprimiera el flujo de bits y a continuación volviera a comprimirlo, consiguiendo borrar la información oculta, si ésta existe (eso sí, provocando una pérdida significativa de la calidad sonora del archivo resultante). Ataques posteriores han demostrado que esto no es necesariamente cierto [65].

En último lugar, es interesante echar un vistazo al estegomedio sobre el que más publicaciones y herramientas esteganográficas y estegoanalíticas se han publicado en la última década: las imágenes digitales. Los principios en los que se fundamentan las técnicas de ocultación sobre este tipo de estegomedio son dos: que la modificación de la imagen no introduzca un ruido visual que levante sospechas a una persona que vea la imagen y que las modificaciones introducidas no proporcionen pistas adicionales a un estegoanalista. En la última década se ha publicado una gran variedad de ellas para diferentes formatos gráficos de fichero (bmp, gif, jpeg, png, etc.). Las técnicas y variantes más documentadas de estos procedimientos consisten en la modificación de los LSB de los píxeles de una imagen (típicamente formato BMP) [12] [66], de los índices que enlazan a la paleta de colores de un formato GIF[3] (otros procedimientos como el reordenamiento de los colores de la paleta es posible) [66] o de los coeficientes resultantes de aplicar alguna transformación matemática a una imagen, por ejemplo, los coeficientes DCT (transformada discreta del coseno) del formato gráfico JPEG o los coeficientes Wavelet del formato gráfico JPEG2000 [12]. Especial interés ha tenido el formato JPEG debido a su enorme difusión en Internet. Algunas de las herramientas notorias han sido, *Jsteg, Outgues 0.2, F5, MB1, MB2*, *steghide*, *YASS* [67], *etc.* Estas herramientas han ido evolucionando para ser más resistentes a ataques estadísticos y ataques basados en el estudio del histograma. Las publicaciones estegoanalíticas

[3] Las implementaciones actuales sobre formato GIF, por su baja capacidad, priorizan ésta sobre la seguridad y por tanto las herramientas actuales son fáciles de detectar. Algunas herramientas significativas son: *S-Tools, MandelSteg, Hide&Seek y EzStego.*

respecto a este estegomedio son cuantiosas en volumen y en calidad. Algunos de ellos son procedimientos estadísticos robustos para la mayoría de técnicas esteganográficas basadas en LSB y DCT como el ataque chi-cuadrado [68], el ataque RS [69], el ataque basado en análisis de parejas de píxeles [70], los ataques basados en parejas de píxeles que se toman como referencia [71] [72] [73] [74], etc. Otras técnicas de estegoanálisis están basadas en caracterización de portadores: ataque *F5* [75], ataque *Outguess* [76], ataque basado en compatibilidad [77], etc.

En la actualidad, los esfuerzos de los estegoanalistas se dedican a una nueva concepción del estegoanálisis, denominado estegoanálisis a ciegas (en inglés, *blind steganalysis*). El concepto de estegoanálisis a ciegas apareció por primera vez en el trabajo propuesto por Avcibas, Memon y Sankur en 2001 [78], y consiste en realizar estegoanálisis sin necesidad de conocer la técnica de ocultación empleada. La idea es clara: como existe un número elevado de variantes posibles de cada técnica esteganográfica conocida y dado que la tendencia actual es utilizar portadores muy comunes, la idea consiste en caracterizar el estegomedio potencial y extraer parámetros cuantificables que permitan estimar variaciones entre un fichero portador "normal" y el mismo fichero portador con información oculta. El trabajo teórico consiste en la cuantificación de esos parámetros; una vez realizado esto pueden realizarse diversas implementaciones prácticas mediante el uso de clasificadores que diferencien entre cubiertas originales y potenciales estegomedios. En la última década los clasificadores SVM (Support Vector Machines) han tenido una importancia crucial en el estegoanálisis a ciegas; tanto que es posible combinarlos para que no sólo se detecte la presencia de información oculta, sino que, además, se puedan clasificar los estegomedios por técnicas esteganográficas conocidas. En general, los ataques estegoanalíticos a medida sobre algoritmos esteganográficos concretos darán mejores resultados que la detección a ciegas, no obstante, si el algoritmo de detección a ciegas consigue clasificar un estegomedio en una técnica esteganográfica conocida será posible posteriormente aplicar ataques a medida para intentar extraer la mayor cantidad posible de información del estegomedio detectado, por ejemplo, el tamaño de la información oculta [79][80] [81] [82] [83].

En las últimas décadas, a todos estos portadores e interés se le ha sumado la actualización de una vertiente más antigua, la posibilidad de utilizar mensajes inocuos en lenguaje natural para enmascarar otros mensajes "menos inocentes". Este documento se centra en dar algo de luz adicional al lector profano en la materia de la esteganografía textual y lingüística.

En general, una lista amplia de aplicaciones esteganográficas con las que experimentar puede observarse en la web del refutado autor Neil F. Johnson [44].

1.1 Recomendaciones para el diseño de estego-sistemas seguros

Históricamente, independientemente del portado elegido, se han citado algunas recomendaciones para el diseño de un canal encubierto seguro:

1. **Introducir los ataques estegoanalíticos** (visuales, estadísticos, caracterización del portador, etc.) **en el propio diseño del algoritmo esteganográfico**. Esto no es nada nuevo en otras ciencias, como por ejemplo en la criptografía. La idea es probar si el algoritmo esteganográfico desarrollado, considerando los criterios comentados a lo

largo de este capítulo, es seguro a los ataques y tendencias conocidas y si resiste a nuevos ataques que podamos presuponer con el tiempo y dinero que tengamos disponibles.

2. **Elección del portador.** En los últimos años la tendencia de la comunidad científica es recomendar la utilización de cubiertas únicas por cada transmisión encubierta, para dificultar ataques de comparación, y seleccionar cubiertas ampliamente disponibles para dificultar la tarea del estegoanalista de "separar el grano de la paja". Una vez elegido un tipo concreto de portador, por ejemplo, ficheros gráficos JPEG, es importante destacar que no todos los portadores de ese tipo son igual de "seguros" para su uso en esteganografía. La caracterización del portador concreto y el estudio de los ataques existentes permitirán concretar esta elección. Por ejemplo, en imágenes digitales los principios comentados anteriormente pueden conseguirse obteniendo una imagen de alta resolución, que puede ser obtenida con una cámara digital de fotos, para cada comunicación a realizar. Una fotografía de alta resolución presentará menos áreas uniformes, y simplemente por esto, minimizará ataques como por ejemplo los ataques visuales, y la medición de variaciones estadísticas no dará tan buenos resultados [12]. Del mismo modo un portador, que puede ser recomendado para su uso esteganográfico, puede tener ciertas zonas que no serían recomendables de manipular porque introducirían anomalías más fácilmente detectables. La pregunta a responder sería: ¿es posible descartar esas zonas de una manera automatizada? En general, este problema es complejo ya que depende de la información a ocultar, de la cubierta seleccionada y del procedimiento esteganográfico concreto. Por suerte, los algoritmos basados en el concepto de *Wet Paper Codes* (códigos WPC), introducido por Jessica Fridrich, permiten abordar este problema e incluso introducen la libertad para el emisor que las posiciones donde se realizan las modificaciones no tengan que ser conocidas por el receptor (*non-shared selection cannel*). El concepto *Wet Paper* puede comprenderse fácilmente con una metáfora. Supongamos que tenemos una imagen que se ha expuesto a la lluvia de tal forma que el emisor sólo puede modificar ligeramente las zonas secas de la imagen, pero no las zonas mojadas. Durante la transmisión, la estegoimagen se seca y por lo tanto el receptor no tiene información de las zonas secas que se modificaron, zonas que almacenan el mensaje oculto. Los códigos WPC intentan solucionar esta situación y permiten recuperar el mensaje oculto sin conocer las posiciones exactas de modificación. Para una mayor información puede consultarse los siguientes artículos [90] [91] [92] [93] [94].

3. **Limitaciones de los algoritmos estegoanalíticos.** La seguridad de un estegosistema no debería basarse en las limitaciones de los algoritmos estegoanáliticos, pues tarde o temprano estos mejorarán. Hay un viejo dicho en la agencia de seguridad norteamericana (NSA) que dice *los ataques siempre mejoran nunca empeoran* o citando a Manuel Machado: *fatigas, pero no tantas, que a fuerza de muchos golpes hasta el hierro se quebranta*. No obstante, la vida real es compleja y en la práctica los sistemas se aposentan en estas limitaciones ya sean algorítmicas, de software o de capacidad de computación. Un ejemplo claro en este sentido es la evolución de la criptografía en el siglo XX. Es en este contexto práctico donde existen ciertas peculiaridades en cierto tipo de algoritmos estegoanalíticos que es interesante destacar.

La propia naturaleza de los algoritmos estegoanalíticos más robustos, normalmente se aposentan en la estadística, limitan su detección a ciertos umbrales mínimos. Es decir,

estos algoritmos siempre detectan una mínima cantidad de información oculta, depende de la cubierta y del algoritmo, que va desde una decena a centena de octetos, independientemente si la cubierta tiene o no información oculta. Este hecho puede comprenderse porque en los potenciales estegomedios, por ejemplo, imágenes digitales, es habitual que exista un pequeño "ruido" de fondo, es decir, un pequeño conjunto de perturbaciones "naturales". Esto supone falsos positivos y, lo más importante, un umbral de acción para seguir ocultando información sin que los algoritmos de estegoanálisis sean capaces de inferir qué cubiertas realmente ocultan información y cuáles no. Este hecho se puede resumir coloquialmente de la siguiente manera: a menor información ocultada la probabilidad de detección será más baja, incluso llegando a dificultar el descernimiento "estegoanalítico" de un potencial atacante. El objetivo por tanto es jugar con el balance perceptibilidad-cantidad de información a ocultar. La solución trivial a este problema consiste en ocultar menos información, pero por suerte pueden combinarse otra serie de criterios, adicionalmente a algoritmos de compresión, para aprovecharse de estos límites de detección. En concreto, el uso de distribución de la información y el uso de matrices de codificación. La distribución de información consiste en la posibilidad de distribuir un mensaje oculto entre distintos portadores e incluso entre distintos proveedores que almacenan estos portadores. La utilidad principal reside en poder ocultar una cantidad mayor de información introduciendo menos información por portador. Alguna propuesta práctica de este concepto es la herramienta *StegPage* que permite ocultar una información distribuyéndola en distintas imágenes JPEG de una página web [95]. Por otro lado, las matrices de codificación mejoran la relación entre la información insertada y las modificaciones de un estegomedio. Estas matrices fueron descubiertas en 1998 por Crandall [96]. Westfeld fue el primero que implementó una aplicación práctica de las mismas en la herramienta esteganográfica *F5* [97]. Estas matrices normalmente consisten en maximizar la información a ocultar minimizando el número efectivo de posiciones (por ejemplo, pixeles) a modificar. Un ejemplo matemático sencillo para comprender su funcionamiento puede extraerse del sistema planteado por Westfeld en *F5* que implementa una matriz de codificación basada en códigos binarios Hamming. Así, por ejemplo, permite modificar, como mucho, una posición de cada 2^n-1 posiciones por cada n bits a ocultar. Entiéndase por posición el "lugar" en el estegomedio donde es posible realizar una inserción, por ejemplo, en los píxeles de una imagen. Un ejemplo de esto sería ocultar 2 bits en 3 posiciones (por ejemplo, el LSB de 3 píxeles) modificando como mucho un LSB, 1 bit, en total:

$$f_E(x_1\, x_2, p_1\, p_3\, p_2) = p_1\, p_3\, p_2 \mid p'_1\, p_2\, p_3 \mid p_1\, p'_2\, p_3 \mid p_1\, p_2\, p'_3$$

Ejemplo de valores: $p_1\, p_3\, p_2 = 000$

$x_1 = p_1 \text{ XOR } p_3$	$x_2 = p_2 \text{ XOR } p_3$	Ocultación sin alteración	00 = 000
$x_1 \neq p_1 \text{ XOR } p_3$	$x_2 = p_2 \text{ XOR } p_3$	Alteramos el valor de p1	01 = 010
$x_1 = p_1 \text{ XOR } p_3$	$x_2 \neq p_2 \text{ XOR } p_3$	Alteramos el valor de p2	10 = 100
$x_1 \neq p_1 \text{ XOR } p_3$	$x_2 \neq p_2 \text{ XOR } p_3$	Alteramos el valor de p3	11 = 001
		Posibles valores de	$x_1\, x_2$

El valor n es un parámetro de diseño, en la práctica el tamaño de la cubierta y la información a ocultar disminuirán el valor de este parámetro. Por ejemplo, ocultar 8 bits con como mucho una modificación requiere de 255 posiciones útiles, 20 bits requieren 128KB posiciones, 200 bits troceados en bloques de 10 como mucho 10 modificaciones

(10*128KB posiciones = 1280KB posiciones necesarias). En los últimos años se han publicado varios trabajos interesantes en esta temática intentando maximizar la capacidad de ocultación minimizando el número de modificaciones y minimizando el número de posiciones efectivas necesarias [98] [99] [100].

2. Esteganografía textual en la antigüedad. Procedimientos basados en oscuridad.

Si hubiera estado presente en la Creación,
habría dado algunas indicaciones útiles
Alfonso X el Sabio

En 1997, Friedrich L.Bauer en *Decrypted Secrets. Methods and Maxims of Cryptology* [18] realizó una clasificación de los procedimientos de esteganografía textual que puede resumir muy bien las tendencias en procedimientos de ocultación en textos antes de la última década del siglo XX. Según ésta, la esteganografía textual puede explicarse en dos grandes ramas: *open codes* y *semagrams*, en terminología inglesa [6] [18]. A continuación, se profundiza en éstos proponiendo una traducción al español de los términos documentados.

2.1 Códigos abiertos

Los códigos abiertos (en inglés, *open codes*) son textos de apariencia inocente, que ocultan información recuperable utilizando ciertas letras, palabras, frases del texto o comunicación. Por ejemplo, ciertas letras situadas en determinadas posiciones de una carta, de la letra de una canción, etc. Procedimientos basados en estas ideas son: a) *cues*, b) *null-Ciphers*, c) *jargon code* y d) *grilles.*

a) Señales o pistas (en inglés, *cues*)

El término *cues* hace referencia a la transmisión de ciertas palabras, que aparecen en un texto o medio genérico de comunicación, que se utilizan como señal para avisar al receptor que realice una serie de acciones. Un uso interesante se puede observar en situaciones de guerra para retransmitir instrucciones a los soldados, agentes o grupos de resistencia ubicados en un país enemigo. En la actualidad, un ejemplo muy simple de esta idea consistiría en que un agente escuchara un programa de radio de emisión nocturna que permite la participación del público, por ejemplo, por teléfono. En función de si se usa una serie de palabras o no, se siguen una serie de instrucciones u otras. Como puede observarse, este método de comunicación es muy flexible y efectivo, sin embargo, requiere de cierta preparación y comunicación previa. No es idóneo para transmitir grandes cantidades de información.

b) Cifradores Nulos (en inglés, *null ciphers*)

En general, el término *null ciphers* hace referencia a aquellos procedimientos esteganográficos que permiten ocultar información en un texto tapadera cuya recuperación se obtiene al seleccionar ciertas letras o palabras del mismo. La distribución de la información ocultada en el mensaje inofensivo, que se usa como tapadera, depende del algoritmo desarrollado, por ejemplo, ocultar información en sentido vertical u horizontal del mismo, cierto número de letras por línea, etc. David Kahn en su excepcional obra *The CodeBreakers* [6] relata algunos ejemplos de su uso en la historia. Por ejemplo, un mensaje, enviado por los alemanes en la I Guerra Mundial, en forma de nota de prensa, decía:

PRESIDENT'S **E**MBARGO **R**ULING **S**HOULD **H**AVE **I**NMEDIATE **N**OTICE. **G**RAVE **S**ITUATION **A**FFECTING **I**NTERNATIONAL **L**AW. **S**TATEMENT **F**ORESHADOWS **R**UIN **O**F **M**ANY **N**EUTRALS. **Y**ELLOW **J**OURNALS **U**NIFYING **N**ATIONAL **E**XCITEMENT **I**NMENSELY.

Las letras iniciales reflejan el mensaje: **Pershing sails from N.Y. June I.**

Durante la II Guerra Mundial este tipo de procedimientos encontraron su uso para comunicar información enmascarada entre soldados norteamericanos y sus familiares. Tal fue el extremo que la armada norteamericana, en la década de los 40, impuso penas severas a los marineros que intentaban comunicarse de forma encubierta con este tipo de código familiar que, en general, era fácilmente detectable, y podía poner en peligro sus vidas y la de los mensajeros, al revelar en esas comunicaciones información táctica a su familiares, como su posición en cierto país o ciudad [8].

Avanzando en estas ideas, es interesante destacar uno de los procedimientos más usados en la historia que utiliza estos principios, son los denominados acrósticos. Un acróstico, del griego *akros* (extremo) y *stikhos* (verso), en sentido estricto, es un poema cuyas letras iniciales, medias o finales de cada verso, leídas en sentido vertical, forman un vocablo o expresión. Por simplificación, se suele llamar también acróstico a la expresión formada con dichas letras, siendo en la actualidad de aplicación a cualquier texto de cualquier naturaleza, no exclusivamente a poemas. Este recurso fue muy utilizado por los poetas italianos del Renacimiento. El siguiente poema, de autor desconocido, es un ejemplo de un acróstico doble en el que las letras iniciales y finales de los versos construyen la palabra Sonia.

SONIA
Supiste una vez má**s**
ocultar tu rostr**o**,
negar al mundo ese do**n**
impreciso pero dulce, as**í**,
así amante: tu boc**a.**

Uno de los acrósticos más famosos de la lengua española está constituido por los versos que conforman el prólogo de la obra *La Celestina* [19] del autor Fernando de Rojas (1470-1541). La selección de la primera letra de cada línea del prólogo permite observar la siguiente oración en castellano: *El bachiller Fernando de Rojas acabó la comedia de Calisto y Melibea y fue nacido en la Puebla de Montalban.* Los fines y uso de este tipo de técnicas son tan variados como personas hay interesadas en utilizarlas. Un caso más reciente y destacable por su notoriedad fue el del Yak-42. En mayo de 2003, tuvo lugar un desgraciado accidente en el cual un avión Yakolev 42 se estrelló en Turquía, cerca del aeropuerto de Trebisonda, cuando transportaba de vuelta a casa a 62 militares españoles tras cumplir cuatro meses de misión en Afganistán. Todos perdieron la vida. La versión inicial del aparente accidente por error humano, se fue modificando tras las denuncias de los familiares acerca del mal estado de ésta y otras aeronaves utilizadas por el ejército español. Meses después de este lamentable suceso, la cadena radiofónica SER **(**Sociedad Española de Radiodifusión perteneciente al grupo de comunicación Prisa**)** publicó que el entonces ministro de Defensa, Federico Trillo, había responsabilizado del suceso, de forma encubierta, al Estado Mayor de la Defensa. Para

ello, Trillo utilizó el editorial de la Revista Española de Defensa para ocultar esta información a través de un acróstico. Posiblemente, dado la sencillez del procedimiento, con la intención de que lo detectarán [20]**.**


EDITORIAL

Un error humano

El proceso de investigación abierto por la Comisión Internacional que trabaja para desentrañar las causas del accidente del YAK-42, en el que perdieron la vida 62 militares españoles, arroja unas conclusiones preliminares, no sometidas a discusión, en las que se pone de manifiesto que el error humano fue la causa de la tragedia. El presidente de la Comisión, Umit Cendek, subdirector general de Aviación Civil del Ministerio de Transportes de Turquía, aseguró en Madrid que aunque las causas definitivas de cualquier accidente aéreo son imposibles de determinar al cien por cien, en muchos casos, y éste es uno de ellos según su criterio, existen suficientes elementos como para determinar con bastante exactitud qué ocurrió. El avión funcionó sin problemas, las pistas a la navegación del aeropuerto también y las condiciones meteorológicas eran razonablemente aceptables. Un error humano determinó el accidente.

Respondiendo de los trabajos realizados hasta el momento, Cendek informó en rueda de prensa que, según los registros extraídos de la «caja negra» de datos, con la que se han reconstruido los últimos 30 minutos de vuelo, los pilotos del avión que intentaba aterrizar en Trebisonda (Turquía) en la madrugada del 26 de mayo confundieron el rumbo cero-nueve-cero con el rumbo uno-nueve-cero y cuando estaban convencidos de que se habían situado en la senda de aproximación a la pista de aterrizaje, se encontraron con una montaña insalvable. El hecho de que la «caja negra» que registra las conversaciones de los pilotos en cabina no funcionara no impide saber que los momentos previos al accidente se vivieron con absoluta normalidad. Existe la grabación de las conversaciones entre la torre de control del aeropuerto y la tripulación del YAK. Y esa grabación pone de manifiesto la rutina con la que los pilotos afrontaban esos últimos minutos. Segundos antes de la colisión, la torre solicita la posición del avión y los pilotos contestan «inbound» («entrando»), en la certeza de que están preparados para realizar la aproximación a pista. Cuando el sistema de alerta de aproximación al terreno les avisa de la inminente colisión, el piloto aumenta la potencia de los motores e intenta ganar altura en un empeño imposible por evitar el choque contra la montaña, donde quedaron inertes los sueños y las ilusiones de nuestros 62 «héroes por la paz».

Definitivo, de momento, es que el error humano provocó la tragedia. No admite discusión. Pero, aunque han pasado dos meses desde que se produjo el accidente, la Comisión aún prolongará sus trabajos un largo trecho antes de elevar a definitivas todas sus conclusiones. Se están analizando todos los elementos que permitan determinar con la mayor precisión posible todo lo que rodea el accidente.

En el Ministerio de Defensa quien quiere saber todo lo que se puede conocer sobre el accidente. Es quien está impulsando la investigación. El ministro Trillo-Figueroa lo dijo ante los medios de comunicación el mismo día del accidente y desde el primer momento ordenó al Estado Mayor de la Defensa un análisis pormenorizado sobre todo lo que ha rodeado la tragedia. Las 62 víctimas, su memoria y el vacío que dejan entre todos nosotros, sus familias y sus compañeros, lo demandan. Las comparecencias en el Parlamento del ministro de Defensa, tanto en Pleno como en Comisión, han querido ir facilitando con transparencia la información que progresivamente se ha ido conociendo, respetando los procedimientos judiciales y de investigación abiertos.

El Ministerio ha sido consciente, desde el primer momento, que quienes necesitaban más ayuda eran y son las familias de las víctimas. Han sido la principal preocupación del Gobierno y la prueba es que se han agilizado todos los trámites necesarios para que se sientan protegidas y acompañadas. Son muchos los familiares que agradecen la disposición del Ministerio para facilitar cuántas precisiones se exijan, aunque hay otros que mantienen una actitud muy crítica respecto al trabajo que se está haciendo. Es, hasta cierto punto, lógico. El rastro del dolor por la ausencia de los seres queridos no admite polémicas. Nada puede devolverles a los suyos. Lo que resulta menos lógico es confundir sistemáticamente a la opinión pública con noticias alarmantes que nunca se confirman y que cuestionan la credibilidad de un proceso serio, riguroso y transparente.

EMAD, Ministerio, Comisión Internacional, investigadores militares y civiles de accidentes aéreos, todo el mundo está trabajando, desarrollando iniciativas, para poder aproximarse a la verdad de lo ocurrido. Sin embargo, parece que a algunos les resulta más sencillo elevar a definitivas las conclusiones a las que previamente habían llegado antes que esperar a que se produzcan. Conviene no olvidar que es el ministro quien aporta los datos de la investigación y sus conclusiones preliminares en sede parlamentaria, por más que a algunos les hubiera gustado que los titulares de prensa, muchos de ellos descontextualizados del desarrollo de las investigaciones, fueran los que marcaran las conclusiones definitivas sobre el accidente. Quizás las prisas por acortar el calendario no sean las mejores consejeras. ◆

RED

Julio-agosto 2003 Revista Española de Defensa 5

Acróstico. Yak-42. Ex-ministro de Defensa. F. Trillo.

Revista Española de Defensa:

"El Responsable Definitivo es El FMAD"

(Estado Mayor de la Defensa)

Figura 1. Acróstico sobre el Yak-42 en la revista española de defensa

c) Código en Jerga **(en inglés, *jargon code*)**

Un código en jerga, consiste en sustituir símbolos o expresiones (por ejemplo, palabras), por otras no tan comunes (o inventadas) para un uso concreto. En sentido práctico, consiste en la creación y utilización de un lenguaje secreto de comunicación, normalmente, sencillo y versátil, conocido por un grupo de personas y desconocido por el resto. Conceptualmente se encuentra en un punto intermedio entre criptografía y esteganografía. Un ejemplo famoso de código en jerga fue el *Tora! Tora! Tora!* usado por la armada japonesa para comunicar el ataque a Pearl Harbor en 1941 [6]. Tal fue el miedo de la aplicación de estas técnicas tan difíciles de detectar que el servicio postal de los Estados Unidos censuró después del ataque de Pearl Harbor diferentes cartas de correo, por miedo a que ocultarán información peligrosa, por ejemplo, juegos de ajedrez vía correo, dibujos de niños, crucigramas, etc. Incluso los sellos de las cartas eran quitados y sustituidos por otros de igual valor, pero diferente forma.

En la actualidad esta modalidad ha tenido una variante pictórica muy importante. Un ejemplo reciente de código en jerga en el mundo informático, es el denominado warchalking.

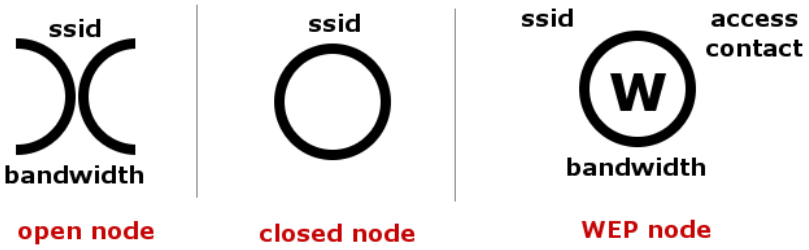

Figura 2. Algunos de los símbolos del lenguaje warchalking

Se conoce como warchalking al lenguaje de símbolos, que, escritos con tiza en paredes y suelo de las calles, informa a los posibles interesados de la existencia de una red inalámbrica con cobertura en ese punto. Está inspirado en otros procedimientos de marcado más antiguos, como el hobo-chalking, sistema de marcado que utilizan los vagabundos para señalar casas que son amables, donde dan comida, etc. La relativa sencillez de los símbolos y su característica de no perdurabilidad durante grandes periodos de tiempo hacen que este código sea muy dinámico y se adapte a las características cambiantes de las redes de las cuales informa. Estos son uno de los factores que han hecho posible su proliferación por las grandes ciudades.

d) Rejillas (en inglés, *grilles*)

Estos procedimientos esteganográficos[4] consisten en la selección de ciertas letras o palabras de un documento utilizando para ello un conocimiento adicional que a modo de plantilla facilita la selección de dicha información. En la terminología habitual esta plantilla se conoce como grille o, en español, verja o rejilla, en tanto en cuanto deja ver solo lo que interesa. El mejor procedimiento para entender estas ideas la encontramos en el renacimiento y es conocido como la *rejilla de Cardano* **(**Cardan grille**)** en honor a su creador el célebre renacentista Girolamo Cardano (1501-1576) [11] [21] que reinventó en 1550 un procedimiento cuyos orígenes se encuentran en la cultura milenaria china. El sistema *Cardan grille* en sus orígenes funciona de la siguiente manera: cada destinatario posee un pedazo de papel o cartón con agujeros cortados en él, la verja o rejilla. Cuando esta plantilla se pone encima de un mensaje inocente, los agujeros dejan ver letras específicas del mensaje, revelando el mensaje oculto. Este tipo de técnicas son muy difíciles de detectar en tanto en cuanto la plantilla que actúa a modo de filtro, a efectos prácticos como si habláramos de la clave del sistema, se mantenga en secreto. El mayor inconveniente de este procedimiento es que tanto emisor como receptor deben distribuir de forma segura la plantilla y la información oculta de un texto inofensivo debe ajustarse a esa plantilla. En la práctica, podría resultar complejo crear mensajes de una forma rápida reutilizando una misma plantilla; si esto no fuera posible el emisor tendría que transmitir de forma segura, en el caso extremo, una plantilla por mensaje oculto que quisiera que el receptor recibiera, lo cual unido a la baja capacidad de ocultación de información, al ser un procedimiento manual que requiere un texto grande para no facilitar la detección, hace de este procedimiento poco práctico hoy día.

Basándose en los mismos principios, se han publicado diferentes variantes en función de cómo se utilice la plantilla. Así, por ejemplo, ir rotando 90 grados la plantilla [22] cada vez que se obtiene una letra del mensaje oculto (turning grille), etc. A lo largo de la historia se han documentado [6] múltiples usos de estas variantes e incluso han tenido su repercusión en la literatura, léase por ejemplo la obra *Mathias Sandorf* de Julio Verne (1828-1905) [23].

Otro procedimiento ingenioso fue utilizar un código especial sobre periódicos, en terminología inglesa se conoce como *newspaper code*. Este método desarrollado en la era Victoriana, época de gran expansión económica y social de Gran Bretaña entre 1837 y 1901, permitía a las clases pobres comunicarse libremente. Para ello hacían pequeños

[4] Conceptualmente la diferencia sutil respecto de los null-ciphers consiste en que estos últimos funcionan mediante un conjunto de reglas preestablecidas mientras que en el caso de las rejillas ese patrón de conducta lo establece la propia rejilla.

agujeros encima de ciertas letras del periódico, que una vez unidas formaban el mensaje encubierto [6]. Aunque es un procedimiento más práctico que el anterior, adolece de mayor visibilidad. Estos procedimientos encontraron utilidad, por ejemplo, en la II Guerra Mundial y en la Guerra Fría entre EE.UU y la URSS [6].

2.2 Semagramas

Los semagramas (en inglés, *semagrams*) consisten en la utilización de la estructura, formato y configuración de símbolos y objetos para establecer un medio de comunicación para ocultar una información. En general, refiriéndose a textos, consisten en pequeñas variaciones de la estructura normal de un documento, que, aunque visibles, no por ello son fáciles de detectar. Un ejemplo clásico es ocultar información utilizando más o menos espacios entre las palabras de un documento o modificar gráficamente los caracteres del mismo. Su utilización, no se limita a textos, puede verse en fotografías, dibujos, música, etc. Por ejemplo, un dibujo con un determinado número de manzanas en un árbol puede contener una información secreta.

En general, se pueden distinguir dos tipos: *visual semagrams* y *text semagrams*.

a) Semagramas visuales

Los semagramas visuales (en inglés, *visual semagrams*) consisten en utilizar todo tipo de símbolos y señales para ocultar un mensaje. Habitualmente objetos físicos, como, por ejemplo, objetos de uso cotidiano, ya que por ser comunes no se le presta excesiva atención. Por ejemplo, ocultar información utilizando un garabato de una hoja, la distribución de ciertos objetos en un escritorio, las manecillas paradas de un reloj (que podría indicar la hora de un hecho), etc.

Figura 3. Mensaje secreto solucionado por Sherlock Holmes (AM HERE ABE SLANEY) en la obra The Adventure of the Dancing Men de Arthur Conan Doyle **[24]**.

b) Semagramas textuales

Los semagramas textuales (en inglés, *text semagrams*) se aprovechan de la estructura, formato y configuración de un documento para enmascarar una información. La estructura natural de un texto puede facilitar la utilización de ciertas técnicas esteganográficas: inserción de espacios, uso de caracteres no visibles, tipografía, etc. El uso del formato particular de un documento y sus atributos posibles permiten la implementación de procedimientos de enmascarado de información. En la actualidad, una evolución de estos principios consiste en utilizar los atributos de un texto digital como el color del texto, el atributo de negrita, cursiva, subrayado, la fuente del tipo de letra elegido, el tamaño del carácter, etc. Todos estos atributos permiten la creación de códigos que permiten la ocultación de información sensible, clásicamente, codificaciones binarias. Por ejemplo, el texto: "`este mensaje almacena un octeto de información 01010101b`" almacena la información binaria 01010101. Para ello, para las palabras impares se utiliza un tipo de letra Courier y para

las palabras pares Courier New. En este ejemplo, se aprovecha la similitud de ambos tipos de letras para establecer una codificación binaria, equivaliendo una palabra en Courier a un bit 0 y una palabra en Courier New a un bit 1, por ejemplo.

Otro ejemplo notorio de este tipo de técnicas consiste en enmascarar información secreta, crear sistemas de codificación binaria, mediante modificaciones horizontales y verticales. Los procedimientos esteganográficos más documentados sobre modificaciones horizontales están relacionados con el uso de espacios en blanco en un documento. Las técnicas de ocultación basadas en esta idea son: la modificación del espaciado entre las palabras de una frase, codificar información añadiendo uno o más espacios al final de una línea, utilizar los espacios después de los signos de puntuación (comas, puntos...), etc. La introducción de más o menos espacios, depende de si estos son de un tamaño prefijado o si dicho tamaño puede modificarse.

Adicionalmente, estos procedimientos de ocultación se pueden realizar mediante modificaciones verticales, es decir, jugar con la distancia vertical, fija o variable, entre elementos de un texto para codificar una información binaria. Independientemente del procedimiento elegido, el tamaño de los "espacios" en un documento, si no se realiza de forma manual, depende de la herramienta de edición utilizada para la creación del texto. Una buena herramienta para este propósito, en el siguiente capítulo se profundizará más, es el sistema de tipografía desarrollado por Donald E. Knuth, denominado TEX [25]. Hoy día, paquetes de macros como LATEX [26], que utilizan dicho sistema, se utilizan con gran éxito. TEX permite la creación de documentos profesionales de gran calidad, permitiendo un control muy preciso sobre todos los aspectos del texto, por ejemplo, su estructura, tamaño de las letras, etc. En este sentido, permite un control muy preciso sobre el tamaño del espaciado entre palabras o el tamaño de los espacios que siguen a ciertos signos de puntuación. Aunque este no fue el objetivo para el cual se creó, ni principalmente el uso que se le da, es cierto que es una excelente herramienta que facilita la ocultación de información en textos (en los documentos generados mediante "compilación"), como se verá posteriormente. Por ejemplo, permite añadir espacios de tamaño tan reducido entre palabras o entre los caracteres de una palabra que un lector no sea capaz de apreciarlos.

Todas estas técnicas documentadas sirven de referencia para profundizar en próximos capítulos en procedimientos más robustos de esteganografía lingüística.

3. ESTEGANOGRAFÍA LINGÜÍSTICA EN EL SIGLO XXI. ANTECEDENTES

Sea lo que sea aquello que se quiere
decir, no hay más que una palabra para
expresarlo, un verbo para animarlo
y un adjetivo para calificarlo.
Guy de Maupassant

3.1. Avances en el procesamiento del lenguaje natural. Protección de comunicaciones digitales

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 on-line, páginas web, correos electrónicos, mensajería instantánea, blogs, redes sociales, sms, voz transcrita automáticamente a texto, etc.

En este entorno, la última década es testigo de la utilidad del procesamiento del lenguaje natural, lo que denominaremos de aquí en adelante lingüística computacional, en tecnologías tan dispares como son los sistemas de traducción automática, los algoritmos de reconocimiento del habla, algoritmos de análisis ortográficos, los sistemas de *data mining*, algoritmos para el resumen automático de textos, compresión de datos, recopilación de inteligencia [108], etc. Además, a todas estas aplicaciones, desde hace bastante tiempo, se le une su utilidad en la protección y anonimato de comunicaciones. Por ejemplo, en procedimientos criptográficos clásicos cómo el estudio de la frecuencia de aparición de digramas, trigramas, etc., permitía hacer más seguros (o atacar) sistemas de cifra utilizados en comunicaciones diplomáticas y militares.

Hoy día, los algoritmos de procesamiento del lenguaje natural tienen una aplicación clara en tareas de inteligencia, recopilación y sintetización de información. Una muestra de ello es el Open Source Center, creado en 2005, organismo de la inteligencia estadounidense encargada de analizar las comunicaciones e información en la red, especialmente de los medios sociales: blogs, wikis, foros y redes sociales de todo el mundo. Adicionalmente, nuevas propuestas permiten vislumbrar aplicaciones más claras del procesamiento del lenguaje natural y la protección de comunicaciones digitales. Un artículo que permite acotar esta cuestión fue publicado por Atallah et al. en el año 2000 [109] donde se resumía la utilidad de estos avances en tareas de inteligencia, recopilación y sintetización de información, y más interesante, en aplicaciones concretas de uso como son: los sistemas de memorización de password aleatorios o los sistemas de marcado digital de textos [110].

En este marco, la lingüística computacional ha facilitado en los últimos 10 años el avance, especialmente en su aplicación a la lengua inglesa, de una nueva vertiente de utilización de todo el conocimiento lingüístico disponible para una lengua concreta. Estamos hablando de la posibilidad de ocultar información en lenguaje natural, es decir, de la ciencia de la esteganografía lingüística.

3.1.1 Esteganografía lingüística. Definiciones

A falta de una definición más completa, es importante diferenciar esteganografía textual de lingüística, podemos definir la esteganografía lingüística como aquel conjunto de algoritmos robustos que permiten ocultar una información, típicamente binaria, utilizando como tapadera información en lenguaje natural. En la actualidad, la esteganografía lingüística intenta mezclar principios de la ciencia de la esteganografía y la lingüística computacional (análisis automático del contenido textual, generación textual, análisis morfosintáctico, lexicografía computacional, descripciones ontológicas, etc.) para crear procedimientos públicos no triviales según los principios de Kerckhoffs. La seguridad de estos procedimientos dependerá exclusivamente de una información adicional conocida exclusivamente por el emisor y el receptor a modo de clave. En la práctica, este postulado no es nada sencillo y la complejidad de generar estegotextos resistentes a ataques estadísticos y lingüísticos por parte de analistas (humanos) y de sistemas automáticos (máquinas), es bastante elevada.

En realidad, los conocimientos lingüísticos que soportan la ciencia de la esteganografía lingüística intentan solventar las dos problemáticas siguientes:

a) Anonimato y privacidad. La posibilidad de ocultar información en textos en lenguaje natural permitiría intercambiar información dificultando su detección por parte de personas y sistemas de monitorización automáticos (Echelon, Carnivore, Sitel…), no sólo por la dificultad de invertir los mecanismos de protección sino además porque el volumen de información textual intercambiado en las redes de telecomunicación podría hacer inviable la recopilación y el análisis por un potencial estegoanalista, mejorando, o eso se espera, la privacidad e incluso el anonimato de dichas comunicaciones. Sería de interés en términos de libertad de expresión.

b) Marcado digital de textos. En la actualidad, la integridad y la autenticidad de una información pueden ser garantizadas mediante la utilización de la denominada firma digital. En general, se trata de procedimientos que generan unos datos extras basados en la información que se quiere proteger y que se adjuntan a esa misma información. Estos procedimientos tienen el inconveniente que la información generada no está autocontenida en la información que se quiere proteger y por tanto puede ser separada, con los problemas en términos de verificación que esto puede suponer. La posibilidad de ocultar información en un texto en lenguaje natural, si esta modificación no supusiera "alteraciones notorias" del texto utilizado como portador, facilitaría la inclusión autocontenida de firmas que podrían tener utilidad en autenticidad e integridad de escritos en una lengua concreta. Una firma autocontenida permite garantizar que la firma de un autor presente en un artículo corresponde precisamente al texto que escribió y se puede, además, demostrar que él es el autor de dicho documento (*authorship proof*) así como "realizar un seguimiento" del mismo, por ejemplo, para medir la difusión de una obra.

3.1.2 Líneas de investigación actuales en esteganografía lingüística

Existen dos grandes líneas de investigación para proporcionar soluciones a las dos problemáticas indicadas: a) la generación automática de estegotextos y b) la modificación de textos existentes.

a) Generación automática de estegotextos

La generación automática de estegotextos consiste en procedimientos que faciliten la generación de textos que ya lleven incluida la información que se quiere ocultar. Esta idea, que suena apasionante, en la práctica resulta de una enorme complejidad, ya que, si bien es viable generar textos con validez léxica y sintáctica, la semántica y la coherencia global son a día de hoy temas sin una solución clara. Existen dos procedimientos generales de generación automática de estegotextos, en ocasiones combinados: los basados en imitación gramatical y los basados en imitación estadística. Esta línea de investigación tiene utilidad en la creación de canales ocultos de información útil para anonimato y privacidad de las comunicaciones.

b) Modificación de textos existentes para crear estegotextos

El mecanismo más tradicional de ocultación de información consiste en utilizar un texto existente para enmascarar información basándose en algunos elementos del texto o modificaciones del mismo. Los procedimientos actuales, no exentos de problemas, consisten en: modificaciones léxicas -el mecanismo más utilizado es la ocultación de información basada en la sustitución de palabras por sus sinónimos-, modificaciones sintácticas y semánticas, ocultación mediante el "ruido" de las traducciones de un texto entre diferentes idiomas, ocultación basada en errores tipográficos y ortográficos, ocultación basada en símbolos de puntuación-abreviaturas y ocultación basada en modificaciones de la estructura o formato de un texto, por ejemplo, el uso de espacios de tamaño variable entre palabras, variación del estilo de fuente, etc. Esta línea de investigación tiene utilidad en la creación de canales ocultos de información (anonimato y privacidad) y en el marcado digital de textos.

En los siguientes apartados se realiza un esfuerzo para tratar de destacar los trabajos más notorios en esteganografía lingüística en las últimas décadas. El período bajo estudio se centra desde principios de la década de los 90 del siglo XX hasta nuestros días. Esto es así porque la información pública recopilada indica que fue a partir de esta fecha cuando se empezaron a publicar, de manera más o menos intensa, propuestas de esteganografía lingüística no basada en oscuridad en cuya seguridad se aprovechaba de algunas características del procesamiento del lenguaje natural (lingüística computacional). Un buen trabajo para situar las publicaciones más interesantes fue publicado en 2007 por Bergmair [111] de la Universidad de Cambridge. Bergmair realizó un esfuerzo en recopilar los trabajos más significativos en esteganografía lingüística de finales del siglo XX a principios del siglo XXI. Es cierto, que hoy día esa lista no está actualizada, por ejemplo, los nuevos artículos recopilados destacan el avance en los últimos cinco años del estegoanálisis lingüístico, pero muchos de los trabajos más significativos, especialmente en su aplicación a la lengua inglesa, están referenciados. En los últimos tres años, el número de publicaciones de esta temática ha ido en aumento, especialmente en diferentes idiomas, no exclusivamente en lengua inglesa. No obstante, todavía es una ciencia muy minoritaria, y poco divulgada, comparada con otros procedimientos esteganográficos, por ejemplo, los aplicados a imágenes digitales, audio o vídeo digital. Por estos motivos, es interesante analizar en los próximos apartados la información más significativa de esta temática.

3.2. Generación automática de estegotextos en lenguaje natural

La generación automática de estegotextos es una rama dentro de la ciencia de la esteganografía lingüística cuyo objetivo consiste en crear textos en lenguaje natural en función de la información que se desee ocultar.

En la antigüedad, y actualmente en otra rama importante de investigación en esteganografía lingüística, la modificación de textos existentes fue la principal tendencia para ocultar información en textos en lenguaje natural. Esta tendencia, al margen de otras cuestiones lingüísticas y estadísticas, tiene la problemática de tener que mantener en secreto (o destruir) el texto original/portador en el cual se realizarán las modificaciones y mediante el cual se creará el estegotexto resultante con la información enmascarada. Debe minimizarse al máximo la posibilidad de que un potencial estegoanalista pudiera realizar comparaciones entre el texto original y el estegotexto creado que le simplificara la tarea de detección. Por estos motivos, la generación automática de estegotextos muestra interés. En primer lugar, el estegotexto generado, que depende de la información a ocultar, puede ser mejor modelado realizando todo tipo de consideraciones lingüísticas y estadísticas en el proceso automático de creación. Por otro lado, esta tendencia facilita la creación de un estegotexto único por cada comunicación enmascarada a realizar, lo que complica el trabajo de un potencial estegoanalista.

Los algoritmos de generación automática de textos deben considerar la calidad léxica, sintáctica y semántica, así como la cohesión y coherencia del estegotexto resultante. Para aproximarse a este problema, desde finales del siglo XX dos grandes líneas de generación, que se pueden entremezclar, se han propuesto: unas basadas en imitación gramatical y otras basadas en imitación estadística de un texto "típico" en una lengua concreta. A continuación, se va a profundizar en algunas de las propuestas conceptualmente más interesantes.

3.2.1 Modelado estadístico del lenguaje natural. Imitación estadística de textos de entrenamiento

La generación de textos en lenguaje natural podría partir de la idea de que las palabras y las expresiones presentes en un lenguaje siguen un determinado orden. Un modelado estadístico del lenguaje natural permitiría cuantificar diferentes aspectos sobre textos en una lengua concreta que tendría utilidad para la creación de textos con validez lingüística que no sólo no levanten sospechas a un software automatizado (máquina) sino tampoco a un lector humano. En general, puede ser muy complejo realizar un modelado estadístico preciso sobre un lenguaje. Por ello, en determinados entornos, como pueda ser la esteganografía, modelados estadísticos más sencillos serían, en principio, prácticos para propuestas reales. Por ejemplo, analizar la estadística de unos textos de entrenamiento que se toman como referencia. Si el modelo estadístico estuviera basado en textos de entrenamiento, los estegotextos generados basados en ellos reproducirían de una manera u otra su estructura. De hecho, esta idea queda presente en algunas de las propuestas conceptualmente más interesantes de generación automática de estegotextos basada en imitación estadística.

Un ejemplo significativo es la propuesta de Peter Wayner en 1992 [112] [113] analizada en su aplicación a lengua inglesa. La propuesta de Wayner se basa en la generación automática de estegotextos basada en la imitación estadística de una o más fuentes de textos (S). La idea conceptual es sencilla: *Cójase una función de imitado f que modifique un fichero A de forma que asuma las propiedades estadísticas de otro fichero B. Es decir, si p(t,A) es la probabilidad de que una cadena t suceda en A, entonces una función de imitado f, hace que la p(t,f(A)) sea aproximadamente p(t,B) para toda cadena t de tamaño menor que n.* La complejidad del modelo estadístico de imitado (análisis de frecuencia) depende, precisamente del orden estadístico n (orden de complejidad del algoritmo). Según esta idea, Wayner definió el siguiente algoritmo de imitado:

1. Construir una tabla con todas las diferentes combinaciones de n letras que ocurran en S y contabilícese el número de veces que ocurren en S.

2. Elegir una de ellas aleatoriamente que actuará de semilla inicial. Esto generará las primeras n letras de T (el estegotexto).

3. Repetir este punto hasta que se genere todo el texto deseado.

    a. Coger las n-1 letras siguientes de T.
    b. Buscar en la tabla estadística (creada) todas las combinaciones de letras que comienzan con esas n-1 letras.
    c. La última letra de esas combinaciones forma el conjunto de posibles elecciones para la siguiente letra que será añadida a T.
    d. Elegir entre esas letras y usar la frecuencia de sus ocurrencias en S para "evaluar" cuál es la mejor elección.
    e. Añadirla a T.

Según este algoritmo un primer orden de imitado genera caracteres aleatorios de acuerdo a su distribución estadística. En un segundo orden se imita la distribución de parejas de caracteres de los textos S de entrenamiento, y así sucesivamente para mayor orden. Se supone, por la información publicada [113], que en su aplicación a la lengua inglesa, dependiendo del texto y del orden, textos de al menos decenas de KB y orden mayor que 6, pueden obtenerse estegotextos con validez léxica y sintáctica, e incluso, algunos, no exento de errores, con apariencia semántica-estructural.

El proceso de ocultación de información se realiza mediante la selección de las opciones de la próxima letra a mostrar. Wayner justificó cómo esto se podría hacer, entre otras opciones, utilizando un árbol de Huffman. El algoritmo esteganográfico, basándose en las frecuencias de aparición de la próxima letra a mostrar, crea un árbol Huffman con ellas, asignándoles un código binario a cada una, este código es el correspondiente a la información binaria necesaria para alcanzar el nodo en el cual está presente la letra en el árbol Huffman. La ocultación de información consistiría en ir eligiendo nodos del árbol, cuyo código–rama coincidan con la información a ocultar. Si la selección de las ramas de este árbol, que imita la estadística de la fuente, es aleatoria el texto resultante imitará (o se aproximará) mejor a la distribución estadística del texto fuente. Si imita la estadística es razonable que imite la sintaxis y gramática del texto de entrenamiento.

Order 3 text:

> Mimic function of character and Compresentextendent-extraditory. The are on . The ther his possible inforcest the parse tree generated. This define method partible. These authough eith a fore alle, it text-free is related he converted searlies.}{Figure noded the task by up the tree, that undefined the of Huffman exper accur withough, instribest of rance,[10] Sahniquely is f is to there mation of the get is figure will repen the equencident composion of one tree a miming an because charaction function cannell. A classage, na ,corress of matree can for feed fix of nj.This in a file one can compressages these used. Notical descendent varized which who examplies of a lon, but to messemblings to bits string-- the lowere 4: Anyonential if the Introduction. The outing. Simpossionstrafficienceal

Order 4 text:

> Mimic function. The fact also process. W. H. Free the tree the mimic function dering of coversion which has on to breaks a tree and Computer that is and recognize the no attacks of productional discussion of a search by labeling of coverse, the precision to get from and Intracter solutions to modified to principlest version f, is a files structure the literate a string dependentical provide the compression.This needed to lead to the tree... {Figure 1 after is to terminally exponentity which can because assigning Context Free computer that than nj. If the practers their provide information. The scrambled to the choose the provide size with a 1. The statistical grammar is letter. These Huffman compression to statistical of variable, 't' is updated. This said to branches in the alphabet to the characters into ther hack provides from technique of the previous encryptographers can be useful follow a strength order

Order 6 text:

> Mimic Functions will productions can be used extend the inverse, Huffman encoded with probabilities that a characters in one-to-many functions by removing the value to be anything. Anyone watching must be seeded by repeatedly querying a Huffman compressed blocks which define the functions convert the root and the character dependent, so a random bits, and the work which always follow t. A Huffman coding technique can be built by using Context Free Grammar can be useful in cases construction procedure that they will be based upon the characters can be done in the mimic function based upon Huffman compresses as bits in a tree.

Figura 4. Ejemplos de estegotextos en inglés aplicando diferentes órdenes del algoritmo de Wayner

Independientemente de problemas lingüísticos y esteganográficos, la utilización de imitado a modo carácter sigue produciendo fallos. Esta propuesta de imitado tiene unas limitaciones intrínsecas al algoritmo. En la práctica la aproximación estadística de la fuente de entrenamiento (texto) realizada por la idea de Wayner y variantes dependerá de varios factores, entre otros de la función de imitado utilizada. Por ejemplo, si la función de imitado está basada en un árbol Huffman (idea original de Wayner) una posible codificación para 3 elementos (a, b, c) con probabilidades (0'80, 0'13, 0'07)

sería (1, 01, 00). Si su función inversa es usada como función de imitado los caracteres aparecerían con frecuencia (0’5, 0’25, 0’25) lo cual dista de ser una aproximación estadística razonable. Esto se debe a que utiliza un árbol binario para la representación de los elementos, ya que su distribución estadística siempre será una potencia negativa de 2. Esta potencia depende de la distancia entre la raíz y la hoja correspondiente del árbol. Existen diferentes mecanismos para disminuir este problema [112]. En general, la existencia de muchos caracteres en el árbol hará que su profundidad sea mayor y la aproximación estadística a la fuente también, así como la utilización de un orden de complejidad mayor. El límite del orden o del tamaño del texto fuente a procesar vendrá dado por los recursos hardware involucrados en las operaciones.

En 2002, A. J. Tenembaum continuó este trabajo en su aplicación a lengua inglesa. Para ello, partiendo de la propuesta de Wayner, entrenó el algoritmo midiendo las frecuencias de aparición de palabras en lugar de letras. Esta investigación abrió la puerta al diseño de algoritmos que basados en la idea de Wayner podrían utilizar otros patrones de imitado en la generación automática para producir estegotextos de mejor calidad lingüística, al menos para lengua inglesa [114].

En esta línea de investigación, pueden incluirse las propuestas basadas en cadenas de Markov. Una cadena de Markov puede describirse como un modelo estocástico en el cual la probabilidad de que suceda un evento depende exclusivamente del evento anterior. Esto tiene aplicación en esteganografía lingüística y estegoanálisis. Por ejemplo, respecto del estegoanálisis puede observarse la propuesta de Simova et al. en 2005 [115] donde describieron cómo entrenando un modelo HMM (Hidden Markov Model) con textos en inglés, utilizando el corpus Brown, era factible determinar cómo de buena era la “apariencia” de estegotextos creados o modificados en lengua inglesa con diversos procedimientos, es decir, clasificarlos o no como potenciales estegotextos.

En realidad, en 2003, sería Shu-feng [116] el que publicaría la posibilidad de generar estegotextos mediante una señal procedente de una fuente de señales basadas en un modelo de Markov. En esta propuesta la sucesión entre elementos, y por tanto los elementos a elegir, se seleccionan con la misma probabilidad. Esta investigación no es interesante, ya que como publicaron Meng et al. en 2009 [117], la elección de los candidatos que suceden a una palabra o expresión deben considerar su estadística de aparición y no ser elegidos como si se produjesen con la misma probabilidad, ya que si no los ataques estegoanalíticos se simplifican notoriamente. Aunque por desgracia el estudio no se realizó con profundidad, en 2009, Dai et al. [118] introdujeron la posibilidad de generación de estegotextos utilizando cadenas de Markov considerando en todo momento la probabilidad de las palabras a seleccionar en función de las palabras antecesoras y de las que se encontraban en su mismo “nivel/estado” del proceso.

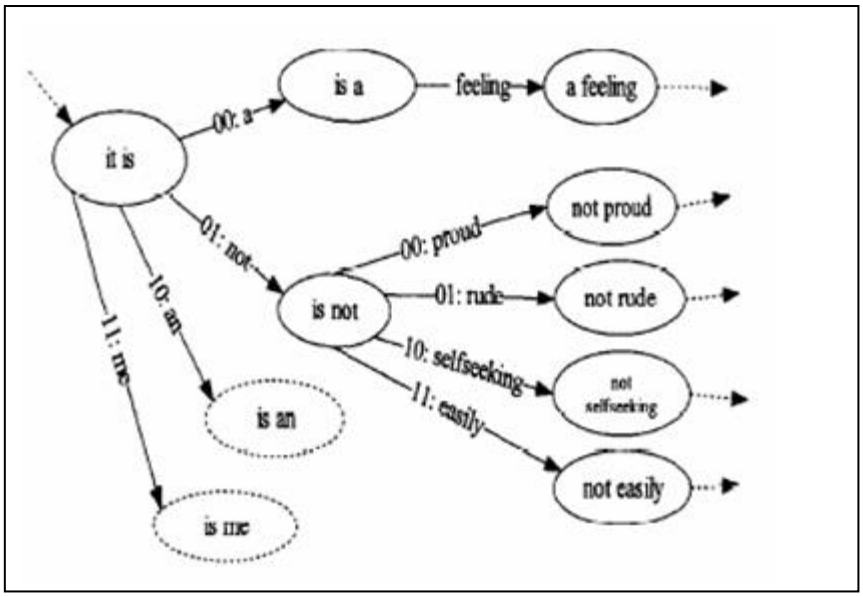

Figura 5. Cadena de Markov sin probabilidades entre palabras

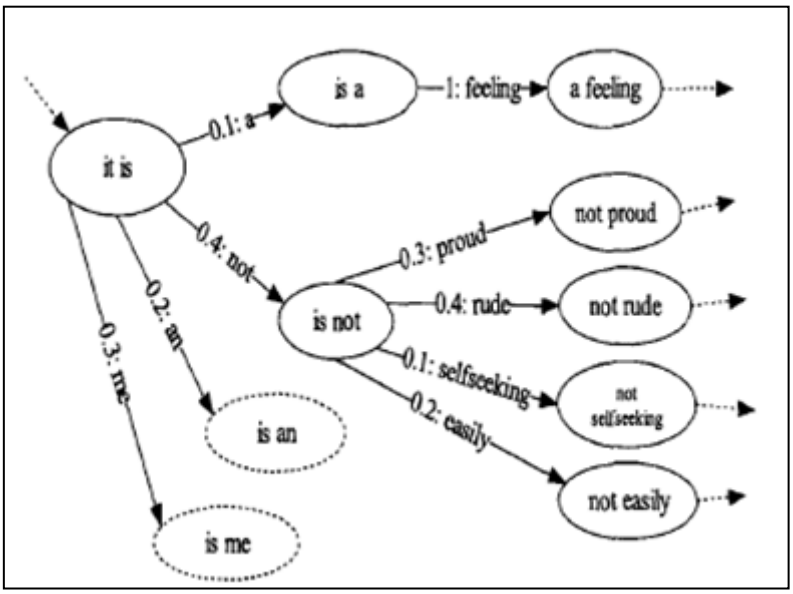

Figura 6. Cadena de Markov con probabilidades entre palabras

Independientemente del proceso seguido para imitar la estadística de un lenguaje, queda claro que su modelización facilita la elección de palabras que darán lugar a oraciones con sentido. Este hecho tiene utilidad en la generación automática de estegotextos en multitud de idiomas.

3.2.2 Modelado gramatical del lenguaje natural. Gramáticas libres de contexto

Los textos en lenguaje natural pueden verse como un conjunto de léxico (palabras) que mediante uniones (reglas gramaticales) permiten construir fragmentos con semántica cuya unión (coherencia) aporta un valor concreto al lector. Dado que de una forma simplista un texto puede verse como un conjunto de oraciones unidas, tiene sentido

analizar la posibilidad de imitar la estructura gramatical de una lengua concreta y analizar si en esa imitación para generar texto válido es posible ocultar información. Una excelente manera de realizar esto es mediante el uso de gramáticas libres de contexto. Para comprender su uso es necesario remontarse a los años 60 del siglo XX.

En la década de los 60 el excepcional lingüista A. Noam Chomsky postuló la gramática generativa. Esta gramática se definió como el conjunto de reglas innatas que permite traducir combinaciones de ideas a combinaciones de palabras y en este sentido, *la gramática se convertía en un sistema combinatorio discreto que permite construir infinitas frases a partir de un número finito de elementos* mediante reglas diversas que pueden formalizarse mediante una gramática formal gobernada por normas de transformación [119]. Según esta teoría de lenguaje formal una CFG (Context-Free Grammar) se define como una gramática en la que cada regla de producción es de la forma v::=w, donde v es una variable y w es una cadena de símbolos terminales y no terminales. Se entiende por *terminal* la información última de cada regla, por ejemplo, una palabra determinada. Por tanto, en general, una CFG se compondrá de terminales, variables y producciones. Las CFGs han jugado un papel nuclear en el diseño de lenguajes de programación y compiladores, así como en el análisis de la sintaxis del lenguaje natural.

En las década de los 90 [112] [120], Peter Wayner vinculó la posibilidad de utilizar las construcciones CFGs en la generación de estegotextos de forma automática. Esta idea facilitaría la creación de estegotextos que, al menos, tendrían validez gramatical-sintáctica. Estos estudios los realizó en su aplicación a la lengua inglesa. A continuación, para facilitar su compresión se añade un ejemplo en lengua española.

Variable_Inicio S ::= *AB (.5) | AC (.5)*
A ::= “Buenos días,”(.25) | “Buenas tardes,”(.25) | “Buenas noches,” (.25) | “Hola”(.25)
B ::= “estimado amigo” C (.5) | “estimado compañero” C (.5)
C ::= “Juan,” D (.25) | “Pedro,” D (.25) | “Lucas,” D (.25) | “Tomás,” D (.25)
D ::= “quedamos algún día para” E (.5) | “dame tu número de teléfono para” E (.5)
E ::= “hablar” F (.5) | “charlar” F (.5)
F ::= Un saludo (1.0).

Figura 7. Ejemplo de PCFG en lengua española en formato BNG. Ocultación máxima de 8 bits.

La ocultación de información se realiza mediante la selección de elementos concretos dentro de una regla específica, regla que es elegida mediante algún algoritmo de selección concreto. En el ejemplo anterior, una posible oración extraída (selección de la regla AB) de las reglas definidas podría ser: “Buenos días, estimado compañero Tomás, dame tu número de teléfono para charlar. Un saludo” la cual ocultaría 8 bits (1+2+1+2+1+1).

Wayner desarrolló varios ejemplos interesantes aplicando estas ideas [113]: spammimic (ocultación en un mensaje con estructura de correo de spam), baseball game, etc. Aunque Wayner se esforzó en formalizar la construcción de CFGs seguras con utilidad esteganográfica [120], es cierto que su utilidad esteganográfica debe ser muy matizada. El primer problema es que la gramática debe permanecer privada, emisor y receptor la deben conocer, ya que si no es así un atacante podría inferir fácilmente la información

oculta. Este problema es mayor si la gramática es estática-manual. Si esta gramática fuera conocida por el atacante forzaría al emisor y al receptor un nuevo proceso tedioso (manual) y costoso de generación de una nueva gramática. La calidad del estegotexto depende claramente de la gramática y si esta tiene pocas reglas es más que probable la repetición de frases y términos en el estegotexto, facilitando a los estegoanalistas su trabajo. Aunque la gramática sea generada automáticamente de uno o más textos de referencia, conocidos por emisor y receptor, deben considerarse otros análisis al generar algoritmos esteganográficos basados en CFGs, por ejemplo, las palabras (términos) en una CFG se relacionan con sus vecinos en formas fijas. Aunque se añadan modelos estadísticos a las gramáticas como son las Probabilistic Context Free Grammars, PCFG, para dificultar ataques de análisis, siempre existirán correlaciones mutuas si se quiere que el texto sea coherente para un humano [113]. Por otro lado, deben considerarse los ataques basados en estudio de terminales, información última de cada regla, ya que, aunque las variaciones de texto creados puedan crecer sustancialmente con el tamaño de una gramática dada, el número de terminales está limitado por el tamaño de la gramática, lo cual significa que forzosamente, si el texto es lo suficientemente grande, se tienen que producir (y por tanto repetir) combinaciones lineales de terminales.

En la práctica resulta realmente complejo utilizar CFGs en herramientas públicas de manera robusta en la concepción actual. Un intento notorio, de los pocos destacables, fue el sistema NICETEXT, del que se pueden extraer ideas para nuevos diseños.

En 1997, Chapman y Davida en diversas investigaciones [121] [122] [123][124] desarrollaron un sistema software, NICETEXT, que permite generar modelos gramaticales basados en la posibilidad de imitar la gramática de uno o varios textos de entrenamiento. Estas reglas gramaticales, a modo de elementos etiquetados de una oración, permiten la generación de frases del estegotexto resultante.

NICETEXT permite la generación dinámica de las reglas gramaticales basada en la imitación gramatical de textos de entrenamiento, es decir, habilita los procedimientos necesarios para identificar reglas sintácticas y mediante un etiquetador PoS (Part of Speech), *pckimmo*, permite definir qué tipo de palabra (categoría lingüística) forma cada elemento de la regla sintáctica generada (verbo, nombre, adjetivo, etc.). La novedad de esta herramienta reside en la forma de ocultación y en la recuperación de la información ocultada, ya que el receptor no necesita conocer la gramática utilizada por el emisor. La herramienta está basada en la sustitución de los elementos etiquetados en cada regla por palabras categorizadas por contenido semántico. En la práctica, este sistema esteganográfico hace uso de dos herramientas, una para ocultar (NICETEXT) y otra para recuperar la información oculta (SCRAMBLE). Según esto, el funcionamiento de este sistema esteganográfico podría sintetizarse en $NICETEXT_{D,S}(C)=T$ y $SCRAMBLE_{D}(T)=C$, siendo D un diccionario de palabras categorizadas por tipo y S (*meta-style source*) un conjunto de reglas de estilo de escritura basadas en las ideas de gramáticas libres de contexto. Además, este sistema incorpora herramientas que facilitan la creación del diccionario D de textos de entrenamiento.

Este esquema tiene varias ventajas importantes. Dado que la información se oculta independientemente de la gramática, el emisor en el peor de los casos podría utilizar una gramática única por comunicación y de la riqueza que desee. La ocultación de información se realiza mediante la selección de una palabra dentro de una categoría de

un diccionario categorizado. Este diccionario es compartido entre emisor y receptor y debe permanecer secreto.

NICETEXT introduce, adicionalmente, la posibilidad de utilizar principios de negación plausible en esteganografía lingüística [124]. En NICETEXT puede suceder que la información a ocultar no sea suficiente para completar todos los términos de una regla seleccionada de la gramática, por ello se necesita utilizar una información aleatoria para seleccionar el resto de palabras hasta completar la regla en curso. Como esta selección es intrínseca al sistema, se podría utilizar a su vez para ocultar una información cifrada de forma que un analista no podría determinar si el texto generado de esa información aleatoria se debe al proceso natural del sistema (es plausible) o a otra información enmascarada (negación plausible). Luego siempre es posible ocultar una información que "pudiera ser detectada" y jugar con esa "ambigüedad" para ocultar otra pequeña información.

Adicionalmente a las características destacadas, es importante destacar que NICETEXT todavía produce estegotextos con defectos derivados de sustituciones no válidas en contexto y anomalías entre el estilo de escritura seleccionado y el vocabulario empleado. No obstante, pocas innovaciones se han dado en esta línea de investigación desde las ventajas conceptuales aportadas por NICETEXT, aunque es cierto que otras propuestas basadas en gramáticas libres de contexto se han publicado, como por ejemplo la herramienta TEXTO que transforma información a sentencias en inglés [125], las herramientas C2txt2c y Csteg [126] [127] que ocultan código fuente de lenguajes de programación en oraciones en lenguaje natural o el sistema Lunabel [128].

Sin duda, lo que sí ha avanzado conceptualmente en el siglo XXI son los procedimientos de estegoanálisis aplicables a este tipo de propuestas. Aunque es cierto que pocos algoritmos de detección de esteganografía lingüística se han publicado, un esfuerzo significativo en esta área ha sido realizado por la comunidad científica china. Especialmente ataques a ciegas (blind steganalysis) a tres diferentes propuestas de esteganografía lingüística: NICETEXT, TEXTO y basados en cadenas de Markov.

En 2008, Zhi-li et al. [129] utilizando las características estadísticas medidas de las palabras existentes en diccionario consiguieron entrenar un SVM para clasificar textos sin información oculta y estegotextos. La precisión de detección de segmentos de estegotextos y textos sin información oculta fue del 94,01% (basado en cadenas de Markov), 98,48% para NICETEXT y 97,96% para TEXTO cuando el tamaño del segmento es de 20kB.

El mismo año publicaron [130] un procedimiento de detección contra estos tres sistemas (NICETEXT, TEXTO y cadenas de Markov) basado en el ataque a la distribución de las palabras en un texto. La idea de este ataque consiste en medir las ocurrencias de las palabras y las localizaciones de las mismas en un texto. En textos en lenguaje natural ciertas palabras habitualmente tienen una distribución no equitativa. Es decir, se repiten frecuentemente en algunos lugares, pero rara vez en otros. Es posible caracterizar la distribución de las palabras y generar reglas que permitan clasificar textos normales y estegotextos. En concreto, el algoritmo propuesto permite una precisión total en la clasificación de segmentos de estegotextos y textos normales de 87,39% para tamaño de 5kB, 95,51% para 10kB, 98,50% para 20kB, 99,15% para 30kB y 99,57% para 40kB.

Ese mismo año, Zhi-li et al. [131] publicaron un algoritmo capaz de clasificar textos y estegotextos para los tres sistemas de ocultación indicados con una precisión mayor del 90% para tamaños de 4kB. En este caso, se utilizó un estimador basado en la entropía de las palabras y su varianza, construyendo un vector bidimensional para entrenar un SVM que se utilizó como clasificador.

Este mismo año, Meng et al. [132] publicaron un ataque demoledor contra el sistema NICETEXT. Su método alcanza unos resultados de clasificación que excede el 99% cuando el tamaño del texto/estegotexto es mayor de 400 octetos. Para fragmentos del tamaño de una oración (al menos 8 palabras, unos 40 octetos) la precisión es mayor del 85%.

Este ataque se basa en la posibilidad de crear un modelo estadístico (N-gram language model) que permite estimar las probabilidades de aparición de las palabras en función de las palabras que le preceden. Es decir, intentar estimar la probabilidad $P(w_n| w_1 ... w_{n-1})$. Una forma de realizar esto es mediante textos de entrenamiento.

$$P(w_1 \dots w_n) = \frac{C(w_1 \dots w_n)}{N}$$

$$P(w_n|w_1 \dots w_{n-1}) = \frac{C(w_1 \dots w_n)}{C(w_1 \dots w_{n-1})}$$

Donde $C(w_1...w_n)$ es la frecuencia de ese "bloque" de palabras en el texto de entrenamiento y N es el número total de "bloques" en ese texto de entrenamiento. Según esto, definen el concepto de *perplejidad* como (usan un modelo 3-gram):

$$P(W) = \sqrt[N]{\prod_{i=1}^{N} \frac{1}{P(w_i|w_i - 2, w_i - 1)}}$$

Si el valor de la perplejidad es pequeño los "bloques" serán más probables. Sus experimentos indican que si se crea un modelo de lenguaje de un texto normal y se calcula la perplejidad de textos normales y estegotextos los resultados serán muy similares, pero si creamos un modelo de lenguaje de estegotextos y lo usamos para calcular la perplejidad de textos normales y estegotextos, los resultados son muy diferentes. Tanto que pueden ser utilizados para diferenciar textos normales y estegotextos. En este caso concreto para los estegotextos producidos por NICETEXT.

Estas ideas se plasmarían en 2009, Meng et al. [133], en la mejora de un procedimiento de estegoanálisis a ciegas basado en un modelo estadístico N-gram del lenguaje para atacar a los sistemas de esteganografía lingüística NICETEXT, TEXTO y basados en cadenas de Markov. Sus resultados muestran precisiones de detección para fragmentos de 2K del 93,9% y del 96,3% para fragmentos de 5K.

3.3. Generación de estegotextos basada en modificación de textos existentes

En el pasado la información textual fue un portador muy socorrido para implementar procedimientos esteganográficos, en general sencillos y que ocultaban poca información, procedimientos basados habitualmente en la modificación del formato del texto o de la posición específica de unas letras en el mismo (null-ciphers y text-semagrams). En la actualidad, mucho de este conocimiento ha derivado en una línea de investigación más amplia intentando aunar los conocimientos en el procesamiento del lenguaje natural y la criptografía para alcanzar propuestas más robustas y que permitan ocultar un mayor volumen de datos.

Esta línea de investigación consiste en la posibilidad de ocultar información realizando modificaciones en un texto existente o un texto que se genera automáticamente para ser modificado. En general, el receptor no necesitará el texto original, al que se le han realizado las modificaciones, para recuperar la información oculta. En los siguientes apartados se verá cómo es posible, además, establecer procedimientos esteganográficos basados en que emisor y receptor posean el texto original al que se realizan las modificaciones, lo que da lugar al estegotexto. En general, esta idea no es tan interesante ya que supone una limitación más a considerar en el sistema esteganográfico. Debe tenerse en cuenta que, si el estegoanalista fuera capaz de conseguir el texto original el procedimiento de detección se simplificaría bastante, luego emisor y receptor debería salvaguardar o destruir la cubierta original.
Aunque los procedimientos clasificados en esta línea de ocultación pueden ser utilizados como procedimientos esteganográficos, su utilidad actual va más destinada al marcado digital de textos, posiblemente por su aplicación práctica. La aplicación práctica de estos principios facilitaría la inversión de dinero necesaria para avanzar en investigaciones serias de estos aspectos. Por este motivo, la ciencia del marcado digital de textos (en inglés, *Natural Language Watermarking* o NLW), está tomando un auge significativo en los últimos cinco años en lenguajes tan dispares como el inglés, el mandarín, árabe, etc.

A continuación, se realiza una clasificación, por procedimiento, de las ideas más significativas publicadas en las últimas dos décadas, así como los ataques estegoanalíticos publicados. Como se observará, el trabajo más significativo ha sido realizado para la lengua inglesa. Por este motivo se toma este lenguaje como referencia, añadiendo si se consideran relevantes propuestas en otros idiomas.

Como se podrá observar la evolución de todos estos procedimientos converge hacia una solución futura que combine modificaciones léxico-semántica con alteraciones sintácticas, así como es posible que dichas sustituciones pudieran llegar a tener una gran calidad si se consideran ontologías para describir “entornos textuales” concretos.

3.3.1 Modificaciones léxico-semánticas

Esta línea de investigación se centra en la posibilidad de utilizar el léxico presente en un texto con utilidad esteganográfica. Una gran mayoría de las propuestas actuales están destinadas a la sustitución de palabras, y más concretamente a la sustitución de palabras

por palabras parecidas, es decir, por sinónimos. Cualquier algoritmo moderno de sustitución de palabras por sus sinónimos puede verse básicamente como:

$$H(T, s, D, k) = T'$$
$$E(T', D, k) = s$$

Siendo T el texto a modificar, s la información a insertar, D el diccionario de sinónimos y k una clave secreta. H es la función que realiza la inserción de la información a ocultar y E la función que permite recuperarla.

Chapman y Davida en 1997 introdujeron por primera vez el método de sustituciones léxicas en su herramienta pública NICETEXT [122]. En esta idea se seleccionaban palabras del tipo semántico establecido por los elementos de cada una de las reglas PCFGs. Estas palabras eran sustituidas por otras similares dentro de un conjunto de sinónimos. Un ejemplo de esta sustitución en lenguaje inglés es el intercambio de big/large.

En 1999, Winstein [134], continuando con esta idea publicaría el sistema T-LEX (Tyrannosaurus-Lex). Un software que permitía realizar sustituciones léxicas en textos en inglés basadas en un diccionario de un conjunto de sinónimos construido con aproximadamente 20.000 palabras y haciendo uso de la base de datos Wordnet[5]. Los sinónimos en cada conjunto son indexados por orden alfabético y la selección del sinónimo a sustituir se realiza en función de una matriz de los candidatos existentes.

$$\texttt{San Jose is a} \left\{ \begin{array}{cc} & \textbf{excellent} \\ 0 & \textit{decent} \\ 1 & \textit{fine} \\ 2 & \textit{great} \\ 3 & \textit{wonderful} \end{array} \right\} \texttt{little} \left\{ \begin{array}{cc} & \textbf{city} \\ 0 & \textit{metropolis} \\ 1 & \textit{town} \end{array} \right\}.$$

Figura 8. Ejemplo de sustitución de sinónimos en el sistema T-LEX.

Por ejemplo, si se desea ocultar la información binaria $(101)_2 = 5$ representamos la matriz con las opciones disponibles y se observa que $0 \leq a_1 < 4$ y $0 \leq a_0 < 2$. Obteniendo $a_1=2$ y $a_0=1$. Por tanto, seleccionando los sinónimos, *great* y *town*.

$$\begin{pmatrix} a_1 & a_0 \\ 4 & 2 \end{pmatrix} = 2a_1 + a_0 = 5$$

Figura 9. Ejemplo de matriz en T-LEX para seleccionar dos sinónimos.

En 2000, Atallah et al. [135] propusieron la realización de sustituciones de sinónimos basándose en residuos cuadráticos. La idea es sencilla si consideramos m_i mod k como los bits del mensaje a insertar y w_i la palabra a ser considerada en el texto a modificar,

[5] La base de datos Wordnet [230] es una voluminosa base de datos léxica en inglés, desarrollada en la Universidad de Princeton, que agrupa nombres, verbos, adjetivos y adverbios en conjuntos de sinónimos (synsets). Estos conjuntos están relacionados mediante relaciones semánticas y conceptuales, estableciendo una estructura de gran utilidad para la lingüística computacional y el procesamiento del lenguaje natural.

cuyo valor ASCII es $A(w_i)$. Si $m_i \bmod k = 1$ y $A(w_i)+r_i \bmod k$ es un residuo cuadrático módulo p entonces w_i no se modifica, en caso contrario se selecciona un candidato. En esa fecha el valor de la clave p era un primo de 20 dígitos, k el número de bits del mensaje a insertar y $r_0, r_1,\ldots, r_{k-1}$ la secuencia de números pseudoaleatorios generados usando como semilla p. Este sistema no proporciona seguridad frente a ataques activos que sobrescriben la información. La evolución de sus trabajos se centraría en los años posteriores en sustituciones sintáctico-semánticas, como se verá en el siguiente apartado.

En 2002, Nakagawa et al. [136] propusieron sustituciones de sinónimos basadas en patrones, no exclusivamente una palabra por una palabra. Por ejemplo: can - be able to, copy – make a copy of, only – at most, do not – don't, etc.

En 2004, Bolskhakov [137], Calvo et al. [138] y Bolshakov et al. [139] profundizaron en la posibilidad de mejorar la aceptabilidad lingüística de las sustituciones léxicas basadas en sinónimos, es decir, de reducir los errores introducidos. Esto es así porque en realidad existen muy pocos sinónimos "puros" o absolutos en una lengua, sinónimos válidos en cualquier contexto de palabras, lo que implica que la modificación de una palabra inserta necesariamente un ruido visual. Para ello es necesario recopilar información de las co-ocurrencias y colocaciones de las palabras en una lengua concreta. Es decir, si se va a sustituir una palabra por otra lo más lógico es conocer con qué probabilidad aparece esa palabra respecto de otra que se considere como referencia (co-ocurrencias), así como considerar el concepto de colocación que restringe más la aparición de un determinado conjunto de palabras en determinadas zonas de un texto. En las tres propuestas [137][138] [139] se trabaja, respectivamente, con ejemplos en ruso, español e inglés, pero por desgracia esta idea atrayente no se desarrolla lo suficiente y no es posible inferir de los ejemplos mostrados la robustez real de esta propuesta. Además, se realiza una estimación muy somera de la capacidad de ocultación. Por ejemplo, en ruso el texto fuente debería tener un tamaño aproximado de 250 veces la información a ocultar. En lo que varían entre sí estas propuestas es en la forma de solucionar el problema de recopilar las co-ocurrencias y colocaciones para un lenguaje dado. En general, esto es una tarea compleja y suele realizarse analizando grandes volúmenes de texto para una lengua dada. Bolskhakov et al. en [139] propusieron una aproximación interesante a la recopilación de esta información estadística haciendo uso de buscadores en Internet como Google. Por ejemplo, si se desea saber qué adjetivo es más apropiado por su uso con un nombre, se podrían realizar peticiones recursivas entrecomilladas para observar en cuantas páginas web aparece esa estructura adj+nombre en concreto. El número de páginas sería un indicativo de cómo de buena sería esta estructura en una lengua determinada.

Collocation	In quot.	Portion	W/o quot.	Portion	MGV	Portion
colossal project	793	0.5%	123,000	0.5%	9,876	0.5%
gigantic project	2,670	1.7%	255,000	1.0%	26,093	1.3%
grandiose project	1,540	1.0%	83,200	0.3%	11,319	0.5%
great project	80,300	51.6%	9,710,000	38.9%	883,013	44.8%
huge project	34,400	22.1%	4,100,000	16.4%	375,552	19.0%
large-scale project	28,700	18.4%	2,660,000	10.7%	276,300	14.0%
tremendous project	1,620	1.0%	1,340,000	5.4%	46,591	2.3%
very large project	5,570	3.6%	6,690,000	26.8%	193,037	9.8%
Total:	155,593	100.0%	24,961,200	100.0%		

Figura 10. Ejemplo de desambiguador basado en consultas en Google

Un trabajo significativo en el estudio del impacto de las sustituciones fue publicado en 2006 por Topkara et al. [140]. En este trabajo se propone que los sistemas que realicen sustituciones de sinónimos deben cuantificar de la mejor manera posible la distorsión introducida [141]. Topkara et al. sugieren que este tipo de sustituciones deberían buscar la mayor ambigüedad posible, entendiendo por ambigüedad elegir los sinónimos del conjunto disponible que más significados tuvieran. Este hecho haría la tarea de desambiguación automática más compleja [142], ya que haría falta identificar si la palabra sustituida encaja o no en su contexto cercano de palabras. Además, las modificaciones deberían estar cercanas a un límite de distorsión cuantificable. Con estos criterios implementaron el sistema *Equimark*, considerando sólo las palabras con más de un sentido (homógrafos). Sólo los homógrafos dentro del conjunto de sinónimos son considerados como potenciales candidatos en la sustitución de sinónimos. En el proceso de decisión hacen uso del diccionario WordNet y de la librería WordNet::Similarity para cuantificar el "parecido" entre dos palabras (véase Figura 11).

Adicionalmente a medir el impacto de las sustituciones, otras investigaciones como la de Nanhe et al. en 2008 [143] han propuesto los criterios necesarios a seguir para maximizar la capacidad de ocultación basándose en el reconocimiento de un mayor número de palabras disponibles a sustituir. De esta forma se analiza el interés de considerar conjugaciones verbales y soporte de género y número para nombres. Por ejemplo, si se detecta un nombre en plural cuyo nombre en singular se encuentra en el diccionario de sinónimos, los sinónimos a elegir, que pertenecen a su conjunto, se convertirán a plural antes de realizar la inserción.

Aunque estas ideas son muy generalizables a diferentes lenguajes, los trabajos anteriores se han centrado especialmente en su aplicación a lengua inglesa. Otras propuestas en otros idiomas con conceptos similares han sido publicadas, por ejemplo, en chino [144] [145].

Otra propuesta más o menos curiosa puede ser la sustitución léxico-semántica basada en variantes dialectales de una misma palabra. Por ejemplo, en 2008, Shirali-Shahreza [146] publicó un curioso sistema que consistía en ocultar información en textos en inglés alternando palabras que se escriben de manera diferente en inglés americano e inglés británico: *Favorite-Favourite, Criticize-Criticise, Fulfill-Fulfil, Center-Centre, Dialog-Dialogue, Medieval-Mediaeval, Check-Cheque, Defense-Defence, Tire-Tyre*, etc. La propuesta aunque ingeniosa dista de ser una propuesta a ser considerada en serio.

No se han publicado estudios significativos del impacto de alternar este tipo de palabras en un texto en inglés.

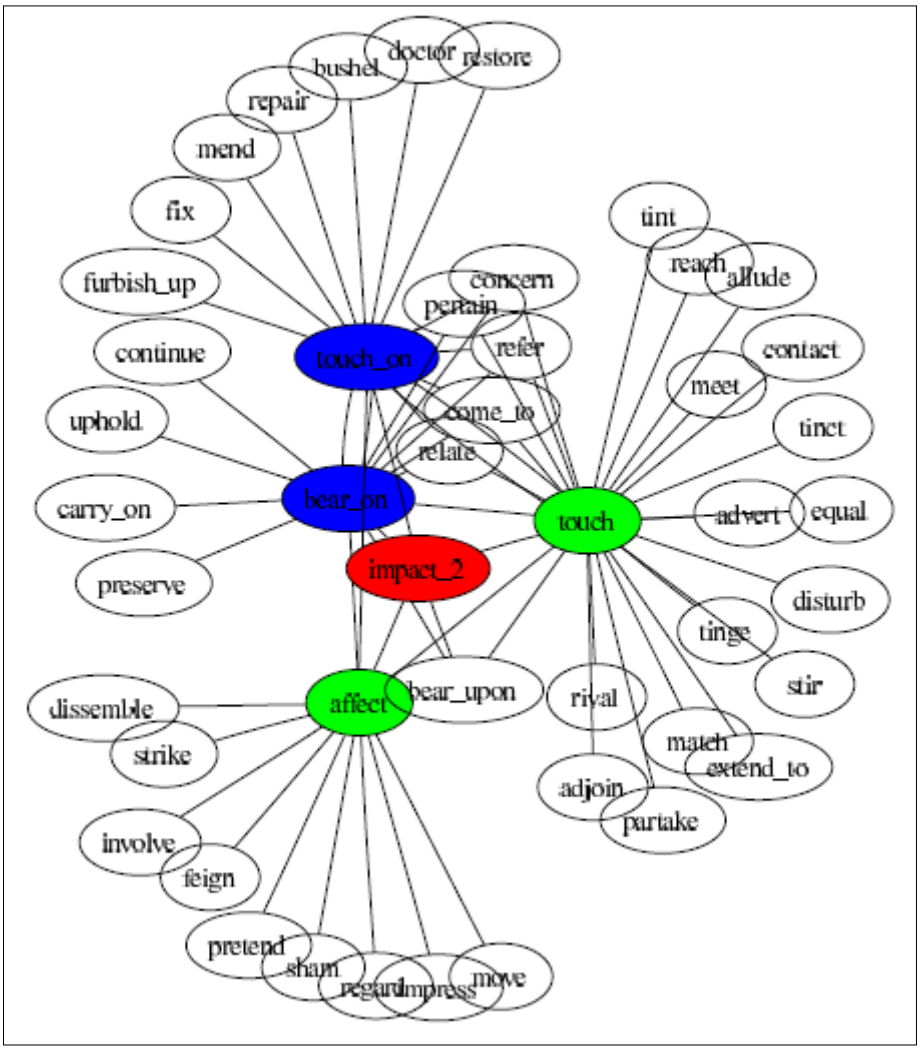

Figura 11. Ejemplo de palabras como múltiples sentidos

Otras propuestas léxicas podrían estar basadas en sistemas de codificación que se apoyan en el valor semántico de las palabras. En esta dirección se orienta, por ejemplo el trabajo de Niimi et al. en 2003 [147] en el cual se desarrolla un modelo para cuantificar el valor semántico de una información. Según este modelo se le asigna una puntuación a conceptos (palabras), otra a modificadores (adjetivos), conectores de conceptos (por ejemplo, conjunciones), a delimitadores (paréntesis y corchetes), etc. El proceso de ocultación reside en la comparación de la puntuación semántica de una información con un umbral. Si está por debajo ocultará un bit 0/1 y si no el opuesto 1/0. Algunas de las técnicas empleadas para incrementar o decrementar el valor semántico y así poder enmascarar información binaria son: remover modificadores, remover conectores (y algunos elementos que conecta), transformaciones sintácticas, etc.

El principal inconveniente de las sustituciones léxicas es la facilidad, en mayor o menor medida, con la que un atacante podría invertir/anular gran parte de las inserciones. A

este problemática se le une que en general los lenguajes no tienen un gran número sinónimos absolutos, válidos en cualquier contexto[6], e incluso podrían todavía tener diferencias semánticas y pragmáticas entre los miembros de un conjunto de sinónimos que provocarían distorsiones cuantificables. En general, solucionar esta última problemática requiere sofisticados procedimientos de desambiguación del sentido de las palabras lo cual está presente sólo para unos pocos lenguajes. Este motivo hizo que en 2004, Bergmair y Katzenbeisser [148] [149] propusieran un sistema HIP (*Human Interactive Proof*) basado en el hecho de que una máquina no podría desambiguar el sentido de las palabras fácilmente, mientras que los humanos podrían hacerlo con una precisión alta. La seguridad de esta propuesta lógicamente depende de la evolución de la tecnología en desambiguación del sentido de las palabras en un contexto. Con lo que la propuesta de Bergmair puede que hoy día no sea tan interesante.

En la práctica, todos estos criterios han sido considerados para construir propuestas reales de estegoanálisis lingüístico para detectar la información ocultada con sistemas que aplican sustituciones léxicas, especialmente de palabras por sus sinónimos.

En 2006, Xin-guang et al. [150] [151] adelantaron varios trabajos sobre las consideraciones que deberían tenerse al realizar sustituciones léxicas. En concreto, los autores realizaron un modelo estadístico basado en textos en inglés, destacaron que el análisis de la distribución de caracteres y de las primeras letras de cada palabra podría alertar la presencia de estegotextos.

Ese mismo año, Taskiran et al. [152] [153] trabajaron en una propuesta más concreta, profundizando en el hecho de que la caracterización estadística de un lenguaje mediante textos de entrenamiento permitiría atacar a propuestas de sustituciones basadas en sinónimos si no se consideraban criterios mínimos de impacto de la palabra a sustituir[7]. Esta idea se plasma en este artículo con la implementación de un ataque real contra el sistema T-LEX (en sus sustituciones no considera el contexto, los sinónimos son elegidos al azar). Utilizan la herramienta SRILM (*Stanford Research Institute Language Modeling*) para entrenar un modelo con fragmentos de texto con información oculta y sin información oculta. Estimadores extraídos de este modelo permitieron entrenar un SVM que reflejó una precisión de detección de oraciones modificadas del 84,9%.

En 2009, Zhenshan et al. [154] mejorarían el ataque de Taskiran [152] [153] con precisiones de detección del 90%. Este ataque mide la "aceptabilidad" de una palabra respecto de sus palabras vecinas. A continuación, se analiza este ataque ya que es la investigación de estegoanálisis más precisa publicada frente a sistemas esteganográficos que ocultan información mediante sustituciones de palabras por sinónimos.

[6] Existen contextos donde incluso palabras que no son sinónimas harían esa función. Por ejemplo, "the sleuth" es sinónimo de "Sherlock Holmes" en muchas de las obras de Arthur Conan Doyle, así como es un sinónimo de "Hercule Poirot" or "Miss Marple" en algunas novelas de Agatha Christie.

[7] Esta consideración implica determinar el sentido correcto de la palabra en su contexto, y esto como se ha indicado anteriormente es un problema complejo en el procesamiento del lenguaje natural (desambiguación).

Este ataque define la función:

$$\mathrm{ST}(w, C) = \ln \frac{N}{\mathrm{CF}(w)} * \mathrm{CF}(w, C)$$

Donde N es el número de documentos (textos) a considerar, $\mathrm{CF}(w)$ es la frecuencia con la que aparece esa palabra, $\ln \frac{N}{\mathrm{CF}(w)}$ es un indicativo de cómo de frecuente es la palabra W en un documento, $\mathrm{CF}(w,C)$ es la frecuencia con la que aparece una palabra W en un contexto de palabras determinado y $\mathrm{ST}(w,C)$ es una función de ponderación que evalúa la importancia de una palabra en los textos bajo estudio respecto de los posibles contextos en los que está presente. Se entiende como contexto un conjunto de 2n palabras respecto de la palabra a considerar. Por ejemplo, dos palabras delante y dos detrás. Por ejemplo: "synonym sets **do not** intersect **with each** other". Una vez calculado los valores $\mathrm{ST}(w,C)$ para cada palabra candidata a sustituir en un contexto determinado, se calcula una ponderación respecto de todas las palabras candidatas. Cuanto mayor sea esa ponderación, VP, más "aceptable" será la palabra.

$$\mathrm{VP}(w, C, S) = \frac{\mathrm{ST}(w, C)}{\sum_{w_i \in S} \mathrm{ST}(w_i, C)} \qquad \text{siendo S el conjunto de sinónimos de w}$$

El ataque consiste en calcular los valores VP de cada sinónimo candidato y a continuación calcular la media y varianza de todos los VPs calculados de todos los sinónimos candidatos a sustituir una palabra dada. Esta información definirá un vector bidimensional. Calculando todos los vectores bidimensionales de textos y estegotextos de partida se puede entrenar un SVM que facilitará la clasificación entre textos con información oculta y sin ella. Entre sus pruebas, Zhenshan et al. [154] usaron documentos de 10Kbits de obras literarias en inglés, generando 1080 documentos, 720 para entrenamiento y 360 para test, un tercio de cada grupo con información oculta mediante el sistema T-LEX (de 20 a 64 bits por documento). Su algoritmo clasificó textos y estegotextos T-LEX con una precisión del 90%. Si la ocultación es inferior a 44 bits la precisión ronda el 86,1% y si es mayor a 44 bits alcanza el 92,2% de precisión.

En resumen, esta técnica de ocultación podría ser interesante en su uso para una lengua concreta. Para ello, es necesario identificar o construir los recursos léxicos necesarios, cuantificar la capacidad de ocultación real de un sistema práctico y medir la invisibilidad de las sustituciones según los ataques publicados. Conocida toda esta información se podría iniciar el estudio de un sistema de sustitución basada en sinónimos cuyas modificaciones fueran resistentes a alteraciones maliciosas, ataques activos, y por lo tanto se pudieran construir sistemas reales de marcado digital de textos.

Estos estudios no están publicados, por ejemplo, para el sistema *Equimark* de Topkara et al. [140]; por lo que en su aplicación a lengua inglesa, se desconoce la capacidad de ocultación real de la propuesta y cómo responde a los ataques públicos de detección y alteración de la información insertada.

3.3.2 Modificaciones sintáctico-semánticas

En teoría, la manipulación sintáctica de una frase con fines esteganográficos se basa en el hecho que las frases son combinaciones de sintaxis y semántica, y la semántica de una frase podría ser expresada por más de una estructura sintáctica. Conocido esto es posible articular procedimientos que aprovechen esta situación con utilidad esteganográfica y de marcado digital de textos. La idea es poder modificar una frase sintácticamente sin que la semántica de la frase ni la coherencia global del texto se vea afectada. Si existe más de una posibilidad de expresar "lo mismo" puede elegirse entre las opciones disponibles, y la decisión de una u otra opción es lo que permitirá ocultar información. El esquema más documentado consiste en que el emisor envíe un texto modificado al receptor. Otro esquema posible, que tiene más restricciones, permitiría ocultar información mediante el conocimiento tanto por el emisor como por el receptor del texto origen sobre el que se va a realizar la modificación. Todos estos procedimientos se fundamentan principalmente en la posibilidad de mover estructuras o palabras dentro de una sentencia, eliminar/añadir palabras "semánticamente vacías" o procedimientos similares.

Habitualmente, la modificación de estructuras sintácticas requiere de procedimientos más sofisticados que las sustituciones léxicas. No obstante, actualmente la investigación en sistemas de etiquetado (*tagger*) y en procedimientos de desambiguación permite construir propuestas reales, aunque no sean perfectas. Su ventaja reside en mostrar una seguridad intrínseca frente a ataques léxicos, es decir, a procedimientos de ataque que únicamente sustituyan unas palabras por otras para intentar anular la información ocultada. Si la ocultación se basa en la estructura de los textos este tipo de ataque no tiene utilidad.

En general, el movimiento de palabras dentro de una estructura es detectable por el receptor sin conocimiento del texto original. Los procedimientos de ocultación basados en la elisión o inserción de palabras requerirán del conocimiento del texto original por parte del receptor para detectar la información oculta.

A continuación, se describen algunos de los trabajos más significativos, principalmente para lengua inglesa. Finalmente se añaden las referencias de otros trabajos de interés para otras lenguas.

En 2001, Murphy [155] realizó un amplio estudio, 165 páginas, de las posibilidades sintácticas de la lengua inglesa con utilidad esteganográfica. Este estudio sirve de modelo conceptual para estudiar este tipo de estructuras sintácticas con utilidad esteganográfica en otras lenguas. Algunas de las estructuras analizadas fueron:

a) Sustitución de *which/who/whom* por *that* dependiendo del contexto.

Esta sustitución consiste en ocultar una información binaria sin modificar el significado de una oración aprovechándose de la posibilidad de sustituir las palabras which/who/whom por that dependiendo del contexto.

(a) The person **that** looks like Mr. T is an embroidery teacher.
(b) The person **who** looks like Mr. T is an embroidery teacher.

b) Eliminar o insertar *which/who/whom/that* en determinadas situaciones.

Murphy estudió la posibilidad de insertar o eliminar estas palabras para ocultar un bit en cada sustitución. Existen diferentes características a ser tenidas en cuenta para que esta sustitución pueda ser "aceptable" lingüísticamente. Es recomendable la lectura en profundidad la siguiente investigación referenciada [155].

(a) The woman [who was afflicted with a fit of hiccups] is recovering in hospital now.
(b) The woman [~~who~~ afflicted with a fit of the hiccups] is recovering in hospital now.

c) Movimiento de complementos, frases preposicionales y adverbiales.

Distintos complementos podrían ser fácilmente reordenados en una oración sin afectar significativamente al significado final de la frase. Así, por ejemplo, en inglés es fácil observar ejemplos en complementos de tiempo, lugar, modo y contingencia.

(a) [In the morning]$_{\text{TIME}}$ I went to work - I went to work [In the morning]$_{\text{TIME,}}$
(b) Life was better [in the home country]$_{\text{PLACE}}$ - [In the home country]$_{\text{PLACE}}$ life was better
(c) I'll call him [if I can find my phone]$_{\text{CONTINGENCY}}$ - [If I can find my phone]$_{\text{CONTINGENCY}}$ I'll call him.

d) Inserción de It. Extraposición.

En ciertas situaciones [155] es posible sustituir un sujeto por It. El sujeto se mueve al final de la frase actuando como un complemento más.

(a) [That he leaves the top off the toothpaste]$_{\text{SUBJECT}}$ annoys me intensely
(b) It annoys me intensely [that he leaves the top off the toothpaste]

e) Inserción/Elisión de *There.*

(a) There$_{\text{SUBJECT}}$ is a horse$_{\text{SEMANTIC SUBJECT}}$ galloping across the field.
(b) A horse is galloping across the field

f) Reordenación de argumentos unidos por conjunción.

En inglés las conjunciones *and* y *or* pueden permitir una cierta libertad en el movimiento de los argumentos que unen.

(a) [Layabouts]$_{\text{NP}}$, [gurriers]$_{\text{NP}}$ and [good-for-nothings]$_{\text{NP}}$, the lot of them!
(b) [Gurriers]$_{\text{NP}}$, [good-for-nothings]$_{\text{NP}}$, and [layabouts]$_{\text{NP}}$, the lot of them!
(c) [Good-for-nothings]$_{\text{NP}}$, [layabouts]$_{\text{NP}}$, and [gurriers]$_{\text{NP}}$, the lot of them!

Para un análisis más detallado de las reglas sintácticas concretas detectadas y sus limitaciones véase su estudio en [155].

En 2001, Atallah et al. [156] trabajaron paralelamente en la posibilidad de modificaciones sintácticas como: el movimiento de complementos, la transformación activa-pasiva, la inserción de elementos semánticamente vacíos del estilo de “generally speaking”, “basically”, “it seems that”, etc.

En 2002, Atallah et al. [157] documentaron una propuesta que hace uso de árboles semánticos TMR (*text-meaning representation*). Las representaciones de las oraciones pueden ser generadas mediante ontologías y el insertado se realiza usando transformaciones centradas en el uso de desambiguadores del sentido de cada palabra (WSD) y transformaciones semánticas. La idea es construir un árbol que facilite transformaciones basadas en eventos y conceptos que describan el significado de un texto. Según esto, los autores formulan tres posibles transformaciones: *grafting* (cortar/copiar información de una oración y pegarla en otro lugar), *pruning* (eliminar información que es repetida) y *substitution* (reemplazar información con datos equivalentes).

En 2005, Topkara et al. [158] publicaron un buen resumen de las tendencias en marcado digital de textos: transformaciones sintácticas, transformaciones léxicas, transformaciones semánticas, recursos léxicos, etc.

En 2006, Topkara et al. [159] profundizaron en los retos a resolver en una implementación real de un sistema de marcado digital de textos en lengua inglesa. Una implementación real debería tener en cuenta factores como el significado, la fluidez, la gramática y el estilo de un texto. En [159] los autores analizaron dos sistemas de marcado, Figura 12 y Figura 13, que aplican las transformaciones sintácticas descritas con anterioridad [155].

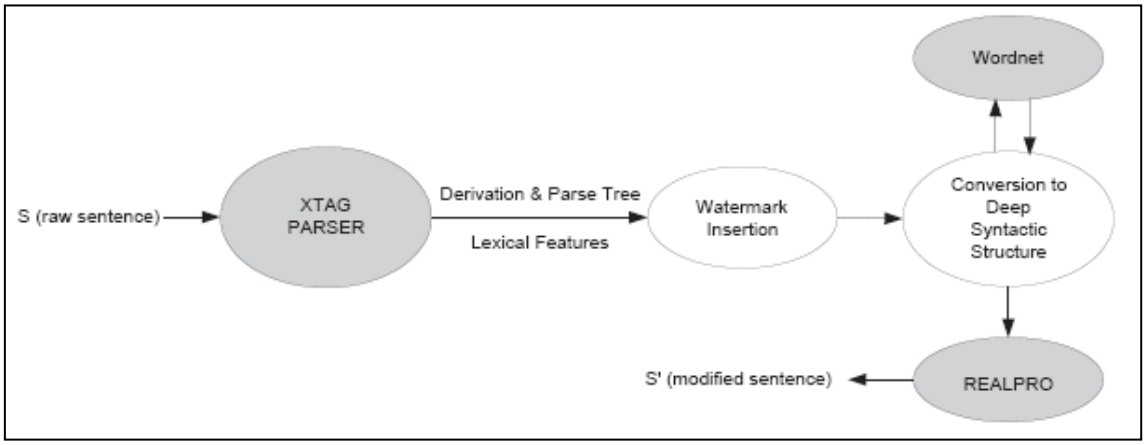

Figura 12. Sistema I. Uso del parser XTAG, del generador de lenguaje RealPro y del diccionario Wordnet

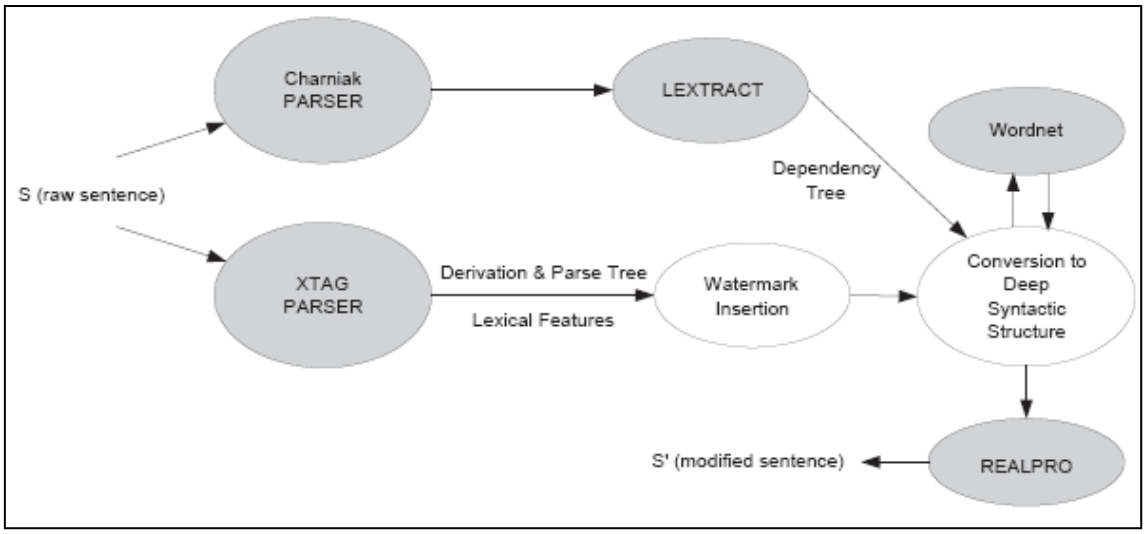

Figura 13. Sistema II. Uso de LEXTRACT para estructurar las oraciones

En este artículo se realiza una evaluación de la calidad de dichas transformaciones utilizando la métrica BLEU (*BiLingual Evaluation Understudy*) y la métrica NIST[8]. En ambos sistemas se convierten las oraciones en el formato adecuado para procesarlas automáticamente y poder insertar la marca de agua deseada. Para ello se utilizan etiquetadores de palabras (*XTAG* y *Charniak*) y se estructura la información resultante, mediante un formato *DSyntS* (*Deep Syntactic Structure*), para facilitar la creación, mediante el software *RealPro*, de las oraciones modificadas esteganográficamente. El segundo sistema, Figura 13, es una versión un poco más compleja que el reflejado en la Figura 12. Los autores con este segundo sistema intentan comprobar que una combinación adecuada de diferentes etiquetadores y el uso de varios formatos para estructurar la información lingüística extraída de las oraciones a modificar permitirían realizar mejores transformaciones sintácticas. Lo cierto es, según las métricas empleadas, que el primer sistema parece generar sentencias con un menor impacto lingüístico. Es decir, se parecen más a las oraciones originales. Los autores dejan para un futuro posibles mejoras y el uso de nuevas combinaciones de herramientas de procesado del lenguaje natural para obtener mejores resultados.

En 2006, Topkara et al. [160] propusieron una implementación práctica que hacía uso de su sistema de sustitución de sinónimos *Equimark* [140] y de transformaciones sintácticas (activa y pasiva, movimiento de complementos, etc.). Para ello se analizaron oraciones del corpus Reuters y fueron utilizados los etiquetadores *X-TAG* y *Charniak* y las herramientas de generación de lenguaje *DsynsS* y *RealPro*. El objetivo final fue perseguir una propuesta más robusta frente a manipulaciones y a transformaciones indebidas. Por ejemplo, las transformaciones sintácticas, al menos en inglés, afectan al estilo del texto y esto dependiendo de la naturaleza del mismo debería ser cuidado, especialmente si el objetivo buscado es el *Natural Language Watermarking*.

En 2007, Murphy et al. [161] implementaron un sistema de esteganografía lingüística basada en el intercambio de complementos y pronombres relativos. Un ejemplo de esto fue el uso de las clausulas relativas, restrictivas y no restrictivas, con utilidad esteganográfica. Este tema fue estudiado anteriormente por Murphy en [155]

[8] Los autores utilizaron para calcular sus medidas el software MT Evaluation ToolKit del NIST.

anteriormente. Las clausulas restrictivas son sentencias que modifican un sintagma nominal para facilitar la comprensión del lector. Contrariamente, las clausulas no restrictivas añaden información adicional que no es vital para la comprensión general del discurso, habitualmente esta información va introducida en el texto entre comas.

(1) Clausula restrictiva

> For people [that insist on jumping in now to buy the funds]$_{rest}$, Newgate's Mr. Foot says: "The only advice I have for these folks is that those [who come to the party late] rest had better be ready to leave quickly. (0034:806).

(2) Clausula no restrictiva

> Rival Boston Herald columnist Howie Carr, [who usually rails at Statehouse "hacks" and nepotism]$_{non-rest}$, argued that the new drawings were designed to hide Mr. Madden's "rapidly growing forehead" and the facial defects of "chinless" Dan Shaughnessy, a Globe sports columnist. (2010:375)

En el caso de las clausulas restrictivas, las palabras que unen el sintagma nominal a la cláusula son típicamente *that* y *who/which*. En determinadas situaciones es posible intercambiarlas, insertarlas e incluso suprimirlas. A continuación, se observa algunos ejemplos. En algunos de ellos está presente un asterisco que significa "transformación incorrecta o dudosa".

(a) The theory [that you refer to] is discredited.
(b) The theory [which you refer to] is discredited.
(c) The theory [~~that~~ you refer to] is discredited.
(d) John, [who you met yesterday], can't come.
(e) *John, [that you met yesterday], can't come.
(f) *John, [~~who~~ you met yesterday], can't come.

Las clausulas restrictivas son muy comunes en inglés y pueden ser fácilmente reconocidas por etiquetadores [161]. En los casos donde es necesario hacer una distinción semántica entre nombres "humanos" y "no-humanos", para determinar por ejemplo si es posible o no sustituir *who* por *that*, Murphy et al. [161] hacen uso de la WordNet2.0, un diccionario electrónico creado por la universidad de Princeton el cual tiene una representación jerárquica, a modo de ontología, de sentidos de cada palabra.

El algoritmo fue programado en *Perl* y el corpus *Penn Treebank II* se utilizó como entrada. Este corpus, colección de textos, fue publicado por la Universidad de Pennsylvania recopilando artículos seleccionados del Wall Street Journal, con un total de 49.000 frases en inglés americano (alrededor de 1 millón de palabras) que fueron automáticamente etiquetadas por "partes del habla" (*Part of Speech*) organizadas en arboles sintácticos, posteriormente verificadas a mano. Su robustez, a diferencia de otras propuestas, que fue testeada con humanos, genera un 96% de oraciones "aceptables" según los autores, con un ancho de banda esteganográfico de 0.3 bits por frase.

En 2007, Murphy et al. en [162] analizaron tres técnicas de marcado digital de textos (*lexical substitution, adjective conjunction swaps, y relativiser switching*) extrayendo

oraciones del British National corpus y analizando su "bondad lingüística" con personas. Sus conclusiones pretenden formular similitudes entre la opinión de humanos que juzgan la aceptabilidad lingüística de un texto (estructura interna del texto, estructura externa del texto, significado de las palabras y coherencia global) y su equivalencia con estimadores estadísticos que se puedan recopilar automáticamente.

En 2007, Wu y Stinson [163] propusieron, considerando las propuestas previas, un nuevo esquema para marcado digital de un documento basado en natural language watermarking. En este caso, utilizaron una representación del significado de cada frase (TMR – Text meaning representation) para generar un ranking y su representación literal para insertar un bit de la marca de agua, así como la distancia de edición (número mínimo de operaciones requeridas para transformar una cadena de caracteres en otra) para analizar la "tolerancia" de la marca introducida.

Las modificaciones sintácticas con utilidad esteganográfica y de marcado digital han sido aplicadas en diversos idiomas: en turco [164] [165] [166], en japonés [167], en coreano [168], en chino [169] [170], entre otros.

3.3.3 Modificaciones basadas en el ruido de traducciones automáticas

La idea de estos procedimientos consiste en ocultar información basándose en la posibilidad de traducir una sentencia, de un lenguaje concreto, en varias sentencias "equivalentes" en un lenguaje destino, entre las cuales se puede elegir estableciendo un sistema binario de ocultación de información.

Esta curiosa idea fue adelantada en 2005 por Grothoff et al. [171]. En este artículo se analiza la posibilidad de ocultar información en el "ruido" creado en las traducciones automáticas de documentos en lenguaje natural. La traducción de fragmentos de texto de un lenguaje a otro crea suficientes alternativas para considerarlas seriamente en un proceso de ocultación. Los errores/imprecisiones introducidos en las traducciones podrían ser utilizados. Es decir, la traducción automática es adecuada para aplicaciones esteganográficas. Los autores analizaron diferentes tipos de errores generados por varios sistemas de traducción automática e incluso algunos de estos errores son razonables en traducciones por humanos. Estas limitaciones fueron explotadas en un sistema de ocultación práctico publicado en *http://www.scs.stanford.edu/~stutsman/stego* (web disponible a 2 de septiembre de 2010). Algunos de los errores considerados, en terminología inglesa, son: *functional words, blatant word choice errors, translations between typologically dissimilar languages, etc.*

Un ejemplo de error sin destruir el significado de las oraciones a traducir consiste en la traducción incorrecta de palabras ("functional words") como artículos, pronombres y preposiciones. Por ejemplo, muchos lenguajes no usan artículos delante de todos los nombres. Así por ejemplo, la traducción del francés al inglés de "*La vie est paralysée*" se traduce como "*Life is paralyzed*". La máquina de traducción cometería un error si produjera "*the life is paralyzed*" dado que el sentido de "life" en general no tiene artículo en inglés, lo mismo que nombres comunes como *water* o *money*. Errores parecidos suceden con la traducción de preposiciones que depende fuertemente del contexto de la oración. Por ejemplo, la frase en francés "*J'habite à 100 mètres de lui*" significa "*I live 100 meters from him*" en inglés, pero traducciones erróneas podrían

traducirla como "*I live with 100 meters of him*" o "*I live in 100 meters of him*", en ambos casos la traducción de *à* como *with/in* son inapropiadas en el contexto. Otros errores más sofisticados podrían hacer uso de las diferencias estructurales (sintácticas, semánticas y morfológicas) entre idiomas tan distintos como el chino y el inglés, el inglés y el árabe, etc.

Para tener una referencia más actual se ha procedido a modo de ejemplo, a traducir los supuestos anteriores con un servicio de traducción automática moderno como el proporcionado por Google (translate Google). Los resultados obtenidos permiten observar como los avances en sistemas de traducción simultánea podrían dificultar la invisibilidad de este tipo de técnicas esteganográficas al cometer cada vez menos errores de traducción.

(a_1) La vie est paralysée → Life is paralyzed
(a_2) the life is paralyzed → La vie est paralysée

(b_1) J'habite à 100 mètres de lui → I live 100 yards away
(b_2) I live 100 meters from him → Je vis à 100 mètres de lui
(b_3) I live with 100 meters of him → Je vis avec 100 mètres de lui
(b_4) I live in 100 meters of him → J'habite à 100 mètres de lui

Como puede deducirse un ataque a un sistema esteganográfico de este tipo depende claramente de cómo evolucione la caracterización de un lenguaje determinado. Este mismo conocimiento y sus limitaciones podrían ser explotados nuevamente por un sistema de este tipo. Por tanto, la seguridad de este sistema recae en la clásica carrera entre el ratón y el gato (protector y atacante). Los autores justifican que dado que generar un modelo de análisis por parte de un atacante no es ni mucho menos trivial y es sencillo adaptar el sistema para eliminar posibles excepciones que faciliten la tarea al analista, este tipo de sistemas, por tanto, establece un "nivel razonable" de protección.

En 2006, Stutsman et al. [172] publicaron una mejora sustancial del trabajo anterior [171] avanzando en esta línea aparentemente prometedora. El principal problema de [171] consistía en que el texto a traducir y la traducción debían ser enviadas al receptor. El receptor tenía que realizar el mismo proceso de traducción para recuperar el mensaje oculto. Por lo que el procedimiento de Grothoff facilitaba teóricamente el trabajo a un potencial estegoanalista. La nueva propuesta [172] permite mantener el texto a traducir en secreto. El receptor únicamente necesita una clave compartida con el emisor para recuperar la información oculta. Ni siquiera necesita tener acceso a la máquina de traducción utilizada por el emisor. Adicionalmente, el esquema permite al emisor mezclar traducciones humanas y automáticas, lo cual podría dificultar la precisión del adversario a la hora de detectar traducciones automáticas y analizar la presencia de información ocultada.

3.3.4 Modificaciones basadas en formato

En apartados anteriores se describieron muchos de los procedimientos tradicionales de esteganografía textual en los siglos pasados. Uno de esos procedimientos consistía en la posibilidad de utilizar la estructura (formato y la posición de las palabras, frases o elementos en un documento) con fines esteganográficos. Sus ventajas residen en un

ancho de banda esteganográfico grande y en la imperceptibilidad visual (depende del método). Desde finales del siglo XX hasta nuestros días, gracias al auge de los contenidos digitales, se han documentado diferentes procedimientos esteganográficos aplicados a todo tipo de documentos que contienen información textual, típicamente documentos ofimáticos creados con *Microsoft Word*, *OpenOffice*, *Latex*, etc [173] [174]. Este empuje ha ido de la mano de todo tipo de propuestas basadas en estas ideas para facilitar sistemas de marcado digital de texto para verificación de autor o contenido. A continuación, se destacan algunos de los artículos más significativos en esta área en las últimas décadas.

Desde un punto de vista académico el interés actual por este tipo de propuestas puede datarse en los primeros años de la década de los 90 del siglo XX, aunque es cierto que algunas de las ideas surgieron anteriormente. Por ejemplo, se ha documentado cómo en la década de los 80 Margaret Thatcher mandó modificar los procesadores de texto, utilizados por sus colaboradores, para ocultar en el espaciado de las palabras un identificador del autor de cada documento, ya que se habían producido fugas de información a la prensa [11].

En cualquier caso, un buen trabajo que sintetiza estas ideas, fue publicado en 1994, donde Brassil et al. [175] [176] proponen tres métodos de ocultación con utilidad en marcado de textos: line-shift coding, word-shift coding y character coding, en terminología inglesa. Durante toda esa década otros autores teorizarían sobre la posibilidad real de utilizar estos métodos en el marcado de textos [177][178] [179] [180][181] [182] [183].

a) **Line-shift coding.** Desplazamiento vertical, de tamaño fijo o variable, de elementos de un texto. Típicamente desplazamiento entre líneas, entre grupo de caracteres, etc.

b) **Word-Shift coding.** Desplazamiento horizontal, de tamaño fijo o variable, de elementos de un texto. Típicamente desplazamiento entre caracteres o entre palabras.

c) **Character coding.** Procedimientos de inserción de información basados en modificaciones de la tipografía de los caracteres y de los atributos asociados a ellos, por ejemplo, brillo, color, etc.

Hoy día, en el primera década del siglo XXI, la tendencia es hacer más robustas esas ideas iniciales, aunque las pocas ideas medianamente novedosas son adaptaciones de esos principios a nuevos formatos digitales que contienen información textual [184] [185] [186] [187] [188] [189] [190] [191] [192] [193]. No obstante, se ha publicado alguna idea curiosa como, por ejemplo, la creación de mensajes ocultos mediante ASCII Art. Un ejemplo de ello es la aplicación online que puede verse en *http://pictureworthsthousandwords.appspot.com* (web disponible a 2 de septiembre de 2010). Estas herramientas permiten construir una imagen mediante caracteres ASCII. Dado que es posible combinarlos de diferentes maneras es posible ocultar información en un texto ASCII que represente una imagen, véase por ejemplo la Figura 14.

En la primera década del siglo XXI diferentes investigaciones han mostrado interés en utilizar sistemas de escritura sofisticados como el sistema tipográfico TEX para generar estegotextos con modificaciones basadas en formato [194][195] dado su versatilidad y

su capacidad de ocultación [196]. Por ejemplo, en 2006 Chao et al. [197] utilizaron el sistema TEX para ocultar información en ligeras modificaciones del interespaciado entre las palabras, siendo el resultado del estegotexto un fichero pdf. Muchas otras propuestas se han publicado para diferentes idiomas basadas en los tres métodos de ocultación citados anteriormente: en árabe-persa [198][199][200] [201] [202] [203] [204] [205] [206] [207] [208] [209], en bengalí [210], en thai [211], en hindi [212] [213], en chino [214] [215] [216][217], entre otros.

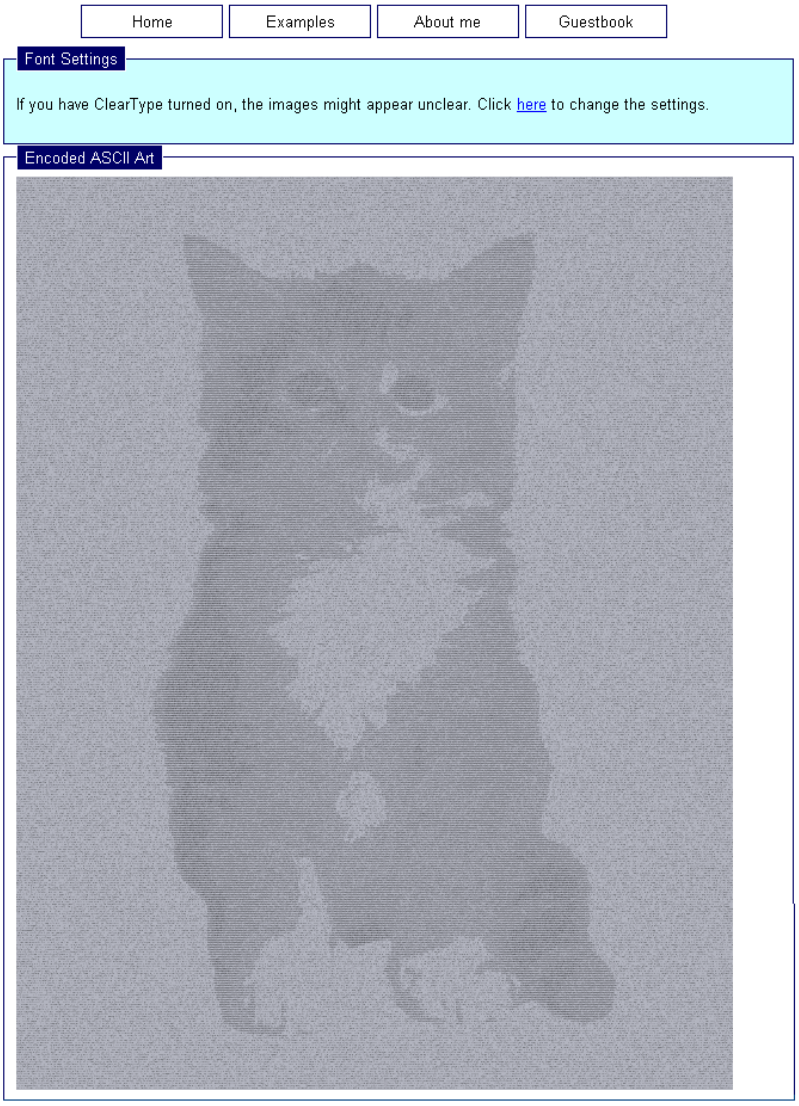

Figura 14. Mensaje ocultado en una imagen en ASCII Chart. Mensaje: “Esto es un mensaje oculto”

Sin duda, el avance conceptual más significativo en el siglo XXI ha consistido en la publicación de ataques lingüísticos a estas propuestas, siendo especialmente significativas las publicaciones de la comunidad científica china [218] [219].

En 2007, Lingjun et al. [220] publicaron un algoritmo para detectar variaciones en los atributos del formato de un texto que podrían tener uso esteganográfico. Su algoritmo mide las diferencias de atributos entre caracteres adyacentes y con esa información entrena un SVM (Support Vector Machine) que le permite clasificar textos innocuos y

estegotextos. La precisión de su algoritmo, bajo las condiciones establecidas, es de un 99,3% cuando el tamaño ocultado es de al menos 16 bits.

En 2008, Lingjun et al. [221] presentaron un ataque estegoanalítico frente a esteganografía textual en documentos pdf basados en introducción de espacios variables entre palabras. Si, según las condiciones establecidas, se utiliza más de un 5% de la capacidad de ocultación el porcentaje de clasificación es de un 98% de éxito. Otra propuesta de ataque frente a propuestas de ocultación de desplazamiento horizontal (*word-shift steganography*) en pdf puede verse en [222].

3.3.5 Modificaciones basadas en errores, abreviaturas y símbolos de puntuación

La presencia de errores ortográficos o tipográficos en los textos presentes en un canal de comunicación permitiría, teóricamente, su uso con fines esteganográficos. La utilidad real de un procedimiento esteganográfico de estas características depende muy mucho del canal donde se transmita y qué habilidades se le consideren a un atacante. Por ejemplo, un lector humano delataría rápidamente la presencia de muchas de esas faltas, y si su presencia es elevada podría incluso hacer sospechar de la naturaleza del texto analizado.

Aunque en la práctica no es sencillo articular una propuesta pública, no basada en oscuridad, considerando estos principios para un volumen de ocultación medio, en 2007 Topkara et al. [223] articularon una aproximación interesante y razonablemente seria[9]. Si el atacante fuera un sistema clasificador automatizado, suposición realista dado el volumen de información que se intercambia en las redes de telecomunicación, la pregunta clave a resolver es ¿cómo sabe un programa automático que existe una falta de ortografía en un texto? La respuesta a esta pregunta permite clasificar tres tipos diferentes de sistemas de ocultación:

a) **Sistemas que usan procedimientos para producir palabras que no existen en un diccionario.** El ataque a estas propuestas se simplifica utilizando diccionarios grandes y modelos estadísticos de la lengua bajo estudio que indiquen como se relacionan las palabras entre sí.

b) **Sistemas basados en errores tipográficos, uso de acrónimos y abreviaturas.** La detección de estos procedimientos queda supedita a algoritmos similares a los utilizados en la corrección de textos, por ejemplo, en los programas ofimáticos. Algunas de las técnicas que se emplean en su detección pueden estar basadas en la mínima distancia de edición (mínima diferencia en letras entre una palabra con errores y una palabra válida en un diccionario), modelos estadísticos N-gram (estudio de la probabilidad de aparición de esa palabra respecto de sus vecinas), etc. En general, estos procedimientos de ocultación, sustituciones léxicas, podrían ser procedimientos adecuados en combinación con otros, ya que resulta complejo definir una propuesta robusta pública con estas ideas de forma individual. Estos procedimientos podrían tener mayor

[9] No se conoce ninguna otra publicación científica “seria” de esta temática.

aplicación en entornos muy determinados como esteganografía en sms [224], codificación de información en emoticonos [225], etc.

Acronym	Translation	Explanation
218	Too late	The time is too late, missed opportunity
ASAP	As Soon As Possible	Immediately
C	See	Do you understand? OR the verb 'to see'
CM	Call Me	Asking someone to telephone
F2F	Face to face	In person
NC	No Comment	I can't say what I think
R	are	The verb 'to be'
SRY	Sorry	An apology
T+	Think positive	You need to be positive about a situation
ZZZZ	Sleeping	I'm tired, bored or annoyed

Tabla 1. Lista de acrónimos de palabras en inglés utilizadas en mensajes sms

c) Sistemas que usan procedimientos para transformar una palabra válida en otra palabra válida. Por ejemplo, vaca-baca, toro-loro, etc. Dentro de este tipo de sistemas también se pueden considerar otros procedimientos basados en la separación de palabras compuestas (saca puntas-sacapuntas) y en la creación de errores gramaticales. La detección de estos procedimientos requiere de técnicas avanzadas de reconocimiento lingüístico, etiquetadores precisos, técnicas de desambiguación y comprensión semántica. Conceptualmente la propuesta de Topkara et al. [223] se acerca más a esta opción. Según ellos, la robustez de la inserción de información en *typos* (faltas de ortografía) puede construirse en base a transformaciones computacionalmente asimétricas, es decir, transformaciones simples para ocultar, pero difíciles de detectar sin intervención de lectores humanos. Basándose en esta idea se desarrolló el sistema *MarkErr* para lengua inglesa orientado principalmente al marcado de textos. No obstante, este trabajo no aporta la suficiente información para inferir su utilidad real, cuál es la capacidad de ocultación y cuál es el uso más recomendado en unos canales u otros. No fue posible acceder al software *MarkErr* para evaluarlo.

A septiembre de 2010, no se conocen más publicaciones interesantes de estudio para el caso de procedimientos esteganográficos que hagan uso de la inserción de errores ortográficos o la inserción de abreviaturas. Aunque este tipo de técnicas suelen ser citadas como posibles no se conoce ninguna propuesta real que las utilice y en la que se analice estadísticamente y mediante clasificadores su robustez e invisibilidad.

En último lugar, existe otro tipo de procedimiento esteganográfico que estaría basado en la posibilidad de alterar símbolos de puntuación para ocultar información. Al igual que sucedía en los dos procedimientos anteriores no se conocen propuestas serias basadas en estos principios. En 2006, Meral et al. [165] realizaron una serie de consideraciones a este respecto en turco. Estas afirmaciones no dejan de ser anecdóticas, poco justificadas y difícilmente extrapolables a otros idiomas.

En conclusión, esta es una rama de investigación que podría ser interesante exclusivamente en canales muy concretos, como pudieran ser las redes sociales, si se demuestra la presencia masiva de faltas de ortografía. Quedan por determinar cuestiones prácticas como la capacidad de ocultación y la invisibilidad de este procedimiento para

evaluar si es interesante considerarla para el desarrollo de una propuesta esteganográfica útil.

ANEXO. Definiciones con utilidad en esteganografía lingüística

Este apartado pretende recopilar una serie de definiciones y principios útiles en el campo de la esteganografía lingüística que podría facilitar el trabajo a futuros investigadores en esta temática no relacionados directamente con la lingüística computacional.

a) Corpus

Un corpus lingüístico es un conjunto, normalmente muy amplio, de ejemplos reales de uso de una lengua. Estos ejemplos pueden ser textos, típicamente, o muestras orales, normalmente transcritas. Se llama *lingüística de corpus* a la subdisciplina de la lingüística que estudia la lengua a través de estas muestras.

b) Contexto

La Real Academia de la Lengua Española define un contexto lingüístico como aquel entorno lingüístico del cual depende el sentido y el valor de una palabra, frase o fragmento considerados. Este concepto afecta directamente a las técnicas esteganográficas que realizan modificaciones en un texto, ya que estas alteraciones podrían alterar su significado. Cómo definir el impacto de una sustitución esteganográfica y cuantificar las palabras que definen el contexto asociado a otra palabra a modificar no es sencillo.

c) Desambiguación lingüística (*Word sense disambiguation*).

En lingüística computacional, la desambiguación del significado de las palabras es un problema abierto en el campo del procesamiento de lenguaje natural, que incluye el proceso de identificar qué significado concreto tiene una palabra en una oración cuando la palabra tiene polisemia, es decir, pluralidad de significados. Como en todo procesamiento del lenguaje natural, existen dos enfoques principales para la desambiguación del significado de la palabra: enfoque profundo y enfoque superficial. El enfoque superficial no pretende entender el texto (enfoque profundo), sólo considera las palabras circundantes para establecer uno de los sentidos posibles. Estas reglas se pueden obtener automáticamente por computadora, utilizando un corpus de formación de palabras con el sentido de las palabras. Este enfoque, si bien no es, en teoría, tan poderoso como los enfoques profundos, da mejores resultados en la práctica.

d) Productividad esteganográfica

Se dice que un procedimiento es productivo esteganográficamente cuando permite ocultar o insertar una información de un tamaño específico en un texto con unas dimensiones determinadas transmitido en un canal concreto.

e) Co-ocurrencia de palabras

Hace referencia a la relación estadística entre palabras, patrones lingüísticos, etc. La ley de Zipf, formulada por el lingüísta Harvard George Kingsley Zipf [226], matiza esta definición afirmando que un pequeño número de palabras son utilizadas con mucha

frecuencia en una lengua, mientras que frecuentemente ocurre que un gran número de palabras son poco empleadas, lo que condicionará la aparición de patrones.

f) Colocaciones de palabras

Conjunto de dos o más palabras consecutivas que tienen característica de unidad sintáctica y semántica, y cuyo significado real no puede derivarse directamente del significado de cada palabra por separado. Por ejemplo, cierre hermético, negar categóricamente, dinero negro, etc. En español, los modelos de colocación de palabras más frecuentes son: Sustantivo + preposición + sustantivo, sustantivo + adjetivo, verbo + (artículo) + sustantivo, verbo + preposición + sustantivo, sustantivo + sustantivo, adjetivo + sustantivo.

g) Coherencia de un texto

La coherencia es una propiedad de los textos bien formados que permite concebirlos como entidades unitarias, de manera que las diversas ideas secundarias aportan información relevante para llegar a la idea principal, o tema, de forma que el lector pueda encontrar el significado global del texto. Así, del mismo modo que los diversos capítulos de un libro, que vistos por separado tienen significados unitarios, se relacionan entre sí, también las diversas secciones o párrafos se interrelacionan para formar capítulos, y las oraciones y frases para formar párrafos. La coherencia está estrechamente relacionada con la cohesión; con la diferencia de que la coherencia es un procedimiento macrotextual y la cohesión es un procedimiento microtextual.

h) Cohesión de un texto

La cohesión es la propiedad que tiene un texto cuando su desarrollo no presenta repeticiones innecesarias y no resulta confuso para el receptor. La cohesión es una característica de todo texto bien formado, consistente en que las diferentes frases están conectadas entre sí mediante diversos procedimientos lingüísticos que permiten que cada frase sea interpretada en relación con las demás. Al redactar un texto resulta inevitable el repetir determinadas ideas o conceptos que son esenciales para el tema que se está tratando. Con el objeto de producir un texto lingüísticamente atractivo, el emisor suele utilizar determinados procedimientos para conseguir que esas repeticiones no sean literales o innecesarias: manteniendo el mismo contenido, con esos mecanismos puede introducir una cierta variación estilística y formal dentro del texto. Por lo demás, el problema que se puede presentar es que si eso no se hace con cierta precisión es probable que surjan dificultades para la comprensión del texto, pues puede ocurrir que haya expresiones o palabras que sea difícil o imposible relacionar con algo ya dicho o que se vaya a decir. La cohesión pertenece al ámbito de estudios del análisis del discurso y la lingüística del texto.

i) Lingüística computacional

La lingüística computacional es un campo multidisciplinar de la lingüística y la informática que utiliza la informática para estudiar y tratar el lenguaje humano. Para lograrlo, intenta modelar de forma lógica el lenguaje natural desde un punto de vista computacional. Dicho modelado no se centra en ninguna de las áreas de la lingüística en particular, sino que es un campo interdisciplinar, en el que participan lingüistas, informáticos especializados en inteligencia artificial, psicólogos cognoscitivos y expertos en lógica, entre otros.

j) Etiquetador

Es aquel software que permite etiquetar elementos, típicamente palabras, en un texto en lenguaje natural para su posterior procesamiento. Son comunes los etiquetadores que asignan etiquetas con las categorías lingüística (nombre, verbo, adjetivo, adverbio, preposición, conjunción, etc.) a la que pertenece una palabra en un texto dado.

k) Aceptabilidad lingüística – impacto lingüístico

Por aceptabilidad lingüística entendemos la validez de un estegotexto desde el punto de vista de un lector humano. Esta opinión es subjetiva, ya que depende de quién sea el lector. Por ejemplo, un texto escrito por un humano podría tener un estilo y un léxico no adecuado para un revisor, que incluso podría dudar de la naturaleza de ese texto. Si el revisor es condicionado para revisar textos originales y textos modificados por procedimientos automáticos los falsos positivos harían su criterio cuanto menos subjetivo, dado que no todas las personas producen textos con la misma calidad lingüística. Un resultado práctico sería aquel en el que un lector humano tuviera dudas de la naturaleza de un estegotexto. Si un humano tiene dudas una máquina tendrá el trabajo francamente difícil.

4. ESTEGANOGRAFÍA LINGÜÍSTICA EN LA ACTUALIDAD.

No hay ningún viento favorable para el
que no sabe a qué puerto se dirige
Arthur Schopenhauer

La documentación que acaba de leer fue generada hace 10 años motivada por las publicaciones de Duncan Campbell con su informe COMIT titulado *Interception Capabilities 2000* para el parlamento europeo, donde se detallaba mucha información del programa Echelon. El resumen: todo el mundo debería ser consciente que el espionaje masivo aplicado al mundo civil y económico-industrial es real.

Por desgracia, la publicación de herramientas prácticas, razonablemente seguras, usando conocimientos de esteganografía lingüística es escasa. Espero que esta información le ayude a evolucionar estos principios de esteganografía lingüística, más allá de ejemplos básicos de esteganografía textual (formato del texto, codificación en espacios, fuentes, etc.), apoyándose en los enormes avances que se han realizado en en lingüística computacional, desarrollo de corpus e inteligencia artificial en esta última década.

Para facilitar al lector este camino le incluyo algunos avances y herramientas publicadas en español por el autor de este libro hace una década en su aplicación a lengua española:

- Herramienta StegoSense
    - http://www.securitybydefault.com/2010/11/herramienta-stegosense-automatizando-la.html
    - Lingüística computacional y esteganografía lingüística. Distribuyendo información oculta con recursos mínimos. http://arbor.revistas.csic.es/index.php/arbor/article/view/1562/1615
    - Muñoz, A., et al. Hiding short secret messages based on linguistic steganography and manual. Third IEEE International Symposium on Trust, Security and Privacy for Emerging Applications, 2010. http://doi.ieeecomputersociety.org/10.1109/ CIT.2010.177.
- Herramienta Stelin
    - http://stelin.sourceforge.net/
    - Esteganografía lingüística en lengua española basada en modelo N-GRAM y ley Zipf http://arbor.revistas.csic.es/index.php/arbor/article/view/1962/2302
- Herramienta JANO – Ocultación por sustitución por sinónimos
    - RootedCON 2014 - https://www.youtube.com/watch?v=KZakb7WBBmY
    - https://www.eldiario.es/hojaderouter/seguridad/esteganografia-ocultar-informacion-texto-secreto-software_0_276122727.html

- Avances sintáctico – semánticos en español

- Modificaciones sintácticas basadas en la reordenación de complementos del verbo con utilidad en esteganografía lingüística - https://dialnet.unirioja.es/servlet/articulo?codigo=3882607
- Modificaciones sintácticas en lengua española con utilidad en esteganografía lingüística - https://dialnet.unirioja.es/servlet/articulo?codigo=3143010

- Herramientas esteganografía textual
  - https://github.com/mindcrypt/stegUnicode

Bibliografía

[1] Kerckhoffs, A. La cryptographie militaire. Journal des sciences militaires, vol. 9, pp. 5–38, Janvier 1883.

[2] Shannon, C. A mathematical theory of communication. Bell System Technical Journal 1948, vol. 27, pp. 379-423.

[3] Shannon, C. Communication Theory of Secrecy Systems. Bell Systems Technical Journal 1949, vol. 28, pp. 656-715.

[4] Carracedo, J. Seguridad en redes telemáticas. Mc-Graw Hill InterAmericana de España 2004, pp. 123-131. ISBN: 84-481-4157-1.

[5] Tzu, S. El arte de la guerra. Editorial Edaf s.l 2001. ISBN-13: 978-8476406533.

[6] Kahn, D. The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. Scribner 1996. ISBN-13: 978-0684831305.

[7] McLean, A. The Steganographia of Johannes Trithemius. Magnum Opus Hermetic Sourceworks 1982.

[8] Singh, S. Los códigos secretos. Debate, 2000. ISBN-13: 978-8483062784.

[9] Oceano. Grandes enigmas de la historia. Códigos Secretos. Oceano multimedia. DVD-ROM.

[10] Plinio, C. Historia natural. Obra completa. Editorial Gredos, 2003. ISBN 978-84-249-1684-8.

[11] Kipper, G. Investigator's Guide to steganography. Auerbach Publications, 2003. ISBN: 0-8493-24 9c.

[12] Cox, I., et al. Digital Watermarking and Steganography. Morgan Kaufmann, 2 edition (2007). ISBN-13: 978-0123725851.

[13] Schott, G. Schola steganographica. Sumptibus Johannis Andreae Endteri & Wolfgangi Junioris Hæred. Excudebat Jobus Hertz Typographus Herbipol. Prostant Norimbergæ apud dictos Endteros, 1680.

[14] Wilkins, J. Mercury: Or the Secret and Swift Messenger. John Benjamins PubCo, 1985. Foundations of Semiotics, vol. 6. ISBN-13: 978-9027232762.

[15] Tobin, J., et al. Hidden in Plain View: A Secret Story of Quilts and the Underground Railroad. Anchor Books edition, 2000. ISBN-13: 978-0385497671.

[16] White, W. The microdot: Then and now. International Journal of Intelligence and CounterIntelligence, 1989. vol. 3, pp. 249-269.

[17] EFF. Machine Identification Code Technology Project. https://www.eff.org/issues/printers.

[18] Bauer, F. Decrypted Secrets. Methods and Maxims of Cryptology. Springer,1997. ISBN-13: 978-3540604181.

[19] Rojas, F. La celestina. Ediciones Escolares, 2001.ISBN: 9788489163676.

[20] El País. Defensa culpó subrepticiamente al jefe de la cúpula militar por. Revista Española de Defensa, Julio 2003. http://www.elpais.com/articulo/espana/Defensa/culpo/subrepticiamente/jefe/cupula/militar/Yak-42/2003/elpepiesp/20041019elpepinac_9/Tes/.

[21] Waters, W. Jerome Cardan: A Biographical Study. Dodo Press, 2009. ISBN-13: 978-1409959595.

[22] Leeuw, K., Meer, H. A turning Grille From The ancestral castle of the dutch stadholders. Cryptologia, April 1995. vol.9, pp. 153-165. http://www.turning-grille.com.

[23] Verne, J. Mathias Sandorf: A Play in Three Acts. Borgo Press, 2010. ISBN-13: 978-1434457684.

[24] Doyle, A. The Adventure of the Dancing Men and Other Sherlock Holmes Stories. Dover Publications, 1997. ISBN-13: 978-0486295589.

[25] Knuth, D. The TeXbook. Addison-Wesley Professional, 1984. ISBN-13: 978-0201134483.

[26] Lamport, L. LATEX. A document preparation system for high-quality typesetting, 1985. http://www.latex-project.org/intro.html.

[27] Simmons, G. The Prisoners' Problem and the Subliminal Channel. Advances in Cryptology: Proceedings of CRYPTO '83". Plenum Press (1984), pp. 51-67.

[28] Lampson, B. A note on the confinement problem. Communications of the ACM, vol. 16/1973, pp. 613-615. ISSN:0001-0782.

[29] Cachin, C. An Information-Theoretic Model for steganography. Springer, 1998. Proceedings of the Second International Workshop on Information Hiding, vol. 1525, pp. 306-318.

[30] Ahn, L., Hopper, N. Public Key Steganography. Advances in Cryptology, Eurocrypt 2004. pp. 323-341.

[31] Guillon, P., et al. Security and watermarking of multimedia contents. Conference No4, San Jose CA , ETATS-UNIS (21/01/2002), vol. 4675, pp. 38-49. ISBN 0-8194-4415-4.

[32] Backers, M., Cachin, C. Public key steganography with active attacks. Springer Berlin / Heidelberg. LNCS, vol. 3378/2005, pp. 210-226. ISBN: 978-3-540-24573-5.

[33] Natori, S. Why Quantum Steganography Can Be Stronger Than Classical Steganography. Springer Berlin / Heidelberg, vol. 102/2006, pp. 235-240. ISBN: 978-3-540-33132-2.

[34] Dobší, M., et al. A Theoretic-framework for Quantum Steganography. Proceedings of Workshop 2006. CTU, vol. A, pp. 124-125. ISBN 80-01-03439-9.

[35] Conti, R., et al. Quantum steganography. Patent 10/849789. 2004.

[36] Wallace, R., et al. Spycraft: The Secret History of the CIA's Spytechs, from Communism to al-Qaeda. Dutton Adult; First Edition ~1st Printing edition (May 29, 2008). ISBN-13: 978-0525949800.

[37] Albrecht, K., McIntyre, L. Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID. Thomas Nelson; First Printing edition (October 4, 2005). ISBN-13: 978-1595550200.

[38] Bauer, M. New Covert Channels in HTTP Adding Unwitting Web Browsers to Anonymity Sets. ACM Press, Proceedings of the 2003 ACM Workshop on Privacy in the Electronic Society, pp. 72-78. ISBN 1-58113-776-1.

[39] El-Khalil, R., Keromytis, Angelos. Hydan: Hiding Information in Program Binaries. 6th International Conference on Information and Communications Security (ICICS),Malaga, Spain. http://www.crazyboy.com/hydan/.

[40] Blasco, J., et al. Steganalysis of Hydan. Springer Boston, Emerging Challenges for Security, Privacy and Trust, vol. 297/2009, pp. 132-142. ISBN: 978-3-642-01243-3.

[41] Huang, H., et al. Detection of Hidden Information in Webpage. Fuzzy Systems and Knowledge Discovery. Fourth International Conference, 2007. pp. 317-321. ISBN 978-0-7695-2874-8.

[42] Huang, H., et al. Detection of Steganographic Information in Tags of Webpage. ACM International Conference Proceeding Series, vol. 304/2007. Article No.: 72. ISBN:978-1-59593-757-5.

[43] Huang, J., et al. Detection of Hidden Information in Webpages Based on Randomness. Information Assurance and Security, 2007. IAS 2007. http://doi.ieeecomputersociety.org/10.1109/IAS.2007.74.

[44] Johnson, N. Steganography Software. http://www.jjtc.com/Steganography/tools.html.

[45] Forrest, S. HTML Steganography Tool. http://wandership.ca/projects/deogol/intro.html

[46] Ahsan, K., Kundur, D. Practical Data Hiding in TCP/IP. Proc. Workshop on Multimedia Security at ACM Multimedia, Dec 2002.

[47] Cabuk, S., E.Brodley, C. IP Covert Timing Channels: Design and Detection. Conference on Computer and Communications Security. Proceedings of the 11th ACM conference on Computer and communications security, 2004. pp. 178-187. ISBN:1-58113-961-6.

[48] Cauich, E., et al. Data Hiding in Identification and Offset IP Fields. 2005. http://gray-world.net/papers.shtml.

[49] Giffin, J., et al. Covert Messaging through TCP Timestamps. Springer Berlin / Heidelberg, Privacy Enhancing Technologies, 2003. ISBN: 978-3-540-00565-0.

[50] Tapiador, J., et al. On the Distinguishability of Distance-Bounded Permutations in Ordered Channels. Information Forensics and Security, IEEE Transactions on vol. 3/2008, issue: 2, pp. 166-172.

[51] Feng, B., Xinkai, W. Steganography of Short messages through accessories. Laboratories for Information Technology Heng Mui Keng Terrace, Singapore 119613

[52] Rivest, R. Chaffing and Winnowing: Confidentiality without Encryption. MIT Lab for Computer Science. March 18, 1998 (rev. April 24, 1998). http://theory.lcs.mit.edu/~rivest/chaffing.txt.

[53] McDonald, A., Kuhn, M. StegFS: A Steganographic File System for Linux. Lecture Notes in Computer Science, vol. 1768/2000, pp. 463–477. doi:10.1007/10719724_32.

[54] Zadjmool, R. Hidden Threat: Alternate Data Streams. 2004. http://www.windowsecurity.com/articles/Alternate_Data_Streams.html.

[55] King, S., et al. Designing and implementing malicious hardware. USENIX Association Berkeley, CA, USA, Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats, 2008. Article No 5.

[56] Markoff, J. F.B.I. Says the Military Had Bogus Computer Gear. New York Times. 9 May, 2008. http://www.nytimes.com/2008/05/09/technology/09cisco.html.

[57] Westfeld, A., Wolf, G. Steganography in a video conferencing system. Proceedings of the Second International Workshop on Information Hiding. LNCS, vol. 1525/1998, pp. 32-47. ISBN:3-540-65386-4.

[58] Chae, J., Manjunath, B. Data Hiding in Video. Proceedings of ICIP 99, vol. 1, pp. 311 - 315.

[59] Robie, D., et al. The use of steganography to enhance error detection and correction in mpeg-2 video. Signals, Systems and Computers, vol. 2/2002, pp. 1204-1209. ISBN: 0-7803-7576-9.

[60] Vatolin, D., Petrov, O. MSU StegoVideo. Available: http://compression.ru /video/stego_video/ index_en.html.

[61] Lu, C. Multimedia Security: Steganography and digital watermarking techniques for protection of intellectual property. IGI Global Publishing, 2004. ISBN-10: 1591402751.

[62] Stegowav. Wav Steganography Tool. Available: http://home.earthlink.net /~emilbrandt/stego/softwaredos.html.

[63] Cvejic, N. Algorithms for Audio Watermarking and Steganography. Department of Electrical and Information Engineering, Information Processing Laboratory, University of Oulu (2004). ISBN 951-42-7383-4.

[64] Petitcolas, F. Mp3stego. Hide information in MP3. http://www.petitcolas.net/ fabien/steganography/mp3stego/.

[65] Romero, A., et al. Esteganálisis de la herramienta mp3stego. Actas de la IX Reunión Española sobre Criptología y Seguridad de la Información (2006), pp. 158-170. ISBN: 84-9788-502-3.

[66] Katzenbeisser, S., Petitcolas, F. Information Hiding techniques for steganography and digital watermarking. Artech Print on Demand (December 31, 1999). ISBN-13: 978-1580530354.

[67] Fridrich, J., et al. Modern Steganalysis Can Detect YASS. Proc. SPIE, Electronic Imaging, Media Forensics and Security XII, vol. 7541/2010, pp. 02-11.

[68] Westfeld, A., Pfitzmann, A. Attacks on Steganographic Systems Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools—and Some Lessons Learned. Editor Springer Berlin / Heidelberg. ISSN: 0302-9743 (Print).

[69] Fridrich, J., et al. Reliable Detection of LSB Steganography in Grayscale and Color Images. Proc. of the ACM Workshop on Multimedia and Security, 2001, pp. 27-30. ISBN:1-58113-393-6.

[70] Goljan, M., Soukal, D. Higher-order statistical steganalysis of palette images. Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents V pp. 178-190, 2003.

[71] Dumitrescu, S., et al. Detection of LSB steganography via sample pair analysis. Springer Berlin / Heidelberg, vol. 2578/2003, pp. 355-372. ISBN 978-3-540-00421-9.

[72] Ker, A. Improved detection of LSB steganography in grayscale images. Springer Berlin / Heidelberg, vol. 3200/2005, pp. 583-592. ISBN: 978-3-540-24207-9.

[73] Ker, A. Quantitive evaluation of pairs and RS steganalysis. Security, Steganography, and Watermarking of Multimedia Contents VI. Edited by Delp, Edward J., III; Wong, Ping W. Proceedings of the SPIE, vol. 5306/2004, pp. 83-97.

[74] Fridrich, J., Goljan, M. Practical Steganalysis of Digital Images–State of the Art. Proc. SPIE Photonics West, Vol. 4675, Electronic Imaging 2002, Security and Watermarking of Multimedia Contents, San Jose, California, January, 2002, pp. 1-13.

[75] Fridrich, J., et al. Steganalysis of JPEG Images: Breaking the F5 Algorithm. 5th Information Hiding Workshop, Noordwijkerhout, The Netherlands, 7-9 October 2002, pp. 310-323.

[76] Goljan, M., Hogea, D. Attacking the OutGuess. Proc. of the ACM Workshop on Multimedia and Security, 2002.

[77] Fridrich, J., et al. Steganalysis Based on JPEG Compatibility. Multimedia Systems and Applications IV, Andrew G. Tescher; Bhaskaran Vasudev; V. Michael Bove; Eds. Proc. SPIE vol. 4518, pp. 275-280.

[78] Avcibas, I., et al. Steganalysis using image quality metrics. In Proceedings of SPIE Electronic Imaging, Security and Watermarking of Multimedia Content III, vol. 4314/2001, pp. 523-531.

[79] Fridrich, J., Pevny, T. Multi-Class Detector of Current Steganographic Methods for JPEG format. IEEE Trans. on Info. Forensics and Security, vol. 3/2008, pp. 635-650. Doi: 10.1109/TIFS.2008.2002936.

[80] Pevny, T., Ker, A. from Blind to Quantitative Steganalysis. Proc. SPIE, Electronic Imaging, Media Forensics and Security XI, January 18-22, 2009.

[81] Fridrich, J., Pevny, T. Multi-class Blind Steganalysis for JPEG Images. Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia

Contents VIII, vol. 6072/2006, pp. 0O1-0O13.

[82] Fridrich, J., et al. New Blind Steganalysis and its Implications. Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VIII, vol. 6072/2006, pp. 1-13.

[83] Voloshynovskiy, T., Holotyak, S. Blind Statistical Steganalysis of Additive steganography Using Wavelet Higher Order Statistics. Communications and Multimedia Security. LNCS, pp. 273-274, DOI: 10.1007/11552055_31.

[84] Provos, N. Stegdetect. Automated tool for detecting steganographic content in images. http://www.outguess.org/detection.php.

[85] Spy-Hunter. Stegspy steganalysis tool. http://www.spy-hunter.com/ stegspydownload.htm.

[86] WetStone. Stego Suite - Discover the Hidden. Official Web: http://www.wetstonetech.com/.

[87] SARC. Steganography Analysis and Research Center. http://www.sarc-wv.com.

[88] Muñoz, A., Carracedo, J. StegSecret: Una herramienta de estegoanálisis pública. Congreso Iberoamericano de Seguridad de la Información. CIBSI 2007. http://stegsecret.sourceforge.net.

[89] Muñoz, A. Proyecto Final de Carrera. Tutor: Justo Carracedo. Universidad Politécnica de Madrid. Escuela Técnica Superior de Ingenieros de Telecomunicación. Junio 2006.

[90] Fridrich, J., et al. Writing on Wet Paper. IEEE Trans. on Sig. Proc., Special Issue on Media Security, Eds. T. Kalker and P. Moulin, vol. 53/2005, pp. 3923-3935.

[91] Fridrich, J., et al. Efficient Wet Paper Codes. Information Hiding. 7th International Workshop. Springer-Verlag. LNCS vol. 3727/2005, pp. 204-218.

[92] Fridrich, J., et al. Perturbed Quantization Steganography. ACM Multimedia&Security Journal, vol. 11/2005, pp. 98-107.

[93] Fridrich, J., et al. Wet Paper Codes with Improved Embedding Efficiency. IEEE Transactions on Information Security and Forensics, vol. 1/2006, pp. 102-110.

[94] Fridrich, J., et al. Steganography via Codes for Memory with Defective Cells. 43rd Conference on Coding, Communication, and Control, Sep 28-30, 2005.

[95] Stegpage. StegPage. An open-source steganography (stego) tool that distributes and embeds data within a web page. Available: http://stegpage.sourceforge.net/.

[96] Crandall, R. Some notes on steganography. Posted on Steganography Mailing List, 1998. http://os.inf.tu-dresden.de/~westfeld/crandall.pdf.

[97] Westfeld, A. F5 - A Steganographic Algorithm: High Capacity Despite Better Steganalysis. Springer-Verlag Berlin Heidelberg, 2001. LNCS, vol. 2137. pp. 289-302.

[98] Fridrich, J., Soukal, D. Matrix Embedding for Large Payloads. IEEE Transactions on Information Security and Forensics, vol. 1/2006, pp. 390-394.

[99] Fridrich, J., et al. On Steganographic Embedding Efficiency. Information Hiding. 8th International Workshop. LNCS, vol. 4437/2008, pp. 282-296.

[100] Fridrich, J., Filler,T. Practical Methods for Minimizing Embedding Impact in Steganography. Proc. SPIE Electronic Imaging, Photonics West, vol. 6505/2007, pp. 02-03.

[101] Hacktivismo. Office page of Camera/Shy. http://www.hacktivismo.com/projects/ index.php.

[102] Muñoz, A., et al. Detection of distributed steganographic information in social networks. EATIS 2008. Euro American Conference on Telematics and Information Systems, September 10-12. Aracaju, Brazil. ACM-DL.

[103] Shirali-Shahreza, M., Shirali-Shahreza, M. New Solution for Password Key Transferring in Steganography Methods. Proceedings of the International Conference on Computational Intelligence and Multimedia Applications, 2007. http://www.hip.ir.

[104] Provos, N., Honeyman, P. Detecting Steganographic Content on the Internet. NDSS 2002.

[105] Jack, Kelley. Terror groups hide behind Web encryption. USA TODAY 5/02/2001. http://www.usatoday.com/tech/news/2001-02-05-binladen.htm.

[106] Taxylon. Herramienta Camuflaweb, 2005. http://usuarios.multimania.es/taxylon/ index.htm.

[107] Peer2mail. Peer to Mail - Store and Share files on any Web-Mail account! http://www.peer2mail.com/.

[108] Raskin, V., et al. Why NLP should move into IAS. International Conference On Computational Linguistics. COLING-02 on A roadmap for computational linguistics - vol. 13/2002, pp. 1-7.

[109] Atallah, M., et al. Natural Language Processing for Information Assurance and Security: An Overview and Implementations. Proceedings 9th ACM/SIGSAC New

Security Paradigms Workshop, pp. 51-65, September, 2000.

[110] Raskin, V., et al. Ontology in Information Security: A Useful Theoretical Foundation and Methodological Tool. ACM Proceedings of the 2001 workshop on New security paradigms, 2001, pp 53-59.

[111] Bergmair, R. A comprehensive bibliography of linguistic steganography. Proceedings - Spi the international society for optical engineering. 2007, vol. 6505. Doi:10.1117/12.711325.

[112] Wayner, P. Mimic functions. Cryptologia XVI, pp. 193–214, July 1992.

[113] Wayner, P. Disappearing Cryptography, Second Edition: Information Hiding: Steganography & Watermarking. Morgan Kaufmann; 2 edition (May 13, 2002). ISBN-13: 978-1558607699.

[114] Tenenbaum, A. Linguistic steganography: Passing covert data using text-based mimicry. 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.

[115] Simova, M., et al. Stealthy ciphertext. Proceedings of 3rd International Conference on Internet Computing (ICOMP'05), 2005.

[116] Shu-feng, W., Huang, L. Research on Information Hiding. Degree of master, University of Science and Technology of China. 2003.

[117] Meng, P., et al. Linguistic Steganography Detection Algorithm Using Statistical Language Model. International Conference on Information Technology and Computer Science, 2009. ISBN: 978-0-7695-3688-0.

[118] Dai, W., et al. BinText steganography based on Markov state transferring probability. ACM International Conference Proceeding Series; vol. 403/2009, pp. 1306-1311. ISBN:978-1-60558-710-3.

[119] Chomsky, N. The Noam Chomsky Website. http://www.chomsky.info/.

[120] Wayner, P. Strong theoretical steganography. Cryptologia XIX, pp. 285–299, July 1995.

[121] Chapman, M. Hiding the hidden: A software system for concealing ciphertext as innocuous text. Master’s thesis, University of Wisconsin-Milwaukee, May 1997.

[122] Chapman, M., Davida, G. Hiding the hidden: A software system for concealing ciphertext as innocuous text. Information and Communications Security. LNCS, vol.

1334/1997, pp. 335-345. DOI: 10.1007/BFb0028489.

[123] Chapman, M., Davida, G., Rennhard, M. A practical and effective approach to large-scale automated linguistic steganography. Fourth International Conference, G. I.Davida and Y. Frankel, eds., Springer. LNCS, vol. 2200/2001, pp. 156-165.

[124] Chapman, M., Davida, G. Plausible deniability using automated linguistic steganography. International Conference, G. I. Davida and Y. Frankel, eds., Springer, 2002. LNCS, vol. 2437, pp. 276–287.

[125] Texto. Texto tool. ftp://ftp.funet.fi/pub/crypt/steganography (Finland).

[126] Blasco, J., et al. Csteg: Talking in C code. INSTiCC, 2008. In Proceedings of SECRYPT International Conference, pp. 399–406.

[127] Zuxu, D., et al. Text Information Hiding Based on Part of Speech Grammar. IEEE Computer Society. Proceedings of the 2007 International Conference on Computational Intelligence and Security Workshops. pp. 632-635. ISBN:0-7695-3073-7.

[128] Chand, V., Orgun, C. Exploiting linguistic features in lexical steganography: Design and proofof-concept implementation. in Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS ’06), vol. 6/2006, pp. 126b.

[129] Zhili, C., et al. Linguistic Steganography Detection Using Statistical Characteristics of Correlations. Information Hiding: 10th International Workshop, IH 2008, Revised Selected. LNCS, pp. 224 - 235. Doi: 10.1007/978-3-540-88961-8_16.

[130] Zhi-li, C., et al., A Statistical Algorithm for Linguistic Steganography Detection Based on Distribution of Words. IEEE Computer Society, 2008. Proceedings of the Third International Conference on Availability, Reliability and Security. pp. 558-563. ISBN:978-0-7695-3102-1.

[131] Zhi-li, C., et al. Effective Linguistic Steganography Detection. IEEE 8th International Conference on Computer and Information Technology Workshops, 2008. ISBN: 978-0-7695-3242-4.

[132] Meng, P., et al. Linguistic Steganography Detection Based on Perplexity. International Conference on MultiMedia and Information Technology, 2008. ISBN: 978-0-7695-3556-2.

[133] Meng, P., et al. Linguistic Steganography Detection Algorithm Using Statistical Language Model. International Conference on Information Technology and Computer Science, 2009. ISBN: 978-0-7695-3688-0.

[134] Winstein, K. Lexical steganography through adaptive modulation of the word choice hash. Illinois Mathematics and Science Academy, 1999.

[135] Atallah, M.J., et al. Natural language processing for information assurance and security: an overview and implementations. In: Proceedings of 9th ACM/SIGSAC New Security Paradigms Workshop, pp. 51–65. 2000.

[136] Nakagawa, H., et al. Information Hiding for Text by Paraphrasing. http://www.r.dl.itc.u-tokyo.ac.jp/nakagawa/academicres/finpri02.pdf.

[137] Bolshakov, I. A method of linguistic steganography based on collocationally-verified synonymy. Springer. Information Hiding: 6th International Workshop, J. J. Fridrich, ed., LNCS, vol. 3200/2004, pp. 180–190.

[138] Calvo, H., Bolshakov, I. Using selectional preferences for extending a synonymous paraphrasing method in steganography. Avances en Ciencias de la Computacion e Ingenieria de Computo - CIC'2004: XIII Congreso Internacional de Computacion, J. H. S.

[139] Bolshakov, I., Gelbukh, A. Synonymous Paraphrasing Using WordNet and Internet. Springer Berlin / Heidelberg. Natural Language Processing and Information Systems. Vol 3136/2004. pp.189-200. ISBN: 978-3-540-22564-5.

[140] Topkara, U., et al. The hiding virtues of ambiguity: quantifiably resilient watermarking of natural language text through synonym substitutions. MM&Sec '06: Proceeding of the 8th workshop on Multimedia and security, pp. 164–174.

[141] Moulin, P., O'Sullivan, J. Information-theoretic analysis of information hiding. IEEE Transactions on Information Theory, vol. 49/2003, pp. 563–593.

[142] Bergmair, R., Katzenbeisser, S. Towards human interactive proofs in the text-domain. In Proceedings of the 7th Information Security Conference. Springer Verlag. Vol. 3225/2004, pp. 257–267.

[143] Nanhe, A., et al. "Improved Synonym Approach to Linguistic Steganography" Design and Proof-of-Concept Implementation. http://dsl.serc.iisc.ernet.in/~mayuresh/ ImprovedSynonymApproachToLinguisticSteganography.pdf.

[144] Chiang, Y., et al. Natural language watermarking using semantic substitution for chinese text. Digital Watermarking: Second International Workshop, IWDW 2003, T. Kalker, I. J. Cox, and Y. M. Ro, eds., Springer. LNCS. vol 2939/2003, pp. 129-140.

[145] Yuling, L., et al. An Efficient Linguistic Steganography for Chinese Text. Proceedings of IEEE International Conference on Multimedia & Expro, 2007. pp. 2094-2097.

[146] Shirali-Shahreza, M. Text Steganography by Changing Words Spelling. ICACT 2008. ISBN 978-89-5519-136-3.

[147] Niimi, M., et al. A framework of text-based steganography using sd-form semantics model. IPSJ Journal 44, August 2003.

[148] Bergmair, R., Katzenbeisser, S. Towards human interactive proofs in the text-domain. Proceedings of the 7th Information Security Conference. Springer-Verlag, vol. 3225/2004, pp. 257–267.

[149] Bergmair, R., Katzenbeisser, S. Content-aware steganography: About lazy prisoners and narrowminded wardens. Tech. Rep. fki-252-05, Technische Universität München, Institutfür Informatik AI/Cognition Group, Dec. 2005.

[150] Xin-guang, S., et al. A steganalysis Method based on the distribution of Characters. ICSP 2006. ISBN: 0-7803-9737-3.

[151] Xin-guang, S., et al. A steganalysis method based on the distribution of first letters of words. IIH-MSP 2006. ISBN: 0-7695-2745-0.

[152] Taskiran, C., et al. Attacks on linguistic steganography systems using text analysis. Delp III 2006.

[153] Taskiran, C., et al. Attacks on lexical natural language steganography systems. Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents, January 2006.

[154] Zhenshan, Y., et al. Steganalysis of Synonym-Substitution Based Natural Language Watermarking. International Journal of Multimedia and Ubiquitous Engineering. Vol. 4, No. 2, April, 2009.

[155] Murphy, B. Syntactic information hiding in plain text. M.S. Thesis, CLCS, Trinity College., 2001.

[156] Atallah, M., et al. Natural language watermarking: Design, analysis, and a proof-of-concept implementation. Proceedings of the Fourth Information Hiding Workshop. LNCS, vol. 2137/2001, pp. 185-200.

[157] Atallah, M., Raskin, V. Natural language watermarking and tamperproofing. Proceedings of the Fifth Information Hiding Workshop. LNCS, vol. 2578/2002, pp. 196-212.

[158] Topkara, M. Natural Language Watermarking. Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents, 2005, San Jose, CA.

[159] Topkara, M., et al. Natural Language Watermarking: Challenges in Building a Practical System. Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents, 2006.

[160] Topkara, M., et al. Words are not enough: sentence level natural language watermarking. Proceedings of ACM Workshop on Content Protection and Security (MCPS). ACM Press, 2006, pp. 37-46.

[161] Murphy, B., Vogel, C. The syntax of concealment: reliable methods for plain text information hiding. Security, Steganography and Watermarking of Multimedia Contents IX. Proceedings of SPIE-IS&T Electronic Imaging SPIE vol. 6505. Doi: 10.1117/12.713357.

[162] Murphy, B., Vogel, C. Statistically-constrained shallow text marking: techniques, evaluation paradigm and results. In: Delp III 2007.

[163] Wu, J., Stinson, D. Authorship proof for textual document. Cryptology ePrint Archive, Report 2007/042.

[164] Meral, H., et al. Watermarking tools for turkish texts. in Proceedings of the 14th IEEE Conference on Signal Processing and Communications Applications 2006, pp. 1–4.

[165] Meral, H., et al. Syntactic tools for natural language watermarking. Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents, January 2007.

[166] Mesut, Hasan., et al. Natural language watermarking via morphosyntactic alterations. Computer Speech & Language, vol. 23/2009, pp. 107-125.

[167] Nakagawa, H., et al. Text information hiding with preserved meaning – a case for japanese documents. IPSJ Transaction vol. 42/2001, pp. 2339–2350.

[168] Mi-Young, K. Natural Language Watermarking for Korean Using Adverbial Displacement. International Conference on Multimedia and Ubiquitous Engineering (mue 2008). ISBN: 978-0-7695-3134-2.

[169] Y, Liu., et al. A natural language watermarking based on Chinese syntax. Advances in Natural Computation. Springer, vol. 3612/2005, pp. 958–961.

[170] Gupta, G., et al. An attack-localizing watermarking scheme for natural language documents. Proceedings of the 2006 ACM Symposium on Information, computer and communications security.

[171] Grothoff, C., et al. Translation-based steganography. Tech. Rep. TR 2005-39, Purdue CERIAS, 2005.

[172] Stutsman, R., et al. Lost in just the translation. Proceedings of the 21st Annual ACM Symposium on Applied Computing (SAC 2006).

[173] Cantrell, G., Dampier, D. Experiments in hiding data inside the file structure of common office documents: a stegonography application. ACM International Conference Proceeding Series; Vol. 90/2004. pp. 146-151. ISBN:1-59593-170-8.

[174] Wen-Chao, Y., Ling-Hwei, C. A novel steganography method via various animation effects in powerpoint files. Proceedings of the Seventh International Conference on Machine Learning and Cybernetics, Kunming, 12-15 July 2008.

[175] Brassil, J., et al. Marking text features of document images to deter illicit dissemination. In Proc. of the 12th IAPR International Conference on Computer Vision and Image Processing, vol. 2/1994, pp. 315 - 319.

[176] Brassil, J., et al. Electronic marking and identification techniques to discourage document copying. IEEE INFOCOM '94, Networking for Global Communications, pp. 1278-1287. ISBN: 0-8186-5570-4.

[177] Young-Won, K., Kyung-Ae, M. A text watermarking algorithm based on word classication and interword space statistics. Conference on Document Analysis and Recognition (ICDAR03), 1995.

[178] Low, S., et al. Document marking and identication using both line and word shifting. In Fourteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Bringing Information to People, INFOCOM 1995.

[179] Chotikakamthorn, N. Electronic document data hiding technique using intercharacter space. In Proc. of The 1998 IEEE Asia-Paci¯c Conference on Circuits and Systems, IEEE APCCAS 1998, pp. 419-422.

[180] Bhattacharjya, A., Ancin, H. Data embedding in text for a copier system. Proceedings of the ICIP, vol.2/1999, pp.245- 249.

[181] Chotikakamthorn, N. Document image data hiding techniques using character spacing width sequence coding. Proc. IEEE Intl. Conf. Image Processing,1999, Japan.

[182] Brassil, J., et al. Copyright protection for electronic distribution of text documents. Proceedings of the IEEE (USA), vol. 87/1999, no. 7, pp. 1181–1196.

[183] Bender, W. Techniques for Data Hiding. IBM Systems Journal, vol. 35/1996, pp. 313-336.

[184] Huang, D., Yan, H. Interword distance changes represented by sine waves for watermarking text images. IEEE Trans. Circuits and Systems for Video Technolo,

vol.11/2001, No.12, pp.1237-1245.

[185] Kankanhalli, M., Hau, K. Electronic Commerce Research, vol. 2/2002, pp. 169-187.

[186] Kim, Y., Oh, I. A survey on text watermarking techniques. Proc. of Honam-Jeju Korea Information Science Society, vol.14, No.1, pp.34-3, August 2002 (in Korean).

[187] Mei, Q., et al. Data Hiding in Binary Text Documents. Security and watermarking of multimedia contents. Conference No3, San Jose CA , ETATS-UNIS (22/01/2001), vol. 4314, pp. 369-375. ISBN 0-8194-3992-4.

[188] Hyon-Gon, Choo., Whoi-Yul, Kim. Data-Hiding Capacity Improvement for Text Watermarking Using Space Coding Method. LNCS, vol. 2939/2004, pp. 593-599. ISBN: 978-3-540-21061-0.

[189] Awan, I., et al. Utilization of Maximum Data Hiding Capacity in Object-Based Text Document Authentication. 2006 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06).

[190] Khairullah, M. A Novel Text Steganography System Using Font Color of the Invisible Characters in Microsoft Word Documents. Second International Conference on Computer and Electrical Engineering, 2009. ISBN: 978-0-7695-3925-6.

[191] Vinicius, P., et al. Text luminance modulation for hardcopy watermarking. Elsevier. Signal Processing, vol. 87/2007, Issue 7, pp. 1754-1771.

[192] Por, L., et al. WhiteSteg: a new scheme in information hiding using text steganography. WSEAS Transactions on Computers. Vol. 7/2008, issue 6, pp. 735-745.

[193] Desoky, A. Listega: list-based steganography methodology. International Journal of Information Security. Vol. 8/2009, issue 4, pp. 247-261.

[194] Chen, C., et al. Data Hiding in Text File Using TeX and Extraction of Hidden Data from Document Image. Journal of Applied Sciences. Vol 24/2006, pp. 115-119.

[195] Lin, S. New Methods of Data Hiding in TeX Documents. Masters Thesis, National Kaohsiung First University of Science and Technology, Taiwan, June 2004.

[196] Aravind, K., et al. High-capacity data hiding in text documents. Media Forensics and Security. Edited by Delp, Edward J., III; Dittmann, Jana; Memon, Nasir D.; Wong, Ping Wah. Proceedings of the SPIE, vol. 7254/2009. Doi:10.1117/12.805960.

[197] Chao, C., et al. Information hiding in text using typesetting tools with stegoencoding. IEEE Computer Society, 2006. Proceedings of the First International Conference on

Innovative Computing, Information and Control, pp. 459-462..

[198] Shirali-Shahreza, M., Shirali-Shahreza, M. A New Approach to Persian/Arabic Text Steganography. Proceedings of the 5th IEEE/ACIS International Conference on Computer and Information Science (ICIS 2006), Honolulu, HI, USA, July 10-12, 2006, pp. 310-315.

[199] Shirali-Shahreza, M., Shirali-Shahreza, S. Persian/Arabic Text Font Estimation Using Dots. Proceedings of the 6th IEEE International Symposium on Signal Processing and Information Technology (ISSPIT 2006), 2006, pp. 420-425.

[200] Shirali-Shahreza, M., Shirali-Shahreza, M. A new approach to persian/arabic text steganography. Proceedings of the 5th IEEE/ACIS International Conference on Computer and Information Science, pp. 310–315, IEEE Computer Society, (Washington, DC, USA), 2006.

[201] Shirali-Shahreza, M., Shirali-Shahreza, M. Steganography in Persian and Arabic Unicode Texts Using Pseudo-Space and Pseudo-Connection Characters. Journal of Theoretical and Applied Information Technology 2008.

[202] Shirali-Shahreza, M., Shirali-Shahreza, M. An Improved Version of Persian/Arabic Text Steganography Using "La" Word". Proceedings of the 6th National Conference on Telecommunication Technologies 2008 (NCTT 2008), Putrajaya, Malaysia, August 26th–28th.

[203] Shirali-Shahreza, S., et al. A Skew Resistant Method for Persian/Arabic Text Segmentation. Proceedings of the First IEEE Symposium on Computational Intelligence in Image and Signal Processing (CIISP 2007), pp. 115-120.

[204] Shirali-Shahreza, M., Shirali-Shahreza, M. A New Approach to Persian/Arabic Text Steganography. Proceedings of the 5th IEEE/ACIS International Conference on Computer and Information Science (ICIS 2006), pp. 310-315.

[205] Gutub, A., Fattani, M. A Novel Arabic Text Steganography Method Using Letter Points and Extensions. WASET International Conference on Computer, Information and Systems Science and Engineering (ICCISSE), May 25-27, 2007, Vienna, Austria.

[206] Jibran, A., et al. Evaluation of steganography for urdu/arabic text. Journal of Theoretical and Applied Information Technology.

[207] Shirali-Shahreza, M. Pseudo-Space Persian/Arabic Text Steganography. Proceedings of the Thirteenth IEEE Symposium on Computers and Communications (ISCC 2008), pp. 864-868.

[208] Gutub, A., et al. Utilizing Diacritic Marks for Arabic Text Steganography. Kuwait

Journal of Science & Engineering (KJSE), Accepted for publication in 2010.

[209] Abdul-Aziz, A., et al. e-Text Watermarking: Utilizing 'Kashida' Extensions in Arabic Language Electronic Writing. Journal of Emerging Technologies in Web Intelligence. Vol. 2/2010, No 1, pp. 48-55.

[210] Changder, S., Debnath, N. A new approach for steganography in Bengali text. Journal of Computational Methods in Sciences and Engineering, vol. 9/2009 n.1, 2S1, p.111-222.

[211] Samphaiboon, N., Dailey, M. Steganography in Thai text. Proceedings of ECTI-CON 2008.

[212] Alla, K., et al. An evolution of Hindi Text Steganography. Sixth International Conference on Information Technology: New Generations, 2009. ISBN: 978-0-7695-3596-8.

[213] Changder, S., et al. A new approach to Hindi text steganography by Shifting Matra. International Conference on Advances in Recent Technologies in Communication and Computing, 2009.

[214] Xingming, Sun., et al. Component-based digital watermarking of Chinese texts. ACM International Conference Proceeding Series; Vol. 85. Proceedings of the 3rd international conference on Information security, pp. 76-81. 2004. ISBN:1-58113-955-1.

[215] Chen, F., Wang, B. An algorithm of text information hiding based on font. Computer Technology and Development, vol. 16/2006, pp. 20-22.

[216] Ou, L., Sun. Adaptative algorithm to text information hiding based on character intensity. Application Research of Computers, vol. 24/2007, pp. 130-132.

[217] Xingtong, Liu., et al. A Steganographic Algorithm for Hiding Data in PDF Files Based on Equivalent Transformation. International Symposiums on Information Processing, 2008. ISBN: 978-0-7695-3151-9.

[218] Gang, Luo., et al. Research on Steganalysis of Stegotext Based on Noise Detecting. Journal of Hunan University (Natural Sciences), vol. 32/2005, pp. 181-184.

[219] Jijun, Zhou., et al. Research on the Detecting Algorithm of Text Document Information Hiding. Journal on Communications, vol. 25/2004, pp. 97-101.

[220] Lingjun, X., et al. Research on Steganalysis fort text steganography based on font format. IAS 2007, pp. 490-495. ISBN: 0-7695-2876-7.

[221] Lingjun, L., et al. A statistical attack on Kind of Word-Shift Text-Steganography. IIH-MSP 2008, pp. 1503-1507. ISBN:978-0-7695-3278-3.

[222] Lingjun, Li., et al. Detection of Word Shift Steganography in PDF Document. Depart of C.S. & Tech., NHPCC, USTC, Hefei, 230027, P. R. China 2. Suzhou Institute for Advanced Study, USTC. SecureComm2008. ISBN: 978-60558-241-2.

[223] Topkara, M., et al. Information Hiding through Errors: A Confusing Approach. Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents, 2007, San Jose.

[224] Shirali-Shahreza, M., Shirali-Shahreza, M. Text Steganography in SMS. Proceedings of the International Conference on Convergence Information Technology (ICCIT 2007), pp. 2260-2265.

[225] Chang, C. Emoticon-based Text Steganography in Chat. http://msn.iecs.fcu.edu.tw/courses/talk/slides/data/2009-11-17/1_Emoticonbased%20Text%20Steganography%20in%20Chat.ppt.

[226] Saichev, A. Theory of Zipf's Law and Beyond. Springer; 1 edition (November 17, 2009). ISBN-13: 978-3642029455.

[227] Molist, M. El Ministerio de Defensa trabaja en un Carnivore europeo mejorado. 22/02/2007. http://www.elpais.com/articulo/portada/Ministerio/Defensa/trabaja/Carnivore/europeo/mejorado/elpeputec/20070222elpcibpor_1/Tes.

[228] Mel'cuk, I. The Theory of the Model 'Meaning Text'. Mouton De Gruyter (December 1997). ISBN-13: 978-9027932891.

[229] Manning, C., Schütze, H. Foundations of statistical natural language processing. The Mit Press. Cambridge, Massachusetts London, England. ISBN: 0-262-13360-1.

[230] Miller, G. WordNet. A lexical database for English. http://wordnet.princeton.edu/.

[231] Subirats, C. Spanish Framenet. An on-line resource and its application to Spanish NLP. http://gemini.uab.es:9080/SFNsite/sfn-people.

[232] Castell, Núria. Spanish and Catalan WordNets. NLP Resarch Group. http://www.lsi.upc.edu/~nlp/web/index.php?Itemid=57&id=31&option=com_content&task=view.

[233] OpenOffice.org. Spanish dictionaries. http://wiki.services.openoffice.org/wiki/Dictionaries.

[234] RAE. Diccionario Panhispánico de dudas. http://buscon.rae.es/dpdI/.

[235] Academia. Ortografía de la lengua española. Real Academia Española, 1999. ISBN: 84-239-9250-0. http://www.rae.es/rae/gestores/gespub000015.nsf/%28voanexos%29 /arch7E8694F9D6446133C12571640039A189/$FILE/Ortografia.pdf.

[236] Sebástian, N., et al. LEXESP Léxico informatizado del español. Barcelona: Edicions de la Universitat de Barcelona. 2000.

[237] Wikipedia. Wikipedia Static HTML Dumps. June 2008. http://static.wikipedia.org/.

[238] Chih-Chung, C., Chih-Jen, L. LIBSVM -- A Library for Support Vector Machines. http://www.csie.ntu.edu.tw/~cjlin/libsvm/.

[239] Galicia-Haro, S., et al. Recognition of Named Entities in Spanish Texts. Lecture Notes in Computer Science. Vol. 2972/2004, pp. 420-429. ISBN: 978-3-540-21459-5.

[240] Muñoz, A., et al. Modificaciones sintácticas en lengua española con utilidad en esteganografía lingüística. RAEL – Revista Electrónica de Lingüística Aplicada, nº8, 2010. I.S.S.N.: 1885-9089.

[241] Carreter, F. Sobre la pasiva en español. Estudios de lingüística. Barcelona: Crítica. 1980, pp. 61-70.

[242] Almela, R., et al. Frecuencias del español. Diccionario y estudios léxicos y morfológicos. Editorial Universitas, S.A. 2005.

[243] Schmid, H. TreeTagger - a language independent part-of-speech tagger. Institute for Computational Linguistics of the University of Stuttgart. 2009. [Disponible en http://www.ims.uni-stuttgart.de/projekte/corplex/TreeTagger/].

[244] Jackendoff, R. X'syntax. A study of phrase structure. Cambridge, Mass: MIT Press. 1977.

[245] Hornstein, N., Lightfoot, D. Explanation in linguistics. Londres, Longman. 1981.

[246] Fernández, S. Sobre el orden de palabras en español. Dicenda. Cuadernos de Filología Hispánica, vol. 11/1993, pp. 113-152.

[247] Seco, M. Gramática esencial del español. Madrid, Aguilar. 1985. ISBN: 9788423992065.

[248] Greenberg, J. Some universals of grammar with particular reference to the order of meaningful elements. Cambridge, Mass: MIT Press. 1966.

[249] Shamir, A., Someren, N. Playing Hide and Seek with Stored Keys. Lecture Notes in Computer Science. Springer Berlin. Vol. 1648/1999. ISBN 978-3-540-66362-1.

[250] Muñoz, A., González, M. PRNG based on new HCI devices entropy sources. Wii ReMote study case. EuroAmerican Conference on Telematics and Information Systems. EATIS PRAGUE 3-5 June 2009.

[251] Hwang, M. A New Redundancy Reducing Cipher. Informatica, vol. 11/2000, no. 4, pp. 435-440.

[252] Muñoz, A., et al. Hiding short secret messages based on linguistic steganography and manual. Third IEEE International Symposium on Trust, Security and Privacy for Emerging Applications, 2010. http://doi.ieeecomputersociety.org/10.1109/CIT.2010.177.

[253] Raymond, Eric. La Catedral y el Bazar. Traducción: José Soto Pérez. http://biblioweb.sindominio.net/telematica/catedral.html.

[254] Wikipedia. Derechos humanos. http://es.wikipedia.org/wiki/Derechos_Humanos.

[255] Boyd, D., Ellison, N. Social Network Sites: Definition, history and scholarship. University of California-Berkeley, Journal of Computer-Mediated Communication. 2007.

[256] Yago, J. Como sincronizar un comando terrorista con Twitter. 15/09/2008. http://www.securitybydefault.com/2008/09/comosincronizar-un-comando-terrorista.html.

[257] Signel, R. Hackers Use Twitter to Control Botnet. August 13, 2009. http://www.wired.com/threatlevel/2009/08/botnet-tweets/.

[258] Muñoz, A., Argüelles, I. Análisis de discurso en redes sociales. Twitter un caso bajo estudio. XXVIII Congreso Internacional de la Asociación Española de lingüística aplicada. AESLA 2010. Abril 2010. Vigo.