ISSN 1688-2806

Universidad de la República
Facultad de Ingeniería

Espionaje por Emisiones Electromagnéticas

Tesis presentada a la Facultad de Ingeniería de la Universidad de la República por

Pablo Menoni

en cumplimiento parcial de los requerimientos para la obtención del título de Magister en Ingeniería Eléctrica.

Director de Tesis
Dr. Ing. Federico La Rocca..... Universidad de la República

Tribunal
Dr. Ing. Pablo Belzarena..... Universidad de la República
Dr. Ing. Gustavo Betarte..... Universidad de la República
M.Sc. Ing. Eduardo Cota..... Universidad de la República
Dr. Ing. Mauricio Delbracio..... Universidad de la República

Director Académico
Dr. Ing. Federico La Rocca..... Universidad de la República

Montevideo
Miércoles 12 de Diciembre de 2018

Espionaje por Emisiones Electromagnéticas, Pablo Menoni.

ISSN 1688-2806

Esta tesis fue preparada en LaTeX usando la clase iietesis (v1.1).
Contiene un total de 121 páginas.
Compilada el jueves 20 diciembre, 2018.
`http://iie.fing.edu.uy/`

ACTA DE DEFENSA

TESIS DE MAESTRÍA

Fecha: 12 de diciembre, de 2018 .-

Lugar: Montevideo, Facultad de Ingeniería – Universidad de la República.-

Plan de Estudio: Maestría en Ingeniería Eléctrica.-

Aspirante: **Pablo Andrés Menoni Dotti**.-

Documento de Identidad: 3,160,569-3

Director/es de Tesis: Dr. Federico La Rocca.-

Tribunal: **Dr. Pablo Belzarena (IIE, Fac. Ingeniería);**
Dr. Gustavo Betarte (INCO, Fac. Ingeniería);
Mag. Eduardo Cota (IIE, Fac. Ingeniería);
Dr. Mauricio Delbracio (IIE, Fac. Ingeniería).-

Los miembros del Tribunal hacen constar que en el día de la fecha el **Sr. Ing. Pablo Menoni** ha sido **APROBADO** en la defensa de su **Tesis de Maestría** titulada: **"Espionaje por Emisiones Electromagnéticas"**

La resolución del Tribunal se fundamenta en los puntos detallados a continuación:

La Tesis de Maestría del Ing. Menoni se centra en analizar e implementar un sistema capaz de obtener la imágen de la pantalla de un usuario a partir de las emanaciones electromagnéticas de los cables VGA y HDMI. Se busca dejar en evidencia las vulnerabilidades desde el punto de vista de la seguridad y privacidad de los usuarios. El trabajo toma como punto de partida un trabajo previo sobre este tema para sistemas VGA para luego extenderlo a la interfaz HDMI.

El documento de la tesis está redactado de manera clara y precisa. En él se ha realizado un correcto análisis teórico de los sistemas y se han probado los mismos mediante gran cantidad de simulaciones y pruebas sobre sistemas reales utilizando como hardware de captura un equipo de Software Defined Radio. A partir de estas pruebas se proponen mejoras, algunas de ellas se implementaron y se probaron y otras se dejan como trabajo futuro, lo que abre las puertas para continuar investigando en esta temática. Previo a la defensa de la tesis el candidato realizó una demostración del sistema en funcionamiento lo que permitió al tribunal observar el trabajo realizado con detalle y despejar diversas dudas. Hay que resaltar la complejidad del sistema en su implementación, lo cual implicó un esfuerzo muy importante. Durante la demostración el candidato logró que el sistema funcionara de manera robusta y se lograron observar las funcionalidades y los posibles puntos de mejora.

La presentación oral de la tesis fue muy clara, complementó el documento escrito y expuso con el detalle adecuado temas que no son fáciles de explicar en el tiempo de una presentación. El candidato contestó a las preguntas que realizó el tribunal de forma correcta y delineó posibles trabajos a futuro.

Para que conste,

Firmas originales

Dr. Pablo Belzarena

Dr. Gustavo Betarte

Mag. Eduardo Cota

Dr. Mauricio Delbracio

We do not wish to penalise the machine for its inability to shine in beauty competitions, nor to penalise a man for losing in a race against an aeroplane. The conditions of our game make some disabilities irrelevant.

Alan Turing

Esta página ha sido intencionalmente dejada en blanco.

Agradecimientos

Siguen unas breves líneas de agradecimiento a quienes me han ayudado a emprender este trabajo y sobre todo a terminarlo.

En primer lugar a mi esposa e hijas, mi inspiración y quienes dan sentido a mis esfuerzos, Ana, Florencia y Eugenia: muchas gracias por su cariño, respaldo y tolerancia.

A mi tutor y orientador, Federico "Larroca" La Rocca, por haber confiado en mi desde el principio, pero sobre todo por el apoyo, buena disposición y amabilidad ante mis consultas, tolerancia ante mis tropiezos, corregir el rumbo y la buena onda que mostró durante todo el tiempo que duró este trabajo.

A los miembros del tribunal, Pablo Belzarena, Gustavo Betarte, Eduardo Cota y Mauricio Delbracio por haber aceptado ser parte del mismo y leer esta tesis.

A mis compañeros Diego Bouvier y Gonzalo Gutierrez quienes me ayudaron con algunas de las medidas de campo.

Esta página ha sido intencionalmente dejada en blanco.

Resumen

La temática del espionaje en general, y en particular el referido a información digital, ha cautivado a muchos colectivos, desde la industria cinematográfica hasta la academia, pasando por campos tan diversos como el periodismo y la política. En este trabajo se profundiza en el estado del arte y se muestran algunos aspectos de una de las vulnerabilidades menos difundidas: las que ocurren por emanaciones de ondas electromagnéticas, a las cuales están sujetos la gran mayoría (sino todos) de los modernos sistemas de información y que muchas veces pasan desapercibidos.

A partir de la detección y procesamiento de esas emanaciones, se dejan en evidencia las debilidades desde el punto de vista de seguridad y privacidad que éstas acarrean. Estos aspectos se pueden vulnerar en un gran número de sistemas de información, por individuos con conocimientos acerca de teoría electromagnética, de los adquiridos en cursos de grado universitario, y un manejo de software a nivel programador, junto con el empleo de herramientas de hardware de bajo costo como SDR (*Software Defined Radio* por sus siglas en inglés).

El trabajo se aborda tomando como punto de partida el espionaje de emanaciones provenientes de la interfaz VGA (*Video Graphic Array*), en particular del desarrollo hecho por Martin Marinov [1], para luego extenderlo a las emanaciones de la interfaz HDMI (*High-Definition Multimedia Interface*).

Se realizan todos los planteos analíticos que permiten complementar el trabajo de Marinov, cubriendo aspectos teóricos que explican las características de la detección de imágenes a partir de las emanaciones. Se aportan algunos elementos para mejorar la detección tales como procesamiento off line y ecualización, además todos los elementos necesarios para analizar las emanaciones derivadas de las señales HDMI.

Enfocando el trabajo hacia las imágenes que contienen texto, se analizan las particularidades que presentan las emanaciones en cuanto a las transiciones bruscas de contraste en la luminiscencia, especialmente bordes entre color negro y blanco.

También se realizan algunas consideraciones y recomendaciones sobre seguridad, donde el hincapié se hace en tomar medidas para burlar el espionaje de emanaciones espurias, y sobre todo ayudar a tomar conciencia de las vulnaribilidades presentes.

Quedan disponibles los scripts usados en los ambientes de simulación tanto para GNU Octave como para GNU Radio Companion, así como también las grabaciones de las emanaciones captadas en las instancias de pruebas de campo, dentro del sitio web del grupo ARTES (Análisis de Redes, Tráfico y Estadísticas de Servicio) del Instituto de Ingeniería Eléctrica de la Facultad de Ingeniería (UdelaR): `https://iie.fing.edu.uy/investigacion/grupos/artes/es/proyectos/espionaje-por-emisiones-electromagneticas/`.

Palabras clave: SDR, espionaje, seguridad, TEMPEST, video, VGA, HDMI

Prefacio

Este documento contiene la documentación final de la Tesis de Maestría titulada: "Espionaje por Emisiones Electromagnéticas". El autor, Ing. Pablo Menoni, es estudiante de la Maestría en Ingeniería Eléctrica de la Facultad de Ingeniería - UdelaR, Plan de Estudios 2004. El trabajo transcurrió en el lapso comprendido entre junio de 2016 y diciembre de 2018 bajo la tutoría del Dr. Ing. Federico La Rocca.

El dedicado, esforzado, minucioso y a veces artesanal trabajo de los físicos del siglo XIX como André Marie Ampère, Hans Oersted y Michael Faraday, contemporáneos, y quienes sentaron las bases del electromagnetismo, despertó el interés y curiosidad de las generaciones que le sucedieron. Entre ellos, James Clerk Maxwell, con cuyo nombre me empecé a familiarizar desde mi primer curso de electromagnetismo en esta Facultad.

¿Habrá remotamente imaginado Maxwell el universo que abría con sus planteos matemáticos? Si bien resulta muy difícil retrotraerse a esa época, especular que habrán sido pocos los espacios donde haya podido compartir, fuera del ámbito académico específico, su logro unificador de la electricidad, el magnetismo y la luz, no resulta tan disparatado sino más bien parece ser una certeza. En ese entonces se desarrollaba la guerra civil en Estados Unidos, lo que sin duda acapararía las tertulias y charlas de la época, y Marx publicaba *Das Kapital*.

Las ecuaciones de Maxwell son la base sobre la que se sostienen todos los desarrollos en el campo de las tecnologías de la información y las comunicaciones (TIC). Tal afirmación nos es fácil de asimilar, sobre todo luego de haber tomado nuestros cursos de electromagnetismo, pero haberlas planteado con las limitaciones con las que sabemos se trabajaba en el siglo XIX, y saber que detrás de cada aparato o sistema electrónico está ese sustento teórico, resulta fascinante.

Maxwell dejó las herramientas para poder inferir los comportamientos de naturaleza físicos, al tiempo que Joseph Fourier, con sus series de funciones trigonométricas, nos ha facilitado la comprensión de los fenómenos desde otro punto de vista: el domino de las frecuencias. Sus grandísimos aportes, junto con las contribuciones de matemáticos e ingenieros de mediados del siglo XX, en particular los trabajos de Shannon sobre teoría de la comunicación y procesamiento de señales, y Turing en el campo de la computación, han sido el sustento para el desarrollo de las diversas disciplinas que nos dan la posibilidad de desarrollar nuestros trabajos académicos o profesionales, siendo su sustento teórico. En el medio quedan sin mencionar un montón de precursores en diferentes campos, por ejemplo los

promotores del SDR, la teoría de antenas y los impulsores del software de código abierto.

En cuanto a quienes han trabajado en el campo de las vulnerabilidades de las emanaciones electromagnéticas en los últimos años, resulta por lo menos curioso como algunos de los precursores, utilizados como referencia en este trabajo, han cambiado de disciplina de estudio, en un sentido diametralmente opuesto al de sus disertaciones. El tema es tan diverso y sus derivaciones tan amplias, que ameritaría un esfuerzo desde la academia apuntando a la concientización de otros actores de la sociedad. Recordando que una cadena es tan débil como el más débil de sus eslabones, es claro que la falta de visualización de estas vulnerabilidades por parte de los usuarios de sistemas de información los deja expuestos a espionajes maliciosos.[1]

El punto de partida para la parte experimental se basa en los trabajos de Wim van Eck [2], Martin Marinov [1] y Markus Khun [3], que a mi modesto entender sintetizan y recorren muy bien el camino de los párrafos precedentes.

Conciliar la fascinación por las disciplinas, con la concreción de resultados tangibles en un campo no menos fascinante como el del espionaje, dejando la tentación de profundizar demasiado en alguna de ellas en detrimento de las otras, ha constituido el mayor desafío en el desarrollo de este trabajo.

Por último, una breve reflexión sobre la palabra *espionaje* utilizada en el título. En tanto haya información que alguien o alguna organización trate como secreta o confidencial, existirá la tentación, o la necesidad dirán algunos, de espiarla. Pasa en una infinidad de ámbitos. En este trabajo no se hace consideración alguna sobre ninguno de los dos aspectos: la necesidad que pueda tener alguien de ocultar información y la de espiar que pueda tener otro. Sí es claro que los trabajos de espionaje han dado lugar a desarrollos fantásticos aplicables en otras disciplinas. Basta recordar el trabajo de Alan Turing y su equipo descifrando los mensajes encriptados de las *Enigma* alemanas, y sus derivaciones. Por lo tanto, este trabajo no mide intenciones y su propósito es sencillo: captar, con fines didácticos, señales electromagnéticas provenientes de monitores de computadoras personales o sus interfaces, viendo parte de su contenido bajo ciertas circunstancias y con relativa calidad que permita distinguir caracteres y formas.

El autor

[1] Si es que hay espionajes bondadosos.

Tabla de contenidos

Tabla de contenidos

Esta página ha sido intencionalmente dejada en blanco.

Capítulo 1

Introducción

Gran parte de los esfuerzos de los diferentes actores que intervienen en la seguridad de los sistemas de comunicación o computación, han sido enfocados en proteger los datos y la información cuando éstos viajan entre emisor y receptor o cuando son generados (y almacenados) dentro de los propios equipos.

Esto es, por un lado se han perfeccionado los métodos de encriptación, de forma tal de evitar o por lo menos dificultar, que quienes puedan tener acceso al flujo de datos entre emisor y receptor, logren hacerse de información útil. Y por otro lado, para evitar el robo de información en los propios receptores o transmisores (en su gran mayoría computadoras con sistemas operativos conocidos). En este sentido, es el desarrollo de sistemas detectores de malware[1] quien ha ido protegiendo estas vulnerabilidades, además, lógicamente, del desarrollo de medidas de seguridad y protocolos que involucran el acceso a los servidores donde se almacena o procesa la información, ya sea física o virtualmente.

Por lo tanto, la gran mayoría de los ataques a los sistemas de información, desde fuera de las organizaciones, requiere algún tipo de acceso a los enlaces, conocer vulnerabilidades muy específicas de la implementación del sistema o donde está alojado, e incluso tener acceso físico. Estas últimas cuestiones generalmente se resuelven una vez detectadas, pues se trata en su mayoría de debilidades en los sistemas operativos, el software de aplicación o en la transmisión de los datos.

Sin embargo, muchas partes de los sistemas de comunicación o computación aún tienen puntos débiles o por lo menos no lo suficientemente protegidos contra el robo o espionaje de la información. Tales partes refieren a aquellas que emiten energía espuria, en particular en forma de ondas electromagnéticas. Emisiones que pueden darse debido a la operativa normal del equipo, pueden ser emanaciones deliberadas o accidentales, o resultar de la ejecución del sistema de información en equipos que deliberadamente emitan señales en forma más potente que lo habitual o lo exigido por la normativa (ver sección A.3). Los equipos electrónicos como tales, producen (y emiten) campos electromagnéticos que causan disturbios al comporta-

[1] Malware como sinónimo de virus informático.

miento esperado de otros equipos que se encuentran en su entorno.[2] Esos disturbios se manifiestan sobre estos equipos de diversas formas bien conocidas, esto es: interferencia en receptores de radio y televisión, acaso las más conocidas a nivel general, y más genéricamente como un deterioro de la relación señal ruido (SNR o S/R) de los sistemas transmisor-receptor en general. Los inconvenientes que ese deterioro trae, y las medidas que se toman en tales sistemas, desde las etapas de diseño, fabricación, y hasta la misma operación para mitigarlos o por lo menos reducirlos, son bien conocidos por la industria y están largamente cuantificados en términos económicos y de performance, solo por nombrar dos aspectos.

Independientemente de si un equipo haya sido diseñado como un transmisor o no, en tanto habrá electrones moviéndose en su interior, que produzcan voltajes y corrientes que varíen con el tiempo, generarán campos electromagnéticos y por lo tanto, emitirán señales electromagnéticas que se propagarán a través del medio en el cual se encuentran inmersos (aire, vacío, agua, etc.). Este fenómeno está resumido por las expresiones de las ecuaciones de Maxwell y las deducciones a partir de ellas repetidas en la sección A.1.

Se infiere entonces que esta generación se lleva a cabo tanto dentro de los dispositivos, como en sus líneas de trasmisión, cables de conexión con dispositivos periféricos o dentro de los propios periféricos. Esta emisión se percibe como molesta o hasta peligrosa, por ejemplo cuando interfiere con sistemas de navegación de aviones. Otro ejemplo bien conocido por la industria de las compañías telefónicas, es el efecto de "crosstalk" [4], que se produce cuando una conversación de una línea se induce en la línea de otra conversación, haciendo que los interlocutores de una conversación escuchen conversaciones de otras líneas, o incluso cuando en las líneas se inducen señales de emisoras de radio.

En la Figura 1.1 se muestra la generación tanto del campo eléctrico ($\vec{E}$) como el campo magnético ($\vec{B}$) cuando circula una corriente I por un conductor, y existe una diferencia de potencial V a lo largo de su recorrido.

Cuando esos campos son lo suficientemente fuertes como para propagarse fuera del equipo, es cuando se tienen los fenómenos de emisión que se verán en este trabajo. Muy groseramente se puede inferir hasta aquí, que cuanto más grande sea I, más grande será $\vec{B}$ y cuanto más grande la diferencia de potencial V, más grande será $\vec{E}$.

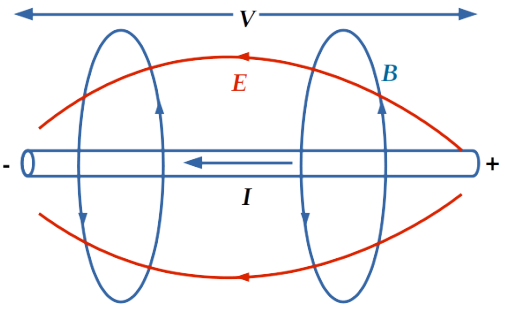


Figura 1.1: Campo electromagnético generado por una corriente.

Fenómenos similares se pueden observar en imperfecciones constructivas en conductores, las que se transforman en fuentes de radiación electromagnética. Estas imperfecciones pueden tener su origen incluso en los requerimientos de minimizar el tamaño del equipo, lo que lleva a tener componentes y cables o pistas

[2]Entendiendo por entorno a aquella área donde el campo electromagnético generado puede ser captado, atendiendo a todas las limitaciones de propagación que éste afronta.

muy próximos entre si, causando acoplamiento y que estos últimos funcionen como antenas para las señales de aquellos.

Sin embargo, esa interferencia no debería ser la única preocupación tanto de usuarios como de diseñadores y fabricantes de dispositivos electrónicos. En algunas casos, especialmente en aquellos donde no se toman precauciones en el diseño o en el uso, es posible obtener información sensible de esas emisiones. Esto es, adquiriendo las señales generadas a partir de las emisiones no deseadas, demodulándolas y eventualmente decodificándolas, con la ayuda de técnicas de procesamiento adecuadas, se podría habilitar la reconstrucción de la información que ellas contienen, a un punto tal que se obtenga de ella información sensible para quien la esté generando. Esto con el agravante que muchas veces quien es el usuario primario de esa información no ha tomado los recaudos del caso o simplemente ignora que tal cosa pueda suceder. Por lo tanto, es probable que no advierta esa adquisición, pues no se requiere acceso directo o contacto "físico" alguno con el equipo generador.

Un diseño minucioso de los dispositivos, sus periféricos y las líneas de trasmisión de datos, considerando aspectos constructivos (material) e incluso la instalación, puede minimizar ciertamente los riesgos de la reconstrucción de información a partir de sus emisiones. Siendo que un diseño seguro en términos de hardware, encapsulado e incluso de software puede acarrear costos elevados que hagan inviable la producción de algunos equipos, se trata entonces de un compromiso entre el diseño, las condiciones de uso, la posibilidad de ser espiado, y la sensibilidad de la información manejada, lo que debería valorizar el riesgo del uso del equipo.

A las emisiones espurias se las denomina tanto como *eEMR*, del inglés *emanation of ElectroMagnetic Radiation* o alternativamente *CE*, por sus siglas del inglés: *Compromising Emanations*. Este último término es usado en forma más habitual en los ambientes de seguridad nacional, en especial en EEUU. Además, se distinguen dos campos estrechamente vinculados a estas emisiones: el monitoreo o espionaje y la protección de dispositivos emisores.

No existiendo una denominación consensuada en cuanto al agrupamiento de estos dos campos, se adoptará en este documento el término TEMPEST, el cual se explicará en las secciones siguientes.

1.1. Motivación

Siendo las *eEMR* una preocupación entre quienes tratan temas de seguridad, ha sido afrontado por gobiernos de diversos países. El término TEMPEST proviene del proyecto de la Agencia Nacional de Seguridad de los EEUU, NSA [5], que en los años 60 le dio ese nombre encubierto, y que probablemente sea un acrónimo de *Telecommunications Electronic Material Protected from Emanating Spurious Transmissions*. La propia NSA se refiere a TEMPEST como un acrónimo para referirse a las investigaciones y estudios de las emanaciones comprometedoras. Entendiendo la agencia como *CE* a [6]:

> *Señales emitidas inintencionalmente las cuales, si son interceptadas y analizadas, revelan información referente a la seguri-*

> *dad nacional, transmitida, recibida, manejada o de alguna forma procesada por equipamientos que gestione infomación en alguna forma. CE consiste en energía eléctrica o acústica emitida por cualquier fuente de información dentro de equipos y/o sistemas que procesan información referente a la seguridad nacional.*[3]

No deberían perderse de vista los diferentes intereses económicos en torno a TEMPEST que impactan directamente en el costo de los equipos y las instalaciones. Por un lado la fabricación de equipos, donde para minimizar costos se ajusta a las certificaciones y normas de compatibilidad electromagnética como la EN55022 [7] (ver sección A.3.1) de la Comunidad Europea, o la regulación 47 CFR [8] (sección A.3.2) de la FCC de Estados Unidos, lo que, como se verá en este trabajo, no asegura niveles de confiabilidad altos contra el espionaje en algunas circunstancias[4]. Por otro lado, la industria de las consultorías en seguridad, donde el tema de la seguridad puede llevarse a extremos, tomando recaudos incluso en aspectos de diseño arquitectónico y constructivos de oficinas o edificios, mandatorios a veces en usos militares o de extrema seguridad [9]. Ubicar los aspectos constructivos y de diseño entre estos extremos dependerá de la evaluación de riesgos que el responsable de dichos aspectos considere.

Vale recordar a esta altura la definición de compatibilidad electromagnética (EMC) de la Comisión Electrotécnica Internacional, IEC por sus siglas en inglés:

> *Es la habilidad de un equipo o sistema de funcionar satisfactoriamente en su entorno electromagnético sin introducir disturbios electromagnéticos intolerables a cualquier otro dispositivo en ese entorno.* [10]

Esta definición describe la capacidad de sistemas o componentes eléctricos y electrónicos de funcionar correctamente cuando son puestos juntos unos con otros. En la práctica esto significa que los disturbios de origen electromagnético de cada parte de un equipo deben estar limitadas y que cada parte debe tener un grado mínimo de inmunidad frente a los disturbios de su entorno.

Se infiere entonces que aún cumpliendo con las normativas referentes a compatibilidad electromagnética, un equipo puede generar emanaciones que, sin afectar el funcionamiento normal de otros equipos, puedan ser captadas y analizadas en un equipo remoto.

Este trabajo pretende focalizarse, dentro de la temática de las emanaciones espurias, en aquellos aspectos que sirvan de base para poder discernir, a partir de experimentación y fundamentación teórica, sobre como mejorar los aspectos más

[3] *CE are defined as unintentiorial intelligence bearing signals which, if intercepted and analyzed, disclose the national security information transmitted, received, handled or otherwise processed by any information processing equipment. Compromising emanations consist of electrical or acoustical energy unintentionally emitted by any of a great number of sources within equipment/systems which process national security information.*

[4] Los monitores espiados cumplen, de acuerdo al fabricante, con la Parte 15 de las reglas de la FCC referida aquí.

vulnerables de los sistemas de información, derivados de tales emanaciones, o por lo menos advertir de sus vulnerabilidades. Es decir, solo se considerarán las emisiones que son irradiadas (*radiated emissions* en inglés) y no las que son conducidas (*conducted emissions* en inglés). Las primeras son propagadas a través del aire, vacío, agua, etc., mientras que las segundas son propagadas por los conductores de señales del equipo o de alimentación. Y dentro de aquellas, en las que son emitidas a través del aire y por lo tanto susceptibles de ser captadas por antenas ordinarias [6].

1.2. Antecedentes

Una simple anécdota y un experimento después, revelan por si mismos todas las preocupaciones que TEMPEST ha acarreado por lo menos desde los años 1940 a la fecha. Preocupaciones que se centraban más en el tema de seguridad, en tanto defensa nacional o seguridad militar, que en la emisión de campos potencialmente peligrosos para la salud humana o la interferencia.

Según se relata en [5], durante la segunda guerra mundial, tanto el Ejército como la Armada de EEUU usaban un sistema de teletipos que a su vez se valía un dispositivo de la compañía Bell, llamado "131-B2" para encriptar mensajes. Mientras uno de tales dispositivo estaba siendo probado en los laboratorios de Bell, un operario notó accidentalmente que cada vez que la máquina era usada (luego de cargar el mensaje, y dar la orden de encriptar y transmitir, *stepped* en inglés), aparecía un pico en el trazo de la señal de un osciloscopio ubicado a unos cuantos metros de distancia. Interpretando más cuidadosamente ese pico el operario podía "leer" el texto plano del mensaje a través de la señal vista en el osciloscopio.

Desde entonces y hasta aproximadamente 1985, TEMPEST permanecía casi exclusivamente reservado a los ambientes gubernamentales. En ese año, aparece quizás el primer trabajo fuera del ámbito militar [2, 11], aplicado e implementado con equipamiento muy sencillo a cargo de Win van Eck[5], quien trabajaba por esa época en los laboratorios de la entonces estatal empresa postal y de telecomunicaciones holandesa: Royal Ducth PTT (*Post, Telegraph and Telephone*). Fue así que con una antena dipolo, un receptor de televisión y circuitería para ajustar el sincronismo, logra captar, desde un auto ubicado en el estacionamiento de un edificio, las señales emitidas desde un monitor de rayos catódicos (CRT) ubicado en uno de los apartamentos, en el cual se estaba usando un procesador de texto, viendo claramente los textos allí desplegados.

Con esto se mostraba que todas las medidas de seguridad que se pudieran tomar en los canales de transmisión serían vanas si no se tomaban medidas adicionales en los receptores. Especialmente si éstos incluían monitores CRT, en lugares poco apantallados electromagnéticamente, donde la antena "espía" pudiera posicionarse cerca de éste. Entendiendo por cerca, en aquel entonces, a unos 50 metros para

[5]Es gracias a este trabajo que muchas veces se usa el término *Van Eck Phreaking* como una alternativa a TEMPEST.

monitores con carcasa de plástico y 10 metros para monitores con carcasa metálica, cuando se usan receptores de bajo costo. Distancias que, según el autor del artículo, podrían aumentarse usando antenas direccionales y receptores más sofisticados que los que él usó.

En años más recientes el desarrollo de iniciativas de software de código abierto como GNU Radio Companion [12], facilitaron el acceso al procesamiento de una amplio espectro de señales de radio usando bloques de software que implementan funciones básicas de ese procesamiento (en banda base). Complementado con el uso de diversas opciones de hardware de bajo costo que captan las señales de radiofrecuencia (RF). El espectro de RF que se puede captar es lo suficientemente amplio como para sintonizar señales provenientes de diversas aplicaciones comerciales, como TV digital o señales de radio AM o FM, y también para espiar señales espurias provenientes de dispositivos electrónicos. Esto es, usando los principios del Software Defined Radio (SDR [14], de quien se verán sus fundamentos en la sección 2.5), GNU Radio facilita todo el procesamiento referente a la parte de banda base, tanto sea para la implementación de soluciones de SDR o para la simulación de entornos.

En ese marco surge el proyecto *TempestSDR* [1], una herramienta de software cuyos detalles se verán en la sección 3.3.2, que es utilizada para captar señales emanadas desde monitores, usando un receptor (hardware) SDR. El software mapea el voltaje inducido en la antena receptora (que depende de la magnitud del campo incidente) por cada píxel del monitor emisor en una escala de grises, lo que genera una imagen, en falso color, de la señal de video original. Todo lo realiza en tiempo real sin modificar el hardware de los receptores, dejando todo el trabajo al software y también, obviamente, al hardware externo SDR.

1.3. Estado del arte

La temática de la seguridad en torno a las emanaciones cubre una amplia gama de amenazas. Algunos ejemplos se verán en esta sección y como se ha mencionado, ha sido una preocupación en los ambientes de seguridad nacional de diversos países. Paulatinamente ha ido penetrando otros segmentos como el de las urnas electrónicas, entre otros. Sin embargo aún sigue habiendo escasez de literatura abierta sobre los aspectos de seguridad de las *CE* [13].

Las limitaciones para obtener información de las emanaciones que escapen a las precauciones tomadas en los equipos fuente, básicamente apantallamiento, vienen por el lado de la propagación y la capacidad para captarlas en su frecuencia portadora o alguno de sus armónicos. Teniendo en cuenta que la señal captada puede tener algún servicio de radiodifusión público cuya portadora la interfiera, como por ejemplo señales de FM comerciales, hace que el proceso de monitoreo o espionaje sea aún más complejo. En ese caso se limita, entre otras cosas, la distancia mínima a la cual debe ubicarse la antena espía o anula las capacidades de espionaje totalmente.

A pesar que la venta de muchos de los equipos destinados al monitoreo de TEMPEST está vedada en muchas legislaciones al público en general, y por lo

tanto restringida solo a agencias gubernamentales, las posibilidades para adquirir un equipo de monitoreo de *eEMR* son diversas, en tanto diversas son las fuentes de emisión. Existen equipos que permiten un monitoreo sobre un amplio rango de frecuencias, combinando hardware y software para procesar las señales captadas. Por ello esta sección comienza con una breve descripción de hardware de propósito general, para continuar mencionando algunas iniciativas que descifran emanaciones electromagnéticas provenientes de diferentes periféricos de computadoras personales, algunas de las cuales requieren intervención en la computadora espiada.

Dentro de las iniciativas que se mencionan, y en referencia directa a la captación de señales provenientes de monitores o sus interfaces, vale resaltar la escasez de trabajos en el ámbito académico, y su gran separación temporal. De los últimos análisis realizados en la Universidad de Cambridge por Marinov, cuyo desarrollo, TempestSDR, es base fundamental de este trabajo, cortó un largo período de once años sin profundizaciones en este campo.

Dado que el tema del espionaje se maneja per se, en la mayoría de los casos, en forma reservada, secreta o "clasificada", aparece otro aspecto de acceso limitado, y refiere a las tecnologías y técnicas disponibles exclusivamente para agencias gubernamentales. Estas agencias disponen de presupuestos que les permiten acceder a las mejores técnicas, equipos y expertos. Con un presupuesto que ronda los USD 10,000: (diez mil millones de dólares americanos [15], [16]) la NSA libera parcialmente documentos conteniendo estudios sobre el tema de espionaje y no lo hace seguido. La inquietud de algunas comunidades de desarrolladores e investigadores por mantenerse actualizados ha llevado a la aparición de esfuerzos colaborativos como NSA Playset [17] donde se centra información filtrada de esas agencias.

1.3.1. Captando señales de video

Captar información útil a partir de las señales de video de un monitor de una PC se puede hacer fundamentalmente a partir de dos fuentes de emanación: el mecanismo para conformar la imagen dentro del propio monitor o las corrientes que fluyen por los cables que van hacia el monitor. Estos cables pueden ser externos, yendo del PC al monitor, o internos en el caso de las notebooks.

La forma de esta información puede ser muy variada. Desde distinguir a distancia y en tonos de grises, aunque no sea en forma nítida, lo que el monitor está desplegando, hasta poder distinguir y almacenar digitalmente señales de caracteres.

En este sentido, Wim van Eck en el año 1985 [2], dado el avance tecnológico y de producción existente cuando hizo sus experimentos (i.e: PC con monitores CRT), captó las emanaciones producidas por las señales aplicadas a la grilla de control, que modula la corriente del rayo de electrones, pudiendo ver el texto desplegado en el monitor espiado.

Posteriormente en el año 2003, ya con un parque de monitores LCD consolidado, Markus Kuhn [3], pudo sintonizar emanaciones provenientes de cables que llevaban la información (digital) de la imagen, desde el controlador de video hasta la pantalla, en una notebook, demodularlas y visualizarlas. Básicamente a partir

de pares trenzados de cables que van desde un conversor paralelo a serie en el controlador, hasta el monitor.

Posteriormente y continuando con el trabajo de Kuhn, Martin Marinov en el año 2014 [1] desarrolla una versión más versátil y económica que aquel. Usa equipamiento SDR como receptor de las señales y un software desarrollado por él (TempestSDR) que permite realizar la selección de variables de ajuste tales como resolución de la pantalla espiada, frecuencia de muestreo del SDR, etc, en forma manual o automática. Todo se realiza en forma muy amigable mediante una interfaz gráfica desarrollada en Java.

1.3.2. Descifrando tipeos

Si bien sin revelar detalles técnicos, Milos Prvulovic [18], muestra en un video en su canal de YouTube, donde es capaz de descifrar las teclas que se presionan en una computadora usando SDR y software propio. En este caso, la computadora objeto del espionaje aparenta haber sido modificada para que, ante cada tipeo, se incrementen los niveles de actividad de la memoria y el procesador, de forma de generar emanaciones con mayor potencia. En este sentido es conocido el concepto de la modulación de emisiones electromagnéticas de una computadora mediante software, a veces llamado Soft Tempest [19].

A pesar de que no queda claro si solo con esa modificación se puede lograr descifrar el tipeo, resta probar si cada tecla podría tener su propia "firma" de RF, y de esa forma lograr descifrarla.

Por otro lado, Kamran Ali et al. [20], utilizan señales WiFi para reconocer tipeos. Asumiendo que los dedos se mueven en una formación y dirección única al momento de tipear en un teclado, se puede inferir que, a partir de la evolución temporal del CSI[6], se deducirían las teclas presionadas. Kamran Ali et al., desarrollan un sistema llamado WiKey, con dos dispositivos WiFi, un transmisor y un receptor. El primero envía continuamente una señal, y el segundo recibe la señal distorsionada por los movimientos de las manos, la cual es interpretada por el sistema, infiriendo las teclas presionadas.

Si bien la asunción parece ser una débil hipótesis, existiendo diversas formas de ubicar los dedos de ambas manos para teclear, el trabajo tiene resultados interesantes aún con esas restricciones.

1.3.3. El bus de datos como emisor

La arquitectura de las computadoras, en particular las de escritorio, habilita el intercambio de datos entre la CPU y la memoria RAM a través de pistas paralelas que los unen. El flujo de datos que circula en las mismas produce emisiones. Por lo tanto, esas pistas pueden hacer las veces de antenas que emitan información. Estas

[6]La *Información del Estado del Canal*, CSI por sus siglas en inglés, refiere a las características principales del canal de comunicación, principalmente su respuesta en frecuencia, las que una vez estimadas permiten adaptar la transmisión para mejorar la performance del canal.

emisiones tendrán componentes de frecuencia del orden de la frecuencia del reloj de la RAM pero con escasa potencia como para que puedan ser captadas incluso a distancias cortas.

El trabajo hecho por Mordechai Guri et al. [21] en 2015, a través de la introducción de un malware en la PC víctima de espionaje, eleva la amplitud de esas emisiones para que sean captadas por dispositivos externos, haciendo uso de la arquitectura multicanal [7] de las placas madre. Muy básicamente, usa el conjunto de instrucciones SSE[8] que "obligan" al procesador a utilizar los multicanales, técnica que en definitiva termina amplificando las emisiones. Para evitar que la CPU use el mecanismo de caché y obligarla a usar el bus, el equipo logró, de acuerdo a lo publicado, transferir a demanda datos desde los registros de la CPU a la memoria usando la instrucción MOVNTDQ (*Move Double Quadword Non-Temporal*).

Con esto se logra transmitir un "1" elevando las emisiones y un "0" bajando la actividad del bus:

$$Tx(data) == 1 \quad ? \quad use \quad SSE \quad durante \quad T: \quad duerma \quad durante \quad T$$

Esto es, si el dato a transmitir es un "1" se usan las instrucciones SSE durante un tiempo T, por lo que todos los canales de la memoria serán usados, aumentando la potencia de la emanación, de lo contrario, si se quiere transmitir un "0", no se transmite nada (también durante un tiempo T). Esa técnica termina siendo una modulación OOK (On-Off Keying), modulando una frecuencia portadora, que es la frecuencia del reloj de la memoria del PC, a un nivel alto cuando hay un "1" y bajo cuando hay un "0".

De esta forma se deja un escenario con capacidades de transmisión que se completa con su uso para enviar datos "útiles" desde la PC espiada. Esto es, el malware tiene además que identificar qué datos debe transmitir, de qué programas, archivos, etc., y así usar el método de aumento intencional de las emisiones.

Por otro lado, la frecuencia portadora de las emisiones (el reloj de la memoria) está en el rango de frecuencias de algunas bandas de telefonía celular (i.e DDR3-1600 trabaja a 800MHz), lo que habilita a usar dispositivos celulares como receptores, para su registro o incluso transmisión en tiempo real hacia otro receptor usando las funcionalidades de SMS, Wifi, etc., que posea el teléfono.

1.3.4. Modulación de emisiones controladas por software

En línea con lo visto en la sección anterior, existen otro tipo de métodos de espionaje que también se basan en la inserción de software malicioso en sistemas operativos o aplicaciones. Kuhn et al. [19] realizaron pruebas donde lograron transmitir información a través de emanaciones controladas por software. Pudieron transmitir texto e imágenes, insertos dentro de (otras) imágenes, no visibles

[7] Es una evolución de la arquitectura de los PC donde para incrementar la velocidad de transferencia entre la RAM y la CPU se agregan más canales (pistas) entre ellos.

[8] Del inglés, *Streaming SIMD Extension* (SSE) son un conjunto de instrucciones de los procesadores Intel y AMD que permiten con una sola instrucción mover más de un dato entre los registros y la memoria.

para quien las estuvieran observando en el monitor espiado, pero demodulables y visibles remotamente por el espía.

Las emanaciones controladas por software pueden provocar la emisión de información sensible en forma de radiación EM. Este software puede ser planificado, desarrollado e introducido en las máquinas a espiar como parte de algún otro software de aplicación, por el propio vendor o desarrollador de este último, o se puede instalar posteriormente, y hurgar en la PC atacada o en la red a la cual esta esté conectada, en búsqueda de información específica. La información sensible podría incluso ser maliciosamente difundida (*broadcasted*) por el mismo software, con el que es gestionada para sus propósitos específicos. La transmisión puede ser en diversas formas, pero una de las formas que se relacionan con la estudiada en este trabajo es justamente la que se mostró en [19]. Es decir, aprovechar las emanaciones de las señales de video, solapando información, por ejemplo en forma de texto o imágenes, que el usuario no percibirá pero serán captadas y descifradas por el espía.

La NSA llama a este tipo de técnicas con el nombre *TEAPOT*:

> *Un término para referirse a la investigación, estudio, y control de emanaciones intencionales (i.e., aquellas que son inducidas y provocadas hostilmente) de sistemas y equipos automáticos de telecomunicaciones* [22].

Si el software es ajeno a las operaciones habituales del sistema, debería ser fácilmente detectable en ambientes medianamente seguros. Pero si el software, básicamente un *trojano*, es parte de otro software que fue provisto a quien es espiado por un proveedor de servicios "confiable", la detección no es tan sencilla sino ya muy difícil.

Estos malware actúan como verdaderos elementos de difusión de la información, y constituyen un arma poderosa con fines de espionaje, ya que logran eludir la mayoría de las medidas de seguridad, como por ejemplo el acceso físico. Una comparación muy primaria entre los malware vistos en 1.3.3 y 1.3.4, indicaría que las prácticas usadas en el trabajo [21] son más difíciles de detectar por programas antivirus.

1.3.5. Espionaje de computadoras en estado "air-gapped" y "audio-gapped"

Cuando una computadora tiene información sensible se la suele aislar de todo tipo de conexiones de red, externa o interna a la organización, donde ésta sirve. Incluso se le sacan o desactivan todas sus interfaces de red. Ese estado de las computadoras se denomina con el término en inglés *air-gapped*.

Aún estando en tal estado, se han explotado, a través del uso de malware, las capacidades de transmitir información sensible que tienen los parlantes de las computadoras [23], [24], mediante ondas de sonido o ultrasonido. Por lo tanto, para eliminar estas capacidades, se recomienda [25], eliminar todo tipo de hardware que pueda ser usado como canal acústico, i.e: parlantes (internos y externos) e incluso

micrófonos. Estas computadoras quedan en estado *audio-gapped*.

Dos trabajos de Mordechai Guri et al., [26] y [27], muestran que se puede espiar información en computadoras que están en los dos estados a la vez: "air-gapped" y "audio-gapped".

En el primero, llamado "Fansmitter", la computadora espiada es previamente infectada con malware. Este recoge información sensible (por ejemplo: claves de acceso), la modula y transmite usando ondas de sonido emitidas por el ventilador interno de la computadora. Ese sonido es recibido por el micrófono de un teléfono celular (también infectado) quien demodula y decodifica la señal, enviando los datos al atacante mediante SMS, Wifi o la red de datos celular.

El malware dentro de la computadora espiada controla la velocidad (RPM) de los ventiladores. A su vez el principal factor que determina los niveles de sonido del ventilador son las RPM [28]. Por lo tanto, variando las RPM del ventilador $\Rightarrow$ se varían los niveles de sonido $\therefore$ se tiene un sistema de transmisión.

El segundo caso, llamado "DiskFiltration", es conceptualmente similar al anterior, salvo que el sonido es causado por el brazo del disco duro, a quien el malware dentro de la computadora espiada controla.

1.3.6. Un adaptador USB a VGA como transmisor

Si bien no es una ataque en el sentido que no se utiliza como una herramienta de espionaje, el proyecto *osmo-fl2k* de Osmocom [29], [30], [31], utiliza un adaptador de interfaz USB a VGA junto con un software desarrollado por miembros de su equipo (Steve Markgraf et al. [31]), como transmisor de señales dentro de la señal VGA. Logrando usar el conversor DAC[9] dentro del adaptador para transmitir señales entre computadoras, moduladas dentro de la señal de video de la computadora usada como transmisor.

La configuración usada como prueba de concepto es bastante sencilla: se conecta la salida del adaptador USB a VGA a la recepción del SDR, un RTL-SDR V3, a través de un atenuador primero que se conecta a otro cable adaptador BNC$\leftrightarrow$VGA quien se conecta a aquel. Esquemáticamente:

En el USB del PC transmisor se conecta el adaptador USB/VGA $\rightarrow$ Salida VGA del adaptador$\rightarrow$ adaptador BNC/VGA $\rightarrow$ atenuador $\rightarrow$ entrada del RTL-SDR $\rightarrow$ PC que actúa como receptor.

El software, en la PC transmisora, permite elegir la fuente de la señal, pudiendo transmitir: WBFM, señales celulares GSM y LTE, entre otras. Al mismo tiempo opera el chip para que se deshabiliten las señales de sincronismo vertical y horizontal que producirían interrupciones en las transmisiones.

En las demostraciones se probaron transmisiones en diferentes armónicos de la frecuencia fundamental de la señal de video.

[9] El DAC (digital $\rightarrow$ analógico) debe ser de la familia Freco Logic FL2000.

1.3.7. Ataques activos con injertos de hardware

Salvo las acciones de espionaje descritas en la sección 1.3.1 de este repaso del estado del arte, todas de alguna forma son ataques activos, pues actúan sobre el equipo del usuario del PC que será espiado (o *usuario inadvertido*), ya sea instalándole malware o irradiándolo con radiofrecuencia.

Los ataques aquí descritos tienen la particularidad que además necesitan de la instalación de una pieza de hardware en la PC a ser espiada. Se basan en la radiación con radiofrecuencia de un implante o injerto en el objetivo o en una de sus interfaces, que modulará la portadora con la cual es iluminado con la señal que se quiere espiar. La antena receptora del espía, recogerá la "devolución" de esa señal modulada como se ilustra en la Figura 1.2. Esa reflexión le da a los injertos el nombre de *RF Retroreflectors*.

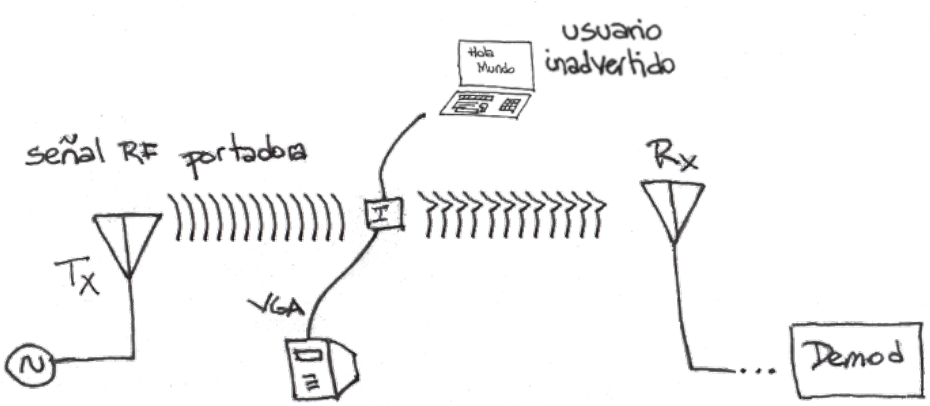


Figura 1.2: Esquema de un ataque activo. El injerto se posiciona entre la antena emisora y la receptora.

El implante no debería usar batería y por eso podría llamarse pasivo, pues actúa por ejemplo en forma análoga a los RFID, pero el ataque en sí mismo no lo es, en tanto hay que implantarlo. El usuario de YouTube "GBPPR" [32] y Michael Osman [33] ambos en 2014, muestran detallados análisis de la forma de realizar el implante con qué frecuencias irradiarlo, cómo irradiarlo y cómo captar sus reflexiones, y en ambos casos solo se han "atacado" interfaces VGA.

Se trata de, simplificando groseramente, conectar en paralelo una de las señales R, G o B de una cable VGA al gate de un transistor MOSFET y una antena (muy chica) al drain, dejando el source a tierra. La señal provocará que la corriente inducida que vaya al drain se apague y prenda al mismo ritmo que lo hace ella misma. Ello crea una señal que modula la RF que la ilumina, la que será captada por la antena espía.

Vale resaltar que las pruebas vistas en ambas referencias, con equipos de costo relativamente accesible, posicionan el injerto entre la fuente de RF que lo irradia y la antena que capta sus reflexiones, como se muestra en la Figura 1.2, no alcanzando distancias mayores a 50cm entre ambas antenas.

1.4. Esquema general del proceso de detección

La Figura 1.3 resume el esquema general de espionaje y detección de las señales. En dicho escenario, un **usuario inadvertido** estará usando un editor de texto en su computadora, cuyo monitor estará conectado a la CPU mediante un cable (VGA o HDMI).

El **espía** será quien ubique la antena, sintonice la frecuencia RF de la portadora ($f'_c \approx f_c$) o alguno de sus armónicos, y hará la demodulación, acondicionamiento y decodificación con las partes de la señal que haya podido recuperar.

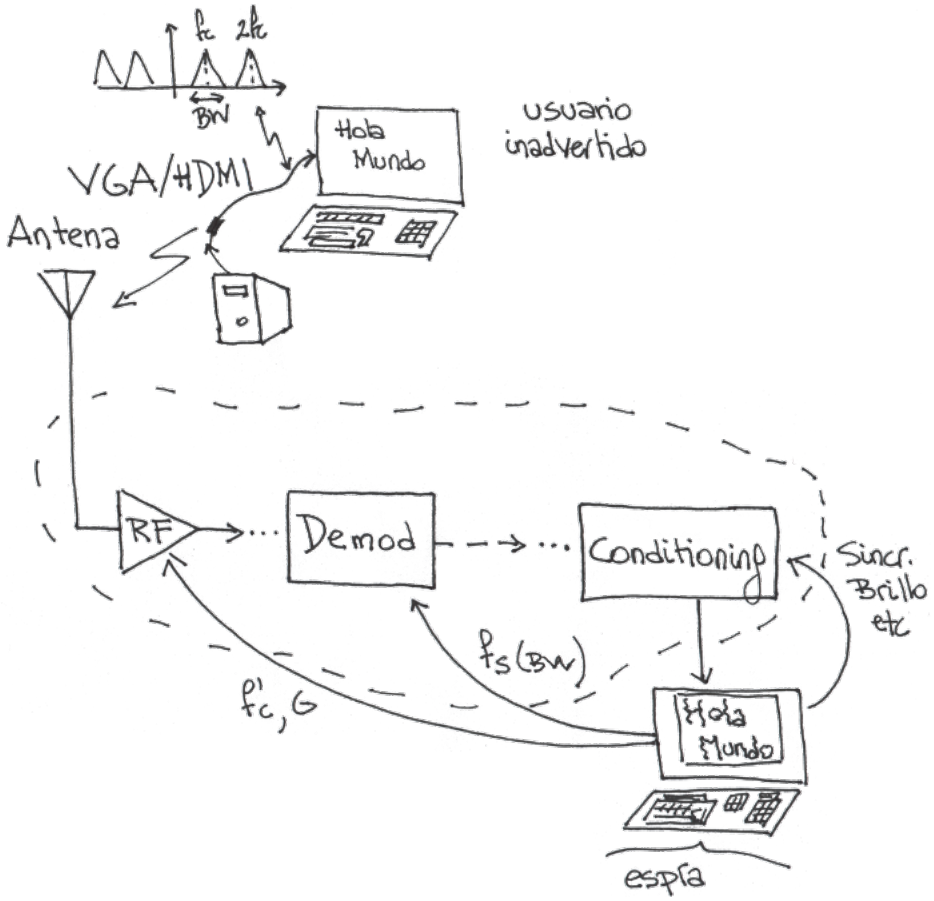


Figura 1.3: Esquema general de la detección.

1.5. Resultados obtenidos

En esta tesis se parte de una comprensión acabada de la modulación de señales de video tanto en la interfaz VGA como la interfaz HDMI, que abarcan sus características eléctricas, conformación, codificación y sus componentes de frecuencia capaces de generar emanaciones. Además se realizaron espionajes (detecciones) de

emanaciones provenientes de tales interfaces. Para ello, se partieron de simulaciones de detección y decodificación, para luego trasladarlas a escenarios reales como el de la Figura 1.3.

Primero se hicieron capturas, a modo de prueba de concepto, de emanaciones provenientes de señales de video de la interfaz VGA como se mencionó en el punto 1.3.1, y se las demoduló en ambientes de simulación y en ambientes reales. Esto último apoyado en el software desarrollado por Martin Marinov, para poder comprender cabalmente los procesos y las dificultades implicadas, que aproximan la visualización remota de texto desplegado en la pantalla de la computadora "espiada".

El trabajo continuó con capturas de emanaciones de la interfaz HDMI. Para ello se extendieron al caso HDMI los análisis hechos para el caso VGA de conceptualización de los fenómenos observados. Se sumó a ese desarrollo una análisis de oportunidades de mejora para trabajos futuros.

Teniendo en cuenta que las señales de la interfaz HDMI tienen la particularidad de incluir una codificación TMDS, que se detalla en la sección 2.4, por lo tanto agregan un grado de dificultad adicional a las experiencias de los trabajos recabados en [1] y [3] que se centraron fundamentalmente en el caso VGA.

Por último y en base a los análisis tanto analíticos como empíricos, se proponen mejoras que contribuyan a una mejor detección de las señales emanadas tanto VGA como HDMI, i.e. imágenes más nítidas o captadas a distancias razonables, junto con algunas recomendaciones sobre aspectos de seguridad para dificultar la captación de información sensible a partir de esas emanaciones. Algunos de esas mejoras se verificaron en ambientes de simulación.

No se debe perder de vista que además de las limitaciones en cuanto a propagación de algunas partes del espectro de la señal y teniendo en cuenta que el objetivo es visualizar texto, existen también aspectos subjetivos del observador. Será en definitiva la capacidad de discernir de nuestra visión quien determine, por lo menos en el alcance de este trabajo, la calidad de la recepción. Un trabajo menos subjetivo en la determinación de la calidad de los textos sin dudas se puede llevar a cabo por diversos métodos, por ejemplo buscando ocurrencias de uno o varios caracteres usando los métodos de correlación espacial o DFT [34].

1.6. Sobre la privacidad

No es el objetivo de este trabajo discutir o contraponer aspectos legales referentes al derecho a la privacidad de información o la privacidad de las personas en general. Cómo, cuándo o bajo que circunstancias primaría el interés público sobre tal derecho. Sin embargo, y más allá de lo que el sentido común de cada técnico capaz de monitorizar estas emanaciones pueda dictar, cabe recordar que en nuestra legislación existe protección de la privacidad al amparo de diversas leyes, algunas de las cuales son:

- La propia *Constitución de la República* en su artículo 28 donde establece que: "Los papeles de los particulares y su correspondencia epistolar, telegráfica o

de cualquier otra especie, son inviolables, y nunca podrá hacerse su registro, examen o interceptación sino conforme a las leyes que se establecieren por razones de interés general.".

- La Ley N^o 18331 sobre *Protección de datos personales y acción de "Habeas Data"*, donde se declara al derecho a la protección de datos personales como inherente a la persona humana y un Derecho Humano.

- La *Declaración Universal de los Derechos Humanos* en el artículo 12 donde se establece que "[...] nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia[...]".

Vale destacar que este trabajo tiene únicamente un interés académico, y del cual se pretende puedan surgir elementos que ayuden a la concientización del riesgo que acarrea la visualización o transmisión de información sensible a algún propósito. Riesgo que se pretende demostrar a través del uso de equipos de fácil adquisición, software de código abierto y desarrollos personalizados.

Por lo tanto, el uso de los conocimientos aquí resumidos, equipos mencionados, bibliografía referida, y cualquier otra información que pueda surgir o inferirse de este documento para realizar actividades prohibidas por la legislación uruguaya, son entera responsabilidad de quien las realice. Se exonera por tanto al autor, a los tutores, y a la Facultad de Ingeniería de toda responsabilidad que por dicho uso causare algún perjuicio a alguien o alguna organización.

Esta página ha sido intencionalmente dejada en blanco.

Capítulo 2

Marco teórico

Las componentes de frecuencia de la señal que se propagan son consecuencia directa en primer lugar de las velocidades de transmisión, la codificación y a partir de ella, las transiciones bruscas como las que ocurren en pulsos. Y en segundo lugar de los amplificadores, cables, periféricos, las características constructivas de las placas, circuitos integrados, etc. En el caso de imágenes generadas en una computadora y transmitidas hacia un monitor, tales transiciones se dan por ejemplo cuando hay texto con contrastes marcados sobre todo en sentido horizontal.

Siguen en este capítulo descripciones de las formas de las señales VGA y HDMI, así como también la importancia de SDR. Mencionado en más de una oportunidad en las secciones precedentes, SDR toma la posta en el proceso de captar las señales emitidas, a través de dispositivos receptores. En éstos, tanto el rango de frecuencias donde se puede sintonizar la frecuencia portadora (o sus armónicos) y la tasa de muestreo son las principales limitaciones. Combinados con dispositivos de bajo costo, se pueden incluso integrar para formar dispositivos más complejos o específicos.

2.1. Formación de la imagen

La imagen de los monitores se forma variando los niveles de luminiscencia de cierta cantidad de líneas horizontales, que con la separación y variación temporal adecuada, dan la sensación al ojo humano de continuidad y una experiencia de visualización agradable y natural.

La separación de las líneas se determina en base a la agudeza visual del ser humano, esto es, el menor ángulo (un minuto) con el cual el ojo puede distinguir una línea respecto a otra a una distancia dada. Originalmente, en los inicios de la televisión, seis veces la altura de la pantalla [35]. Esto determina la resolución vertical de una pantalla (Figura 2.1).

La variación temporal es determinada por dos requerimientos de calidad. En primer lugar, la frecuencia con la cual hay que actualizar o refrescar (*refresh*) la imagen para experimentar una sensación de continuidad en los movimientos, lo que se conoce como persistencia temporal, llamada cuadros o tramas por segundos

(*frame rate* en inglés). Y en segundo lugar el ancho de la pantalla, dado por la relación de aspecto (cociente entre el ancho y la altura), que en los inicios de la televisión se definió como de 4:3 [35].

En el caso de imágenes digitales muchas de sus características han sido heredadas de la televisión analógica o del cine. La resolución está definida por el tamaño de la menor unidad (área) que puede ser identificada (direccionada) para ser iluminada como un elemento distinguible y que contemple los requerimientos antes citados. Esta unidad se llama *píxel*. El ancho (horizontal) de cada píxel y el ancho de la pantalla determinarán cuantos píxeles entran en una línea horizontal. Esto, junto con la cantidad de líneas determina la cantidad total por pantalla de los mismos y su área individual.

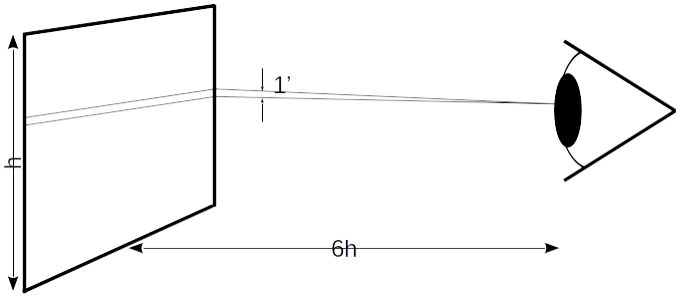


Figura 2.1: Cálculo legado de la televisión analógica de la cantidad de líneas.

La relación de aspecto mencionada, juega un rol significativo en esta temática. En las computadoras personales, se impuso durante muchos años la relación de aspecto 4:3 heredada de la televisión abierta. Al evolucionar la televisión a relaciones de aspecto de pantallas más anchas, como por ejemplo la relación 16:9, que permiten tener una sensación más integrada o panorámica cuando se ven películas, también lo hicieron los monitores de computadoras personales, que permiten tener espacios de trabajo ampliados. En la actualidad es innecesario distinguir entre televisiones y monitores.

2.2. Parámetros de una trama de video

A partir de las líneas horizontales que cubren toda el área de la pantalla, mencionadas en la sección anterior, se conforma las imágenes que fueron captadas en este trabajo. Líneas que a su vez contienen una cantidad de píxeles, cada uno de los cuales es la combinación de tres colores: rojo, verde y azul (RGB). La intensidad de cada color se representa por un voltaje proporcional a la misma en el caso de las señales VGA, o un conjunto de bits cuya cantidad depende de la profundidad de color [1] en el caso de señales digitales como HDMI o DVI.

La posición de la línea y del píxel dentro de ésta sigue siempre la misma forma secuencial, comienza arriba a la izquierda (posiciones relativas al televidente posicionado de frente a la pantalla), recorre desde izquierda a derecha la pantalla,

[1] La profundidad de color o los bits por píxel (bpp, por sus siglas en inglés) refiere a la cantidad de bits necesarios para representar los colores. Cuanto mayor sea, más colores se podrán representar.

baja a la otra línea, comienza desde la izquierda, y así hasta que llegar al rincón derecho-inferior desde donde vuelve al comienzo. Por lo tanto, no solo se precisa información de la imagen (i.e. de los colores de cada píxel), sino información de sincronización para poder ubicar los comienzos de cada línea y de cada imagen (frame), la cual es transmitida junto a la imagen.

Esta forma de conformación de la imagen es la usada en la enorme mayoría de las interfaces entre computadoras y monitores, en contraposición a la conformación vectorial de la imagen. Esta última, donde no solo se envía información de la intensidad sino también el camino que debe recorrer el haz de electrones en el caso de monitores CRT, es usada aún en algunos osciloscopios analógicos y monitores muy viejos. Por lo tanto, la señal de video no necesariamente recorre siempre la misma secuencia y no se podrían espiar con las técnicas usadas en este trabajo.

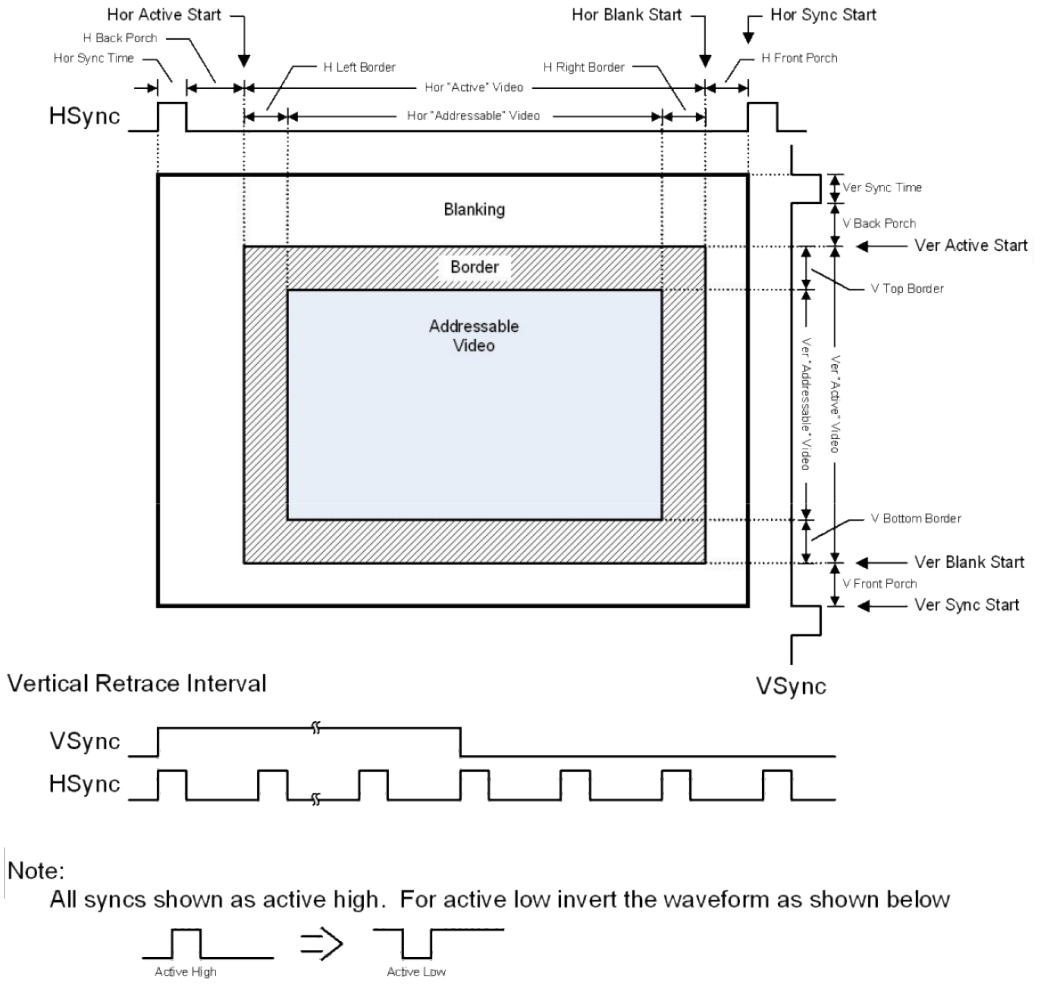


Figura 2.2: DMT: Definición de los parámetros temporales de la señal de video. Tomada de la norma VESA Display Monitor Timing Standard© Copyright 1994-2007 Video Electronics Standards Association.

En la Figura 2.2, tomada del estándar VESA *Monitoring Timing Specification Version 1.0*, se puede apreciar que para cada trama existen tiempos adicionales para sincronización tanto vertical como horizontal, que terminan aumentando la cantidad efectiva de píxeles (con píxeles sin información de color), y aumentando la frecuencia de envío. Esos píxeles, al no tener información útil de la imagen, se los llama de relleno (del inglés *Blanking pixels*).

Los tiempos involucrados se calculan, para cada resolución, de acuerdo a la norma VESA *Coordinated Video Timings (CVT) Standard, Versión 1.2, de Febrero de 2013* [36]. En particular se obtienen de ella las cantidades totales de píxeles: p_H y p_V para cada resolución.

2.2.1. Frecuencia fundamental de las señales de video

Una señal que varía en el tiempo se puede propagar en cualquiera de sus componentes de frecuencia, esto es: su frecuencia fundamental o sus armónicos. Determinar la frecuencia fundamental de una señal de video permitirá acotar la sintonización a ella misma o alguno de sus armónicos, ya que la mejor propagación y recepción dependerán de muchos factores, pero básicamente del entorno y los dispositivos de recepción que se dispongan.

Sean:

p_H	Cantidad de píxeles por línea transmitidos
p_V	Cantidad de líneas transmitidas
f_t	Frecuencia de trama (*refresh*)
f_h	Frecuencia de línea
T_p	Duración de cada píxel
r_h	Resolución horizontal en píxeles
r_v	Cantidad de líneas por trama
n_b	Cantidad de bits transmitidos por píxel
T_b	Duración de cada bit

Cada trama tiene $p_H p_V$ píxeles, y hay f_t tramas por segundo, por lo tanto:

$$T_p = \frac{1}{p_H . p_V . f_t} \tag{2.1}$$

La información que se dispone de la resolución de los monitores es siempre del estilo r_h x r_v@f_t, esto es: *ancho* x *alto* (en píxeles) y la frecuencia de trama. Ejemplo: 1920 x 1080 @ 60 Hz.

La cantidad de píxeles de sincronización tanto vertical como horizontal se estipula para cada resolución, de acuerdo al estándar VESA ya referido antes [36]. En particular se obtienen las cantidades totales de píxeles i.e: p_H y p_V para cada resolución. Por lo tanto, el tiempo efectivo o con información útil es menor que $1/f_t$ siendo:

$$\begin{aligned} p_H &= r_h + v_H \\ p_V &= r_v + v_V \end{aligned} \tag{2.2}$$

Donde v_H y v_V son la cantidad de píxeles sin información tanto horizontales como verticales fijos, dados por la norma VESA, y dependen de cada tripleta (r_h, r_v, f_t). Por consiguiente la frecuencia fundamental de las emanaciones de las señales de video es:

$$f_0 = p_H.p_V.f_t \tag{2.3}$$

Si la señal de video para cada píxel usa una codificación digital de n_b bits, multiplicará la frecuencia fundamental de la ecuación (2.3) por n_b, esto es:

$$f_0 = n_b.p_H.p_V.f_t \tag{2.4}$$

siendo $n_b = 10$ en el caso de señales HDMI.

2.2.2. Persistencia temporal de las imágenes

Gran parte de las herramientas usadas en este trabajo se basan en la poca variación que tendrá la imagen dentro de cierto rango temporal (algunas cuantas tramas), como sucede cuando una persona lee o escribe. Esto es: por rápido que escriba en el teclado o lea en la pantalla una persona, la trama se repetirá casi totalmente en las sucesivas tramas.

Esta persistencia temporal se manifiesta en el comportamiento de la autocorrelación de la función que representa la señal de video, $x(t)$, esto es:

$$R_x(\tau) = \int_{-\infty}^{\infty} \bar{x}(t+\tau)x(t)dt, \tag{2.5}$$

donde R_x es la función de autocorrelación de $x(t)$ y $\bar{x}$ es el conjugado de x.

Como R_x es una estimación de qué tan similar es $x(t)$ consigo misma trasladada τ (segundos en este caso), un máximo relativo de ella dará una pauta de algún patrón que se repite en $x(t)$. En particular que pudieran haber transcurrido $1/f_t$ segundos (duración de cada trama) o algún múltiplo de éste, esto es: la repetición de la trama.

Las herramientas que se verán en este trabajo tratan con señales digitales, por lo tanto se expresa en la siguiente ecuación la versión discreta de (2.5):

$$R_x(j) = \sum_{i=-\infty}^{\infty} \bar{x}_i x_{i+j}. \tag{2.6}$$

Análogamente al caso continuo, el valor de j donde ocurre un máximo relativo de R_x puede ser un indicio de la repetición de la trama. O más específicamente la cantidad de píxeles que tiene una trama: $p_H.p_V$.

En un escenario de espionaje, no se tiene a priori información sobre la resolución con la que está trabajando el monitor espiado. Por lo tanto, para tener una primera aproximación se recurre a buscar los valores j_m de j que den máximos relativos de la autocorrelación de la señal captada y de esa forma ir infiriendo la resolución: $j_m \approx p_H.p_V$.

Otra información importante que se puede inferir de R_x dada esta persistencia, refiere a la información sobre el espectro de $x(i)$ que esto puede aportar [37]. De

manera muy sucinta e informal, la persistencia de las tramas se expresa en que $x(i)$ es muy "similar" a $x(i + j_m)$, entonces $R_x(j) \approx R_x(j + j_m)$. Por lo tanto, la información de la "repetición" de $x(i)$, es decir sus principales componentes de frecuencia, se reflejan en su autocorrelación. Esto implica que la Transformada de Fourier de la autocorrelación, $\mathcal{F}\{R_x\}$, contendrá mucha información de las componentes de frecuencia de la propia x. Siendo j_m una componente de baja frecuencia, i.e: 60Hz, se tendrá un espectro con mucha energía concentrado en frecuencias bajas, lo que se usará más adelante en la sección 3.1 para ilustrarlo.

2.3. Señal VGA

La señal de video de la interfaz VGA, de cada uno de los tres colores, representa el nivel de intensidad de ese color dentro de cada uno de los píxeles cuya duración es T_p. Se tendrán entonces tres señales de video, una por cada componente de color.

Comenzando el análisis para uno de esos colores, se tiene que si x_i es el valor de la intensidad de ese color, del i-ésimo píxel, y $p(t)$ la forma de la señal de cada píxel, la señal de video resulta:

$$x(t) = \sum_{i=-\infty}^{\infty} x_i p(t - t_i) \tag{2.7}$$

donde $t_i = iT_p$. La forma de $p(t)$ debería ser tal que evite la interferencia inter-simbólica, permita construir una señal causal para que sea realizable y que sea limitada en frecuencia. Estas condiciones, no alcanzables en forma simultánea, se relajan pidiendo que $p(t) \to 0$ y $\mathcal{F}\{p(t)\}(f) \to 0$ cuando $t \to \infty$ y $f \to \infty$ respectivamente (pulsos de Nyquist). Como se verá más adelante en la sección 3.5.3, la forma del pulso conformador de la señal VGA no cumple con el criterio de Nyquist, siendo su forma $p(t) = 1$ cuando $0 < t < T_p$ y 0 en otro caso.

Considerando las características eléctricas de esa señal, básicamente que se trata de una señal que varía de 0 a 0.7V (unipolar), y atendiendo a la ecuación (2.7), se está frente a una señal PAM (Pulse-Amplitude Modulation, Figura 2.3).

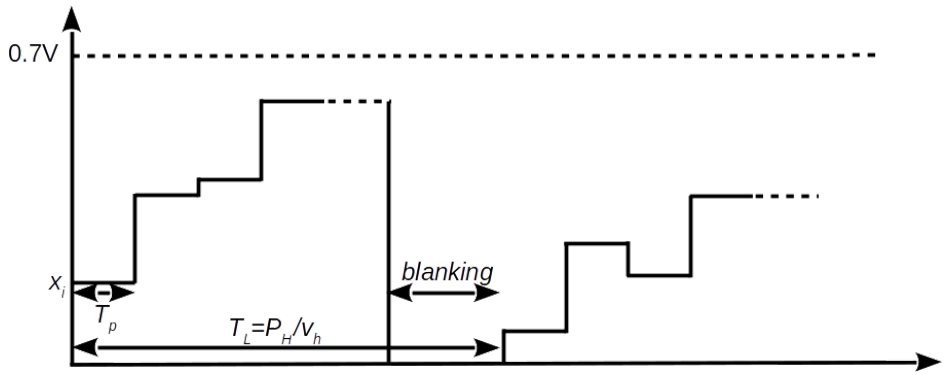


Figura 2.3: Señal de video, modulación PAM unipolar.

Tendrá por lo tanto una **componente de continua**, que se llevará gran parte de la energía y tendrá nulo aporte de información más que el nivel promedio de brillo de las imágenes.

La forma de la señal de video descrita anteriormente, que en definitiva es la que circula por cable que va desde la salida de la tarjeta de video de una computadora hasta el monitor, vista en un osciloscopio se muestra en la Figura 2.4.

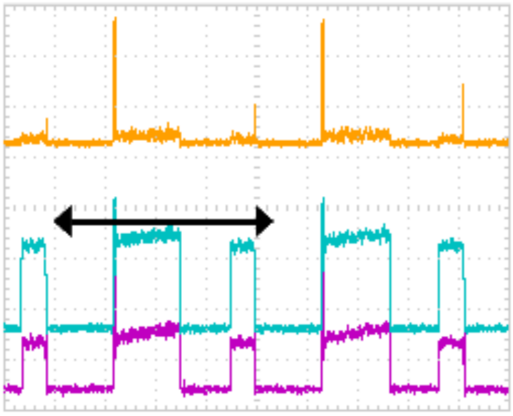


Figura 2.4: Señal de los colores R, G y B representadas en amarillo, celeste y magenta respectivamente, tomadas directamente del cable VGA. La duración de una línea se marca con una flecha.

En esa imagen se observan los niveles de voltaje de las tres componentes de la imagen, RGB, durante un intervalo equivalente a dos líneas horizontales, en la cual por un lapso de tiempo se ven niveles de voltaje ≈ 0 correspondientes al blanking y a la propia imagen, dado que, a propósito, tiene un espacio negro grande volcado sobre su derecha.

En la Figura 2.5 se observa una imagen y sobre ella, la gráfica de los niveles de señal correspondientes a la componente R de la línea que se ha resaltado con un rectángulo rojo. Se observa como los negros de las letras alternan con los blancos del fondo del texto, yendo del máximo al mínimo nivel de señal.

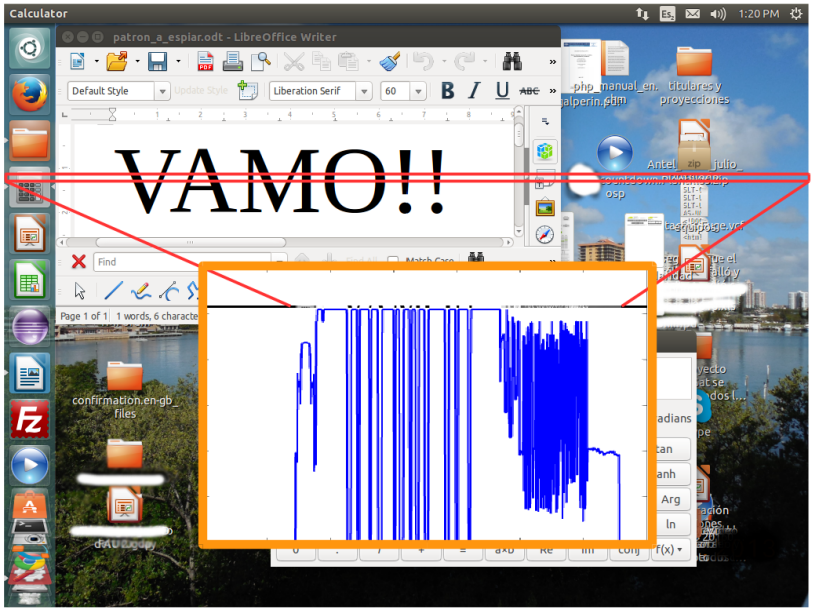


Figura 2.5: Ejemplo de niveles de voltaje de la señal R (rojo) de la línea 295 (1027x768 @60). Se observan los frentes y fondo de sincronismos. Lo encuadrado en amarillo, no pertenece a la imagen, es parte de la gráfica del nivel de señal superpuesta a la imagen.

2.3.1. Configuración de los pines VGA

El estándar VGA, entre otras cosas dispone la ubicación de los pines de los conectores (Figura 2.6 y Tabla 2.1) de los cables que van desde el PC hasta el monitor.

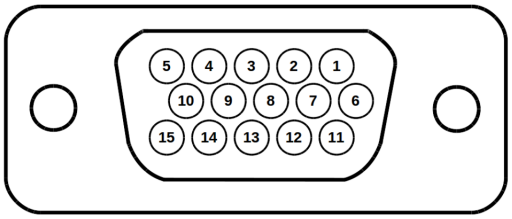


Figura 2.6: Ubicación de los pines en un conector VGA hembra.

Por lo tanto se encontrarán las señales PAM de la Figura 2.3 en los pines 1 y 6 para la componente de rojo, 2 y 7 para la de verde y, 3 y 8 para la de azul. Cada una con el nivel de voltaje, entre 0 y 0,7V, que corresponda al color según la paleta que se esté usando y la profundidad de color.

PIN	Señal	Descripción
1	RED	Componente de color rojo
2	GREEN	Componente de color verde
3	BLUE	Componente de color azul
4	RES	Reservado
5	GND	Tierra (HSync)
6	RED_RTN	Componente de color rojo
7	GREEN_RTN	Componente de color verde
8	BLUE_RTN	Componente de color azul
9	KEY/PWR	+5V DC
10	GND	Tierra (VSync, DDC)
11	RES	Reservado
12	SDA	I^2C
13	HSync	Sincronización Horizontal
14	VSync	Sincronización Vertical
15	SCL	I^2C clock

Tabla 2.1: Señales y pines VGA.

2.4. Señales HDMI

A diferencia del estándar VGA, HDMI trabaja con señales binarias y codificadas. Consiste en canales de datos que transportan ocho bits de información por cada color, y tres canales (RGB) forman un enlace TMDS (del inglés *Transition-Minimized Differential Signaling*). Es decir, que un enlace TMDS lleva información de los tres colores RGB con veinticuatro bits de información (profundidad de color de 24 bits/píxel). La interfaz puede soportar hasta dos links TMDS, aumentando entonces la información a dieciséis bits por cada color.

TMDS es el algoritmo de codificación cuyo objetivo es reducir la interferencia electromagnética (un grado adicional de dificultad para el espionaje) y facilitar la recuperación del reloj en el receptor.

Se codifican los 8 bits de cada canal en 10 bits mediante un proceso de dos etapas. En la primera etapa, el primer bit se mantiene sin cambios, y cada bit subsecuente se transforma aplicando XOR o XNOR con el resultado de la transformación del bit anterior. La elección entre XOR y XNOR resulta de minimizar la cantidad de transiciones y el noveno bit indica la operación fue utilizada. En la segunda etapa, los primeros ocho bits opcionalmente se invierten para equilibrar el balance de unos y ceros, y por lo tanto el nivel promedio de continua. El décimo bit se codifica indicando si esta inversión se llevó a cabo o no.

El código se esquematiza en la Figura 2.7 tomada de la norma [38] elaborada por el grupo de trabajo DDWG (del inglés, *Digital Display Working Group*).

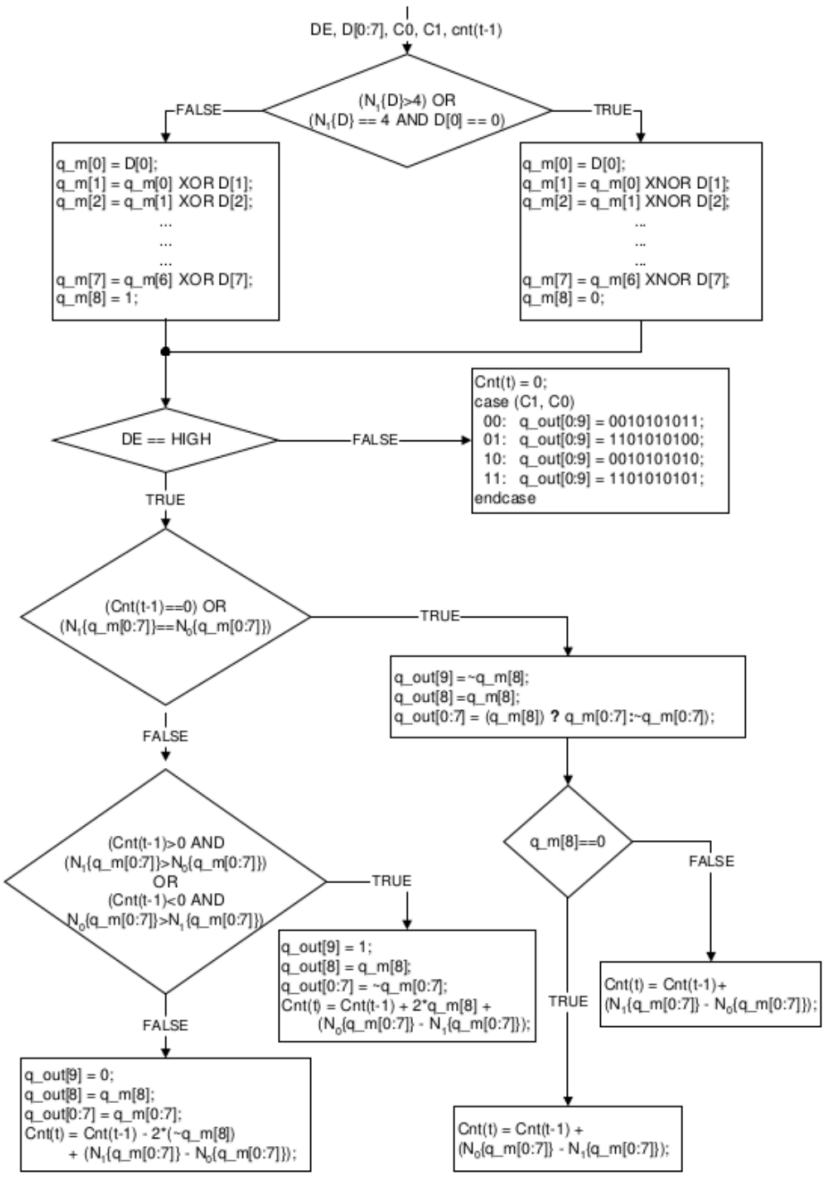


Figura 2.7: Codificación TMDS [38].

En la tabla 2.2 se describen los nombres de las señales usadas en el algoritmo de codificación. Éste produce solo cuatro patrones durante los blanking y otros cuatrocientos sesenta cuando hay datos activos. Una vez que se codifican los bits se serializan para su transmisión por la interfaz siendo el bit menos significativo (q_out[0]) el primero en transmitirse.

D, C0, C1, DE	D, datos de entrada, son los 8 bits de cada píxel para cada color. C1 y C0 son los datos de control para ese canal, y DE *data enable* que indica presencia de datos.
cnt	Lleva control de la disparidad del flujo de datos. Un valor positivo/negativo representa un exceso de "1"/"0" transmitidos.
q_{out}	Salida codificada en 10 bits.
$N_1\{x\}, N_0\{x\}$	Cantidad de "1"s/"0"s para el argumento x.

Tabla 2.2: Señales del codificador TMDS.

El decodificador se muestra en la Figura 2.8 tomada de la norma. El receptor se sincroniza con el flujo de datos durante los períodos de blanking cuya duración sea mayor a ciento veintiocho caracteres.

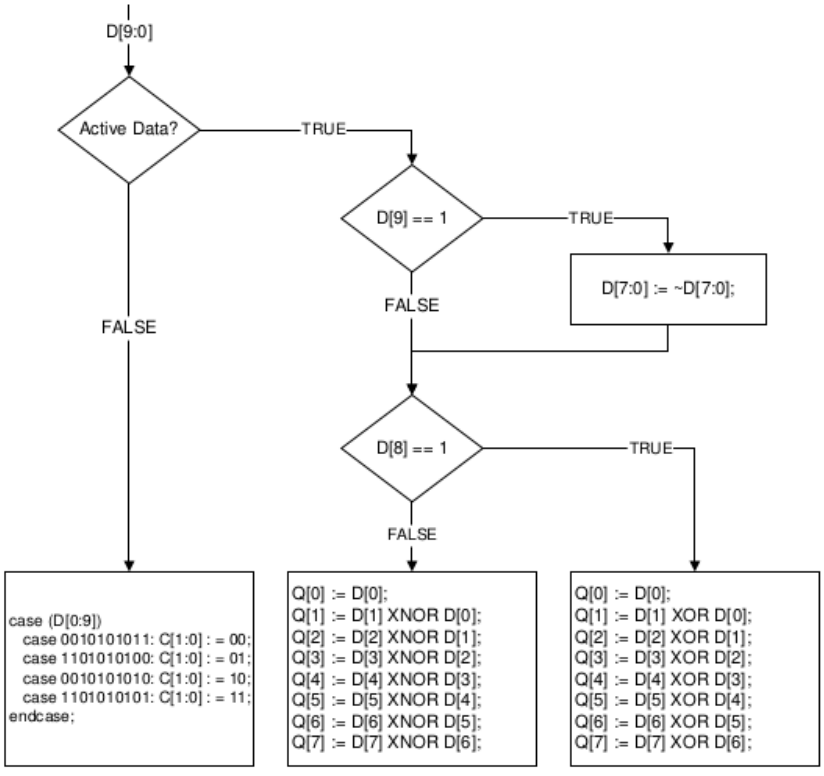


Figura 2.8: Decodificación TMDS [38].

Según se explicó en los párrafos anteriores el décimo bit (D[9]) lleva información sobre la inversión, por lo tanto, la primera etapa de la decodificación deberá invertir o no los bits de datos (D[7]:D[0]) según indique aquel bit.

La segunda etapa es muy simple, recordando que el noveno bit (D[8]) indica si la operación de codificación fue hecha con XOR o XNOR, se procede a realizar la operación que corresponda entre los bits sucesivos para obtener los ocho bits originales.

2.4.1. Configuración de los pines HDMI

En la Figura 2.9 se muestra la disposición de los pines en el conector y en la tabla 2.3 la correspondiente información de los canales y pines.

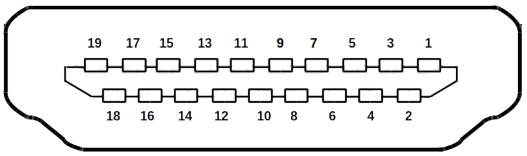


Figura 2.9: Ubicación de los pines en un conector HDMI.

HDMI heredó el formato digital del estándar DVI, por lo tanto son compatibles, y un adaptador HDMI ⇔ DVI solo tiene que cablear (conectar) los pines de uno y otro conector sin necesidad de elementos activos.

Por lo tanto, todas las consideraciones de este documento hechas sobre HDMI valen para las interfaces DVI, teniendo en cuenta que DVI en algunas de sus versiones (DVI-I) coexiste con VGA en el mismo cable.

PIN	**Señal**	**Descripción**
1	TMDS Data2+	
2	TMDS Data2 Shield	Color rojo
3	TMDS Data2-	
4	TMDS Data1+	
5	TMDS Data1 Shield	Color verde
6	TMDS Data1-	
7	TMDS Data0+	
8	TMDS Data0 Shield	Color azul
9	TMDS Data0-	
10	TMDS Clock+	
11	TMDS Clock Shield	
12	TMDS Clock-	
13	CEC	Consumer Electronics Control
14	Reservado	
15	SCL	Serial Clock for DDC
16	SDA	Serial Data for DDC
17	Tierra	
18	+5V	55mA mínimo
19	Hot Plug Detect	

Tabla 2.3: Señales y pines HDMI.

Las señales de HDMI trabajan del mismo modo que VGA en el sentido que llevan información útil referente a la intensidad del color de cada píxel y además información de sincronismo (blanking) tanto vertical como horizontal, y la pantalla se recorre de arriba a bajo y de izquierda a derecha.

En cuanto a las características eléctricas, según se ve en la Figura 2.10, existen dos modos de transmisión, uno con componente de continua y otro sin ella. La norma también establece las tolerancias de los voltajes, tiempo de subida y bajada (*rise time* y *fall time*), jitter, diagramas de ojo para transmisor y receptor, etc.

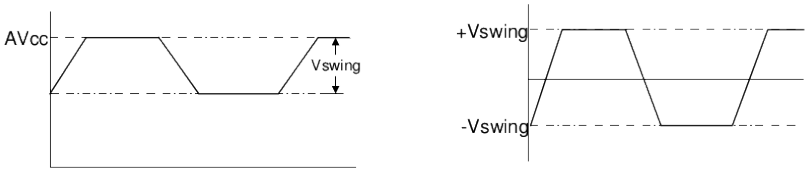


Figura 2.10: Características eléctricas de la señal TMDS. Modo diferencial sobre la derecha [38]. Donde $AV_{cc} = 3{,}3V \pm 5\,\%$ y $0{,}4V \leq V_{swing} \leq 0{,}6V$.

2.5. SDR: Radio definido por software

Las técnicas SDR son las grandes habilitadoras para el desarrollo de trabajos de espionaje como el de este trabajo. En éstos, tanto el rango de frecuencias donde se puede sintonizar la frecuencia portadora (o sus armónicos) y la tasa de muestreo son las principales limitaciones. Combinados con dispositivos de bajo costo, se pueden incluso integrar para formar dispositivos más complejos o específicos.

Los equipos de radio tradicionales normalmente usan, tanto para transmitir como para recibir señales, hardware dedicado. Es decir, su implementación se basa principalmente en el hardware. Esto es, dependiendo de la aplicación específica, tienen una limitación en cuanto al espectro de frecuencias que pueden sintonizar y, la codificación y protocolos que pueden usar, limitados a sus aplicaciones específicas. Estas limitaciones generalmente solo pueden ser modificadas por un cambio en sus componentes o en su firmware.

Existiendo una gran variedad de protocolos de comunicaciones inalámbricos, la limitación descrita muestra la nula flexibilidad que los dispositivos basados en hardware tienen para manejar diversos protocolos o cubrir grandes espectros de frecuencia.

SDR lo que hace es trasladar algunas de las funcionalidades de esos equipos hechas en hardware, hacia soluciones basadas en software, lo que le da más flexibilidad y versatilidad por ejemplo en cuanto a reconfiguraciones. Provee a los equipos con "hardware programable por software".

Este esquema de trabajo permite que el hardware se pueda utilizar en múltiples propósitos, dejando las complejidades de la detección (o modulación en el caso de la transmisión) para el software. La limitación radica, como se mencionó, en el ancho de banda que puede sintonizar el hardware y con que frecuencias de muestreo puede operar [14, 39].

Los dispositivos SDR proveen la sintonización en la frecuencia portadora, la cual puede ser superheterodina u homodina, y el muestreo, entregando señales digitales en fase y cuadratura.

En la Figura 2.11 se puede observar un esquema de un receptor SDR. Desde el software le indica al hardware que frecuencia debe sintonizar (f_c), y con que

período de muestreo trabajar (T_s). Este entrega las señales digitales al software, quien se encargará de la decodificación.

Por lo tanto, y con el mismo hardware, se pueden ejecutar desde una sencilla radio que sintonice emisoras de FM hasta una radiobase celular, en equipos con capacidad de transmisión, simplemente ejecutando distintos programas en el PC.

Obsérvese de la Figura 2.11, donde en gris la parte de hardware y en amarillo la parte de software, que el dispositivo entrega la componente en fase I_r, y la componente en cuadratura Q_r de la señal recibida.

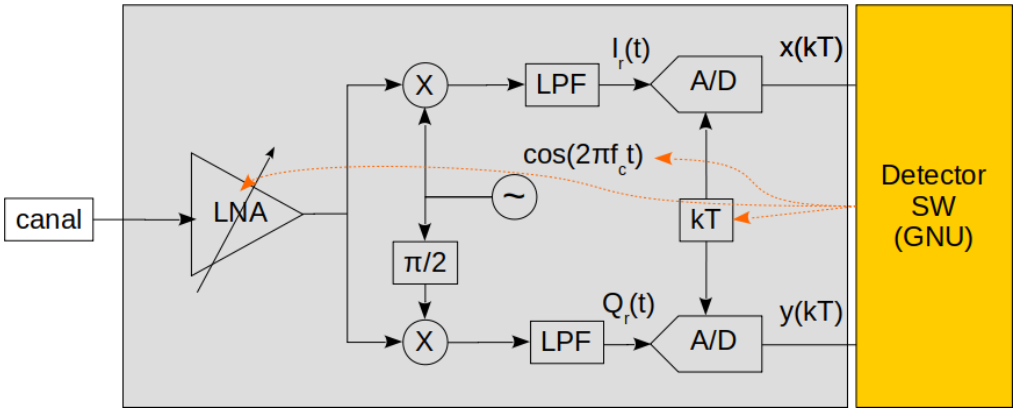


Figura 2.11: Esquema en recepción de un dispositivo SDR. Las flechas punteadas anaranjadas indican las variables del SDR que pueden ser configuradas desde el software.

En cuanto al procesamiento por software a partir de las señales entregadas por los dispositivos SDR, existen aplicaciones a medida de acuerdo a la aplicación específica, como TempestSDR desarrollado en el marco del trabajo [1] o versátiles como GNU Radio [12].

Lo expuesto de ninguna forma deja fuera de consideración a las soluciones que desarrollen equipos o software dedicado. Es más, el propio trabajo de van Eck es una muestra de ello.

Esta página ha sido intencionalmente dejada en blanco.

Capítulo 3

Espionaje de una señal de video VGA

En este capítulo se presentan las bases conceptuales y los trabajos que terminan concretando el espionaje de señales VGA usando las herramientas disponibles que se describen en la sección 3.3. Se comienza con una extensión del marco teórico desarrollado en el capítulo 2, pero esta vez apuntando a las ecuaciones temporales y el espectro de frecuencias.

Luego se continua con trabajos y resultados divididos en dos partes, a saber:

a) **Pruebas de concepto o simulaciones**, descritas en la sección 3.4, donde se confirman a grandes rasgos los resultados que se pueden esperar con las herramientas usadas y los entornos de trabajo. Estas pruebas fueron hechas con herramientas de software.

b) **Pruebas de campo o espionaje** propiamente dicho, donde se ajustan las condiciones de espionaje tanto del equipamiento, de acuerdo a las limitaciones presupuestales que determinaron el hardware a usar descrito en la sección 3.3.1, como del software.

Por último se realiza una comparación entre las dos pruebas para tener cierta certeza que las mejoras que se ensayarán en software, y cuyos resultados se presentarán en el capítulo 4, allanarán el camino a trabajos posteriores.

Cuando corresponda, y a pesar que en este capítulo se trabaja con señales VGA, se hará referencia a consideraciones para el caso HDMI con la vista puesta en que las contribuciones apuntan a la extensión del trabajo de Marinov a tal interfaz.

3.1. Representación temporal y espectral de la señal de video

Retomando el análisis de la ecuación de video (2.7) vista en el capítulo 2,

$$x(t) = \sum_{i=-\infty}^{\infty} x_i p(t - t_i)$$

se toma su transformada de Fourier:

$$X(f) = \sum_{i=-\infty}^{\infty} x_i P(f) e^{-j2\pi i f T_p}, \tag{3.1}$$

donde $X(f) = \mathcal{F}\{x(t)\}(f)$ y $P(f) = \mathcal{F}\{p(t)\}(f)$ son la TF (Transformada de Fourier) de $x(t)$ y $p(t)$ respectivamente. Por lo tanto,

$$X(f) = P(f) \sum_{i=-\infty}^{\infty} x_i e^{-j2\pi i f T_p}. \tag{3.2}$$

De la ecuación (3.2) podemos inferir que la transformada de Fourier de la señal de video (del color elegido), es la transformada de Fourier del pulso conformador de los píxeles multiplicada por la DTFT (*Discrete Time Fourier Transform*) de los píxeles x_i, evaluada en $2\pi f T_p$. Esto es:

$$X_s(e^{j\Omega})\Big|_{\Omega=2\pi f T_p} = \sum_{i=-\infty}^{\infty} x_i e^{-j2\pi i f T_p}. \tag{3.3}$$

La evaluación que figura en la ecuación (3.3) es un reescalamiento en frecuencias de la DTFT, en particular el punto $\Omega = \pi$ corresponde al punto $f = \frac{1}{2T_p}$.

Tomando como forma del pulso conformador un rectángulo, a cuenta de un análisis más exhaustivo en la sección 3.5.3, $p(t) = rect(t/T_p)$, entre 0 y T_p, resulta entonces:

$$\mathcal{F}\{p(t)\}(f) = \frac{sin(\pi T_p f)}{\pi f} \tag{3.4}$$

En la Figura 3.1 se aprecia una representación simplificada del espectro, lo que da una idea del efecto que el pulso conformador tiene sobre el espectro de la señal propagada. En la misma se asume sólo con efectos prácticos que el espectro de la señal x_i es una especie de triángulo con lados levemente redondeados hacia la base. Esta forma de X_s no es del todo antojadiza, ya que como se vio en la sección 2.2.2, dada la persistencia de las imágenes, la energía se concentra sobre las componentes de baja frecuencia. Siendo $X_s(e^{j\Omega})$ por definición una señal periódica, es un tren de triángulos. Dichos triángulos son atenuados por el $sinc = sin(\pi T_p f)/\pi f$, resultando entonces el módulo del espectro de la señal en el cable VGA el representado en color rojo de la figura, que sería lo que efectivamente generaría las emanaciones de la señal de uno de los tres colores.

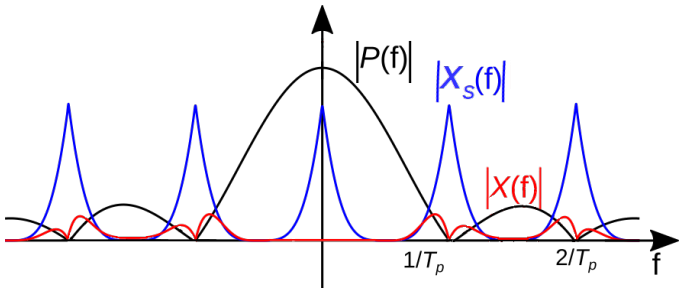


Figura 3.1: Representación esquemática del módulo del espectro de la señal de video de la ecuación (3.3), donde la componente banda base de X(f) no se grafica ya que no propaga.

Las componentes frecuencias susceptibles de propagarse son aquellas con frecuencias del orden de los megahertz o superior. Por lo tanto, un espía deberá centrarse en el primer armónico alrededor de $1/T_p$ (aproximadamente 63.5MHz para el caso de 1024x768 @60Hz). De todas formas, es importante notar que, al menos para esta forma de $p(t)$, la señal en ese armónico no contendrá la información de la continua. Esto significa por ejemplo que una pantalla con valores constantes (o que varían poco) no se podrá espiar, como sería el caso de una línea horizontal del mismo color en la pantalla de origen generada por un valor constante del nivel de brillo, lo que a priori parece muy difícil de propagarse y por ende de reconstruirse.

Hasta ahora en esta sección las deducciones que comienzan con la ecuación (2.7) y terminan en la ecuación (3.4) se basan en una señal: $x_i(t)$, que indica los valores de intensidad de cada píxel que se presentan en la señal PAM de la interfaz VGA. Pero en una señal HDMI, cada píxel se codifica en forma de una palabra binaria, por lo tanto $x(t)$ debe sustituirse con:

$$x(t) = \sum_{i=-\infty}^{\infty} b_i p_b(t - t_i), \tag{3.5}$$

donde la forma más común de $p_b(t) = rect(t/T_b)$, siendo $n_b T_b = T_p$ con n_b la cantidad de bits por píxel. En el caso de HDMI se tiene $n_b = 10$. El pulso conformador, si bien de duración más corta que el caso de las señales VGA (diez veces menor para la misma resolución), tiene la misma forma, por lo tanto las consideraciones hechas en los párrafos precedentes, y graficadas en la Figura 3.1 siguen siendo válidas [1]. Lógicamente las frecuencias se multiplican en igual proporción, lo que se reflejaría en la Figura 3.1 con frecuencias $1/T_b$, en lugar de $1/T_p$, y sus múltiplos.

Este impacto en el espectro de la señal de video tiene una directa consecuencia en las frecuencias de muestreo que se necesitan para recuperar la señal (i.e. en el hardware utilizado para la detección). A priori se tenderá a pensar que dadas las frecuencias que maneja el hardware SDR con el que se trabajó y las frecuencias de las señales VGA de baja resolución son del mismo orden, visualizar señales emanadas desde interfaces HDMI es poco probable. Ya se irán despejando estas dudas, hasta comprender qué se puede ver, y cómo, a pesar de estas limitaciones.

Por otro lado, los niveles de la señal, esto es, los valores que puede tomar b_i son binarios, como se muestra en la Figura 2.10. Este hecho a priori constituiría una ventaja en el momento de decidir qué valor es el representado en la transmisión si se contara con hardware que trabaje a las frecuencias adecuadas.

Por último, los bits transmitidos (10) por cada valor de cada color son producto de la codificación de los bits originales que representan la componente de color del píxel transmitido codificado según se vio en la sección 2.4. Esto implica que no se podría, en principio, hacer una demodulación análoga a la hecha en [1] para el caso VGA, dado que hay que decodificar en la recepción.

[1] Si bien la codificación tiene dos variantes, una con componente de continua y otra no, como se vio en la sección 2.4, las consideraciones respecto al espectro no cambian teniendo en cuenta que la componente de continua no se propaga.

3.2. Análisis de las señales detectadas

Tomando como base la forma de la señal de video VGA de la ecuación (2.7), el esquema general de detección de la Figura 1.3 y la recepción con técnicas SDR explicadas en la sección 2.5, se retoma aquí el análisis de la sección anterior.

El primer análisis se hace partiendo de las señales VGA, y el proceso de recepción que se muestra en la Figura 3.2

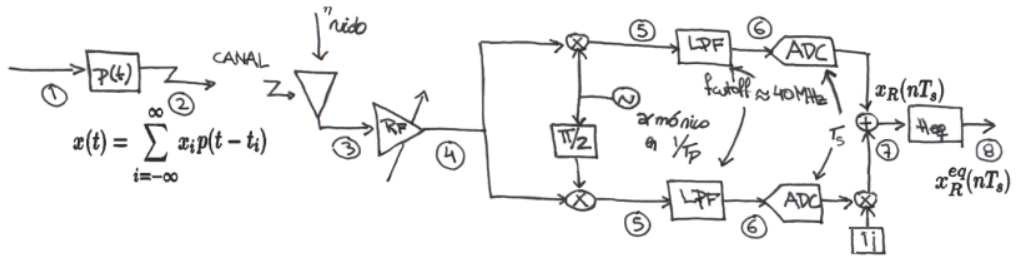


Figura 3.2: Esquema de recepción, donde se numeran las diferentes etapas que se consideran relevantes para el análisis y al mismo tiempo sirven para referir en las simulaciones. La señal a la salida del SDR que ingresa a la computadora para su procesamiento es la que está presente en el punto (7). H_{eq} refiere a la posibilidad de ecualizar la señal a la salida del SDR.

La señal entregada por la antena (punto (3)) a la etapa de sintonización, contendrá, si es que logra captar las emisiones del cable, información útil en la portadora f_p o alguno de sus armónicos mf_p. Por lo tanto el oscilador se elige en alguno de esos armónicos.

Entre los puntos (4) y (5) habrá que demodular la señal con el armónico en el cual se sintonizó, y entregarla a los filtros pasabajos (LPF).

Los filtros pasabajos se representan a través de una transferencia ideal $H_{lpf} = rect(f/f_{cutoff})$, y son los que seleccionan uno solo de los componentes del tren "triángulos" de la Figura 3.1 modulados. Luego de muestrear a tasa $1/T_s = f_s$, en el punto (7) de la Figura 3.2 se tendrá la señal de la ecuación (3.2) trasladada $f_p = 1/T_p$ más ruido aditivo, corrimientos en fase y frecuencia que se considerarán más adelante:

$$x_R(nT_s) = \mathcal{F}^{-1}\Big\{ X(f - mf_p) rect(f/f_{cutoff}) \Big\}\Big|_{t=nT_s}. \tag{3.6}$$

La ecuación (3.6) tiene la siguiente representación temporal:

$$\boxed{x_R(nT_s) = \Big[x(t) e^{-j2\pi f_p t} \Big] * h_{lpf}(t)\Big|_{t=nT_s}} \tag{3.7}$$

Esta ecuación representa la señal discreta y compleja (fase y cuadratura) que entrega el SDR, punto (7) de la Figura 3.2 y es fácilmente implementable en simulaciones por software.

La señal a la salida del ecualizador, punto (8), formará parte de las correcciones que se proponen, y se lograron hacer en las simulaciones en Octave que se verán más adelante.

Es importante resaltar en este punto que hay diferencias sustanciales entre la frecuencia de la señal f_p o f_b y la frecuencia de muestreo $1/T_s$ que puede alcanzar el hardware SDR. Diferencias que explican casi en su totalidad las dificultades de una visualización clara de las emisiones. En el caso de una resolución de 1024x768 @ 60Hz la señal VGA tendrá $f_p = 63{,}4MHz$, y una señal HDMI con una resolución de 800x600 @60Hz, se tendrá $f_b = 383{,}4MHz$, resoluciones ambas muy bajas por cierto. La frecuencia de muestreo que alcanza el modelo de SDR usado es como máximo $1/T_s = 52MHz$. Este efecto también será analizado.

3.2.1. Más sobre la recepción de la señal VGA

En la sección anterior se llegó a una expresión para la señal entregada por el equipo SDR al software de procesamiento plasmada en la ecuación (3.7).

Si se parte de la ecuación anterior a esa, (3.6), y se sustituye el valor de $X(f)$ dentro de la antitransformada de Fourier por su valor en la ecuación (3.2) y usando el valor de X_s en (3.3) se tiene:

$$x_R(nT_s) = \mathcal{F}^{-1}\Big\{P(f - mf_p)X_s(f - mf_p)rect(f/f_{cutoff})\Big\}\Big|_{t=nT_s}. \tag{3.8}$$

A los efectos de simplificar se toma $m = 1$, esto es, el primer armónico de la frecuencia fundamental.

También se sabe que la señal $X_s(f)$ es periódica de período $1/T_p$, en tanto es la DFTF de $\{x_i\}$ por lo tanto (3.8) es igual a:

$$x_R(nT_s) = \mathcal{F}^{-1}\Big\{P(f - f_p)X_s(f)rect(f/f_{cutoff})\Big\}\Big|_{t=nT_s} \Rightarrow \tag{3.9}$$

$$x_R(nT_s) = \mathcal{F}^{-1}\Big\{X_s(f)\Big\} * g(t)\Big|_{t=nT_s} \tag{3.10}$$

donde:

$$g(t) = \mathcal{F}^{-1}\Big\{P(f - f_p)rect(f/f_{cutoff})\Big\}. \tag{3.11}$$

La ecuación (3.10) dice muchísimo, pues indica que las muestras recuperadas de $x(t)$ resultan de evaluar la antitransformada de Fourier de las muestras x_i de la señal VGA (cada valor de la señal PAM), convolucionada por una señal $g(t)$ cuya forma a priori se conoce (ecuación (3.11)). Esto es:

$$\mathcal{F}^{-1}\Big\{X_s(f)\Big\} = \sum_{i=-\infty}^{\infty} x_i\delta(t - iT_p). \tag{3.12}$$

Sustituyendo (3.12) en (3.10) y operando:

$$x_R(nT_s) = \sum_{i=-\infty}^{\infty} x_i \delta(t - iT_p) * g(t)\Big|_{t=nT_s} \tag{3.13}$$

$$\boxed{x_R(nT_s) = \sum_{i=-\infty}^{\infty} x_i g(nT_s - iT_p)} \tag{3.14}$$

La representación espectral de la función $g(t)$ es la porción del *sinc* en color negro de la Figura 3.1 entre $1/2T_p$ y $3/2T_p$ bajada a bandabase, lo que permite trazar algunas conclusiones a la vez que aparecen oportunidades de mejora en la recepción que se verán en las siguientes secciones. Vale destacar que salvo que $g(nT_s - iT_p)$ sea 1 para $i = 0$ y 0 para el resto de las i habrá interferencia de los demás píxeles, i.e. Interferencia InterSimbólica (ISI).

3.3. Herramientas usadas en este trabajo

La recepción de las señales y la sintonización se hace a través de hardware SDR, conectado a una antena externa mediante cable coaxial. El SDR, como ya se mencionó, provee la sintonización, la cual puede ser superheterodina u homodina, y el muestreo, entregando señales digitales en fase y cuadratura (Figura 2.11), mientras que el procesamiento de las señales en banda base se hace mediante software, usando GNU Radio Companion versión 3.7.10.1 [12] o TempestSDR [5]. En las etapas de simulación y pruebas de concepto que se describen en la sección 3.4 se utiliza GNU Octave, versión 4.0.0 [40].

En otras etapas de la simulación (sección 3.4) se usan encadenadas: señales generadas en Octave, tomadas como entrada mediante archivos en GNU Radio quien a su vez escribe archivos del tipo *fifo* de Linux[2] que son consumidos por el software TempestSDR.

El espionaje propiamente dicho (sección 3.5), se hizo usando el software TempestSDR, explicado en la sección 3.3.2, tomando las señales captadas por el SDR.

3.3.1. Hardware

El hardware utilizado, en tanto SDR, es multipropósito y dado que se tomó como requerimiento que sea de bajo costo, resultó en la elección de un USRP B200 de Ettus, cuyo costo resulta en el entorno de los USD 1300 (dólares americanos un mil trescientos, precios al 6/5/2017). Se utilizaron diferentes antenas (ver Figura 3.3), de muy bajo costo (menos de USD 100) conectadas siempre al mismo equipo.

SDR: El kit USRP B200 SDR de Ettus [41] puede recibir y transmitir en el espectro que va desde los 70 MHz a los 6 GHz, y trabaja con una frecuencia de muestreo que alcanza los 56Mhz (usando GNU Radio Companion y en las condiciones de prueba de este trabajo solo se alcanzaron 45MHz como frecuencia

[2]Este tipo de archivos pueden ser abiertos por múltiples procesos en modo escritura o lectura, y son útiles en el caso de este ejemplo, mientras un proceso lo escribe otro lo lee.

de muestreo). Posee una interfaz USB 3.0 y es fácilmente integrable con Software de procesamiento como GNU Radio Companion (ver sección 3.3.2).

Antenas: El USRP B200 permite la conexión de diversas antenas en tanto tengan una interfaz SMA. Se aprovecha por lo tanto esta versatilidad para intercambiar antenas con diferentes características de respuesta en frecuencia, activas y pasivas, etc., a saber:

a) **LP09650 de Ettus**. Es una antena direccional consistente en un array de dipolos (*log-periodic array*). El diseño especifica que su mejor rango de operación es entre 850-6500 MHz.

b) **Funke Home 5.0**. A diferencia de las anteriores, es una antena que puede funcionar en forma activa, precisando por lo tanto alimentación externa de energía, en este caso de 5V DC. Su mejor rango de trabajo es en UHF, entre 470 y 790 MHz.

c) **Ikusi modelo Flash HD NANO**. Es un poco más grande que el resto de la antenas, diseñada para recepción de TV Digital, y montaje exterior a través de un mástil. Su rango de frecuencias va desde los 470 a los 862 MHz.

d) **Voltech**. De dimensiones similares a la anterior, diseñada para recepción de señales de TV abierta y montaje exterior a través de un mástil. Su rango de frecuencias va desde los 45 a los 862 MHz, más específicamente: Canales 2 al 13 de VHF y Canales 14 al 83 de UHF.

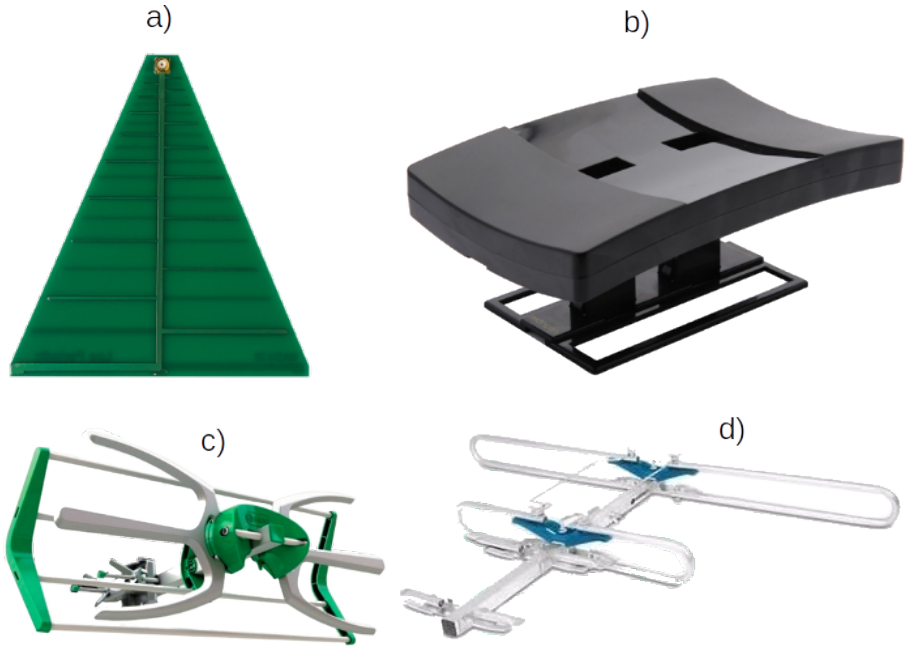


Figura 3.3: Antenas utilizadas: a) LP09650 de Ettus, b) Funke Home 5.0, c) Ikusi Flash HD NANO y d) Voltech

Las bandas de frecuencia donde mejor se desempeñan las antenas a), b) y c) de la Figura 3.3 difieren bastante de la frecuencia fundamental de emanación (2.3).

Sin embrago las pruebas con ellas resultaron satisfactorias, siendo la Ikusi la que mostró más versatilidad (distancia y resoluciones de pantalla captadas).

La antena que trabaja en el rango VHF que se utilizó (d) en la Figura 3.3), y en general las antenas que se comercializan en plaza para captar señales dentro de ese rango del espectro radioeléctrico, son de propósito general. Funcionan muy bien para recibir señales de TV abierta y están diseñadas para trabajar con mástil. En este trabajo no se logró una buena recepción con ella.

Se buscaron dos cosas para complementar el panorama en referencia a las antenas. Primero tener un estimativo de costos de una antena diseñada específicamente para los rangos de frecuencias de interés, i.e. desde 38.3 MHz a los 173,1 MHz para resoluciones desde 800 x 600 @ 60 Hz a 1920 x 1080 @ 60 Hz respectivamente, lo que resultó en una cotización muy por encima del presupuesto marcado para el trabajo[3]. En segundo lugar analizar someramente las características constructivas, especialmente las dimensiones, de las antenas que se pueden fabricar para ese rango de frecuencias, resultando en antenas con array de dipolos (log periodics) que alcanzan cerca de dos metros en su elemento más largo.

3.3.2. Software

Las herramientas de software se usaron tanto en la etapa de simulaciones de software (sección 3.4) como en la detección de las señales. En la primera etapa de pruebas de concepto y simulaciones se usaron tres herramientas: Octave, TempestSDR y GNU Radio Companion.

Octave: GNU Octave es un software libre de procesamiento numérico bien conocido en el ambiente académico, y compatible en un alto porcentaje de sus prestaciones con Matlab®. Cuenta con herramientas de procesamiento de imágenes muy sencillas, gráficas y herramientas de manejo de FFT, que permiten adelantar y visualizar las formas de las señales tanto en el espacio temporal como en el de frecuencias.

Por otro lado la ayuda en las comunidades de desarrolladores es muy amplia y el software se encuentra en la mayoría de los repositorios de las distintas versiones de Linux. Para este trabajo solo fue necesario cargar los paquetes adicionales: “control”, “general” y “signal”.

GNU Radio Companion: GNU Radio y GNU Radio Campanion son herramientas de software libre para procesamiento de señales de radio, que pueden ser utilizados junto con el USRP de Ettus como dispositivo externo receptor de tales señales de radio. El procesamiento de señales se hace a través de bloques conectables entre si mediante una interfaz gráfica del estilo diagrama de flujo (GNU Radio Companion, el *compañero* de GNU Radio). Al ser de código abierto permiten también modificar los bloques o crear bloques propios, aunque la biblioteca es tan amplia que para este trabajo no fue necesario tal desarrollo.

La herramientas de visualización de señales, tanto en el dominio temporal como en frecuencia son sumamente útiles y de fácil manejo.

[3]Encima de los USD 1000.

TempestSDR: Desarrollado por Martin Marinov, es un software que consta de dos partes, una librería y un programa host. La librería es la encargada de recibir la señal desde el hardware y decodificarla. Mientras que el host la controla a través de una API, y provee la interfaz gráfica. En la práctica son un único ejecutable. El software decodifica la señal en base a la amplitud de las muestras recibidas ($|x_R(nT_s)|$), y utiliza la autocorrelación para detectar las dimensiones de la resolución, como se mencionó en la sección 2.2.2.

Acepta como entrada, además de las señales captadas por el SDR, archivos. Esto permite postprocesar grabaciones de señales o tomar señales simuladas desde archivos. Esta última prestación es la que se usa como uno de los escenarios de simulación en las secciones 3.4.1 y 4.1.2.

3.4. Escenarios de simulación de emisión y espionaje

Las herramientas de software usadas, tanto GNU Radio como GNU Octave, permitieron realizar simulaciones que a los efectos de este trabajo sirvieron para aclarar aspectos conceptuales de la transmisión y generación de las señales, de la recepción y de la posibilidad de usar ecualización y su efecto, entre otros conceptos relevantes.

En la Figura 3.4 se ha representado el esquema de las simulaciones hechas, donde se construye por software desde la señal de la ecuación (2.7) para el caso VGA o (3.5) para HDMI, que sería la que se transmite por el cable, marcado como (2), hasta los elementos tanto de la recepción como de la demodulación.

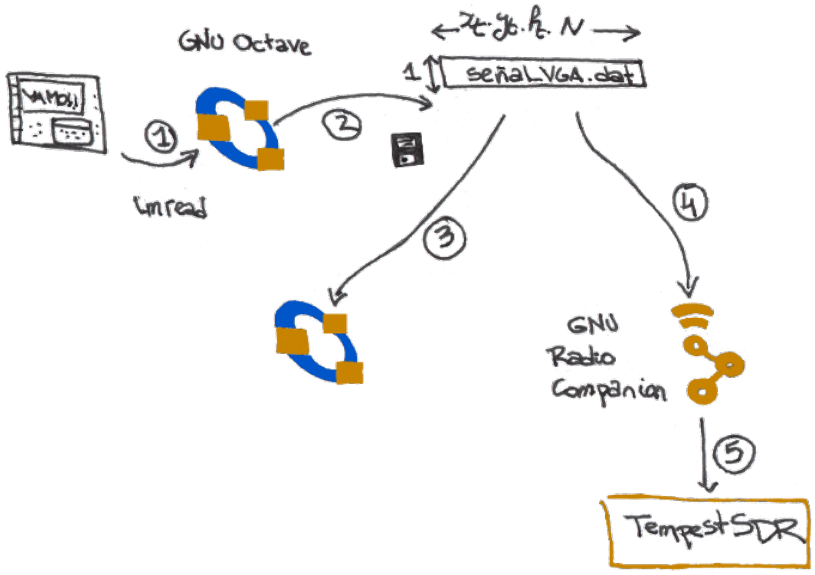


Figura 3.4: Escenarios de simulación. Desde Octave se carga la imagen que se espiará (1). Esa imagen se codifica como señal VGA o HDMI, resultando en un vector de largo $x_t y_t f_t N$ (2) (N es la cantidad de tramas). Esa misma señal, que no es otra que la de la ecuación (3.7) se procesa en Octave (3) o se levanta desde GNU Radio, (4), y mediante un archivo *fifo* de Linux, se levanta desde TempestSDR, (5).

A partir de dichas señales se pudieron construir dos escenarios de simulaciones, a saber:

- Escenario 1 (E1) ①→②→③ A partir de la señal generada por software se realizan las operaciones de la Figura 3.2 en Octave, agregando ruido, corrimientos en frecuencia, errores de fase, etc. y visualizando las imágenes tanto sin ecualizar como ecualizadas.

- Escenario 2 (E2) ①→②→④→⑤ Se toma la imagen generada por software en GNU Radio Companion desde un archivo. Las operaciones se hacen esta vez con los bloques de este software, lo que en cierta forma se asemeja más a un escenario real, y mediante un archivo *fifo* se "levanta" la salida desde el software TempestSDR. Este tipo de archivos se crea con el comando *mkfifo* de Linux, quien se encarga de este manejo tipo *pipeline* en forma totalmente transparente para el usuario. Primero se crea el archivo con este comando desde el terminal, se le indica a GNU Radio Companion que escriba en él, con el bloque *File Sink*, y por último se le indica a TempestSDR que ese archivo es su entrada (se sustituye la entrada del SDR en ese software por un archivo, opción muy versátil de este software de Marinov). GNU Radio comenzará a ejecutarse tan pronto comience TempestSDR.

Estas simulaciones permitieron aventurar aportes tendientes a mejorar los resultados del software desarrollado por Marinov, y oportunidades de procesamiento off line de las señales. Esto último se refiere a que no siempre la visualización en tiempo real es un requisito indispensable, por lo tanto, en algunos casos, se puede grabar la señal o las señales captadas, por ejemplo con GNU Radio, y procesarla con herramientas más poderosas que impliquen consumo de recursos computacionales que harían inviable el trabajo en tiempo real.

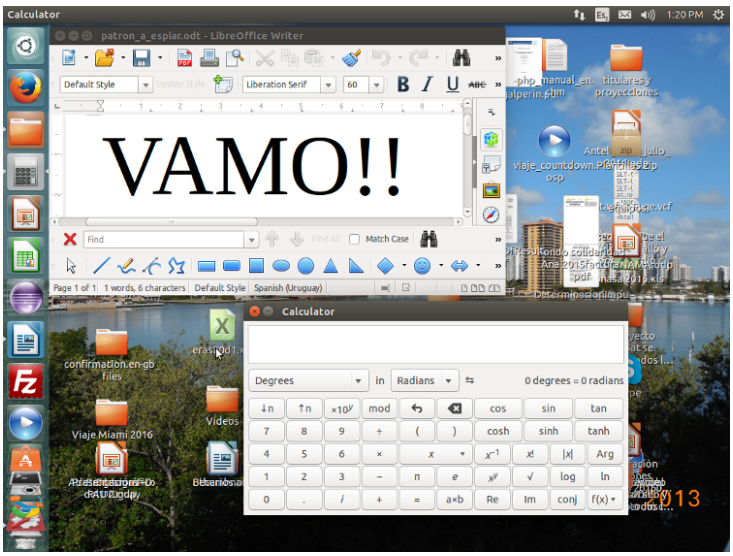


Figura 3.5: Imagen del monitor en la computadora objetivo.

A los efectos de tener una primera aproximación visual y gráfica de las señales emanadas a partir de las señales de video, se procedió de la siguiente forma:

a) Se toma una captura de pantalla del monitor espiado (Figura 3.5). Con esa imagen se genera la señal de video que viaja por el cable VGA o HDMI[4], esto es: se "rellena" con los píxeles de blanking según se detalla en la sección 2.2, se serializa y conforma con los pulsos que dan lugar a la señal PAM (Figura 2.3) o se codifica en el caso de la señal HDMI de acuerdo a lo explicado en la sección 2.4. Esto se realiza en Octave (Ⓒ en la Figura 3.4), por lo tanto como resultado de esto se tiene un vector donde cada valor (o n_b valores binarios en HDMI) representa uno de los píxeles, con información de la imagen o de sincronismo.

b) Como pulso conformador se usa un rectángulo, $p(t) = rect(t/T_p)$ para VGA o $p(t) = rect(t/T_b)$ para HDMI, como se vio en la sección 3.1.

c) La señal que emanará del cable será el primer o algún otro armónico de esa señal. Se elige trabajar con el primer armónico (pero el razonamiento no cambia si se eligiera cualquier otro), lo que sería, en la Figura 3.1, la porción magenta que está entre $1/2T_p$ y $3/2T_p$. Ese primer armónico es uno de los que podría captar la antena del espía, no el único obviamente pero si fuera a captar otro, habría que tener las consideraciones del caso, por ejemplo en cuanto a la atenuación introducida por el *sinc*.

d) Pretendiendo tener un patrón común con el cual comparar, aunque sea subjetivamente, los resultados de los distintos procesos de simulación y captación de las emanaciones, se utilizó siempre la misma figura en la computadora objetivo, la que se pretendía espiar. En ella se abrieron dos ventanas, una de un editor de texto donde se escribió con fuentes grandes (tamaño 66 pt) usando el editor Writer de LibreOffice©, y otra ventana con la aplicación Calculadora nativa de Ubuntu (Figura 3.5). El fondo de pantalla tiene además una imagen con follaje, lo que muchas veces se confunde con ruido, y resultó muy útil para evaluar el resultado del espionaje.

   Esto último sin perjuicio que se usen otras imágenes para evaluar comportamiento de la recuperación de ciertos patrones como en la sección 3.5.1 o situaciones reales y vulnerables como la de la sección 5.1.

3.4.1. Simulación de recepción de emisiones de señales VGA

A partir de las señales generadas por software en el esquema de la Figura 3.4 se simula la recepción de emisiones VGA y se las comparará con las emisiones y recepciones reales que se muestran en la sección 3.5 captadas por antenas, muestreadas por el SDR y visualizadas usando el software de la referencia [1], TempestSDR.

[4]Cabe recordar que la imagen color se divide en RGB, por lo tanto, hay que lidiar con la emanación de los tres pares de cables. La señal simulada puede ser una de las tres componentes, la suma de las tres, o alguna combinación de todas.

De esa manera se podrán cotejar los resultados y evaluar que tan válidos pueden resultar los escenarios simulados.

Los procesos de lectura de la imagen original desde un archivo en cualquiera de los formatos que maneja Octave (por ejemplo PNG), y escritura en formato VGA serial en un vector señalados por el punto (2) de la Figura 3.4 se realizan con un script para Octave disponible en el repositorio de este trabajo.

En primera instancia, todo el proceso de leer la imagen serializada, modularla, etc. hasta obtener la señal $x_R(nT_s)$, que simulan los procesos marcados desde los puntos (3) hasta (7) en la Figura 3.2, y como parte (3) en el esquema de simulación de la Figura 3.4 se realizan también con apoyo de un script para Octave disponible en el repositorio.

Los resultados del escenario E1 se reflejan en la Figura 3.6, donde se ve el texto recuperado, o por lo menos sus bordes (lo que se explicará en algunas secciones más adelante), se distingue la ubicación de los íconos, la ventana con la calculadora y su números, parte del follaje de fondo (solo sabiendo previamente que es follaje) y los edificios de ese paisaje. Los bordes horizontales no se detectan, lo que se puede apreciar tanto en las ventanas de las aplicaciones como en los edificios de la imagen de fondo de pantalla.

Figura 3.6: Simulación de la imagen VGA recuperada, $|x_R|$ en la Figura 3.2, escenario E1 de la Figura 3.4.

Luego se trabaja con el escenario E2 en el esquema de la Figura 3.4, que se encarga de simular entonces el proceso de recepción con GNU Radio Companion y el software TempestSDR.

Los resultados se muestran en la Figura 3.7, la cual es una captura de pantalla hecha desde el mismo TempestSDR. Cabe resaltar que la imagen se aprecia más comprimida en sentido horizontal, o más "alargada" producto de la forma de sincronización y detección del software. Nuevamente se nota la ausencia de bordes horizontales.

Las imágenes obtenidas en los dos escenarios no tienen elementos que las diferencien en forma sustancial, por lo tanto se puede inferir que ambos escenarios arrojan resultados similares.

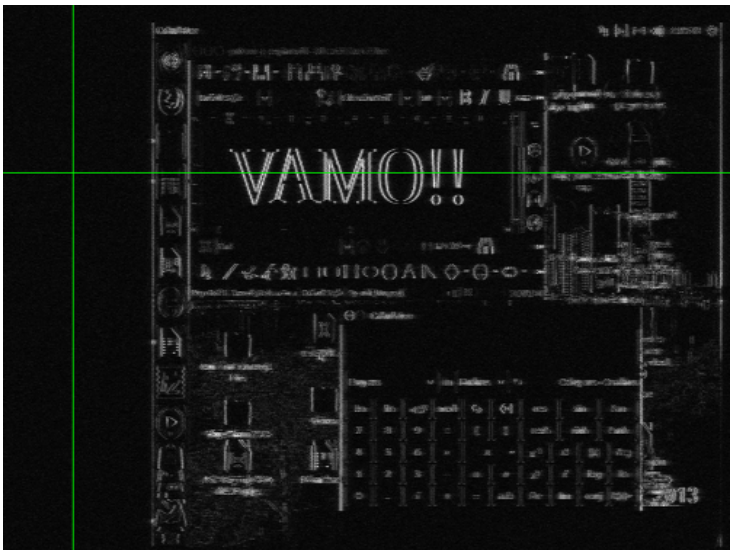


Figura 3.7: Simulación de la imagen VGA recuperada, $|x_R|$ en la Figura 3.2, usando el escenario E2 del 3.4. Las líneas verdes son prestaciones del software TempestSDR para indicar que está trabajando en modo de sincronización (corrigiendo los errores de frecuencia) automática.

Nota: En los dos escenarios de simulación de esta sección se trabajó con resoluciones de 800x600 @60Hz, solo para optimizar los tiempos de ejecución de los scripts. Esto también cambia el escenario de propagación pues los armónicos de escenarios reales serán de más alta frecuencia en tanto se suelen usar resoluciones más altas. De hecho se ensayaron pruebas con resoluciones más altas y a los efectos prácticos no existen diferencias sustanciales.

3.5. Detección de emisiones de señales de video VGA

En esta sección se muestran los resultados de escenarios de espionaje propiamente dicho, lo que tiene como primer propósito compararlos con las simulaciones de la sección 3.4.

Los equipos usados para espiar se describen en la tabla 3.1, mientras que el equipo espiado varió entre la detección de señales VGA y HDMI (un monitor de PC en el primer caso y una TV HD en el segundo), pero en ambos casos mostrando la misma imagen y usando la misma resolución.

Hardware	Software
Antena: Ikusi modelo Flash HD NANO	TempestSDR en Ubuntu
SDR: USRP B200 de Ettus	
PC Lenovo™ Ideapad™ 100	
Conexión PC → SDR (USB 3.0)	

Tabla 3.1: Equipo y software usado para espiar.

En el caso de espionaje de señales VGA, con el equipamiento usado, se puede decir que se configuró un escenario bastante realista de espionaje, no así en el caso HDMI por la proximidad de la antena al equipo espiado.

Con el objetivo de reproducir los experimentos realizados por Marinov en la Universidad de Cambridge [1] en primera instancia y de validar los resultados de las simulaciones de software por otro, se sintonizaron emanaciones provenientes de un cable VGA que conectaba un monitor, AOC™ de 19" a una computadora de escritorio. La antena se situó a una distancia de más de 3m de la conexión del cable al monitor. En esa computadora se estaba visualizando la ventana del editor de texto y la calculadora de Ubuntu (Figura 3.5).

El escenario de espionaje se observa en la Figura 3.8. Se configuró en una habitación donde se ubicó la PC y el monitor, objetivos de espionaje, y la antena (Figura 3.3 c) se puso justo afuera de la habitación sin línea de vista con el monitor, el cable VGA o la PC. Las paredes de la habitación son de mampostería y el piso de madera flotando unos 5cm sobre la losa. El monitor está ubicado sobre un escritorio y la torre de la PC se ubicó en el piso. Todo en un entorno rodeado de más equipos electrónicos encendidos tales como: routers de fibra óptica, routers con Wi-Fi activa, otras computadoras personales, constituyendo un ambiente con mucho ruido en diferentes partes del espectro.

Figura 3.8: Escenario de espionaje "visto" desde el lugar de la antena. La flecha roja indica el lugar del monitor espiado.

La antena utilizada, si bien portátil, no es fácil de ocultar, ya que mide aproximadamente unos 30x53x20 (cm) y pesa un poco menos de 1kg. La conexión desde la antena al SDR, se hizo un con cable de unos 5m, con $Z_0 = 75\Omega$, produciéndose un desbalanceo respecto al equipo SDR ya que este tiene una impedancia característica $Z_0 = 50\Omega$. Este esquema ubica a la computadora espía a unos 8m (5 + 3) de la computadora espiada.

Se pudo captar e interpretar el texto (grande) desplegado en la pantalla de la computadora espiada como se muestra en la Figura 3.9. Donde el texto no aparece en el mismo lugar absoluto de la pantalla, obviamente por temas de sincronismo tanto vertical como horizontal, apreciándose incluso ambos espacios de borrado o blanking. Esto se puede ajustar en el software TempestSDR pero se prefirió incluir

esta imagen que parece más demostrativa de las señales captadas.

Otros ajustes manuales de TempestSDR permiten reducir el tiempo de captación basado en la información de correlación de la señal que el mismo muestra en tiempo real.

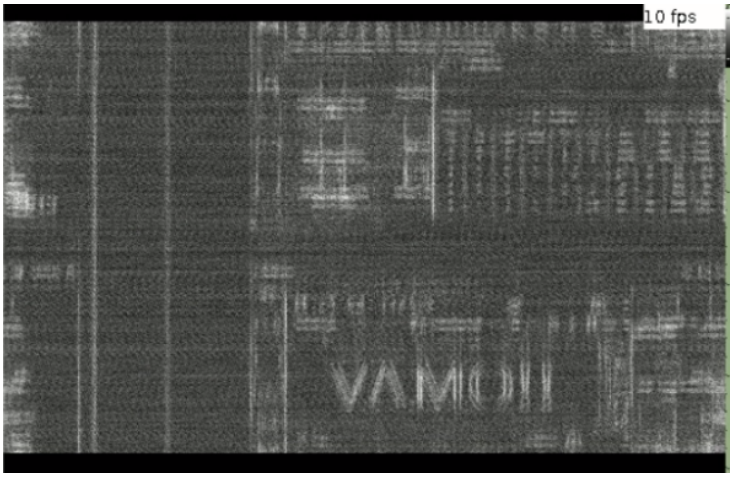


Figura 3.9: Captación de una ventana activa de un procesador de texto, $f_s = 40MHz$.

Posteriormente se desplazó la ventana de la Calculadora de forma tal que tape parcialmente el texto y se logró captar la imagen incluso en forma más nítida como se muestra en la Figura 3.10.

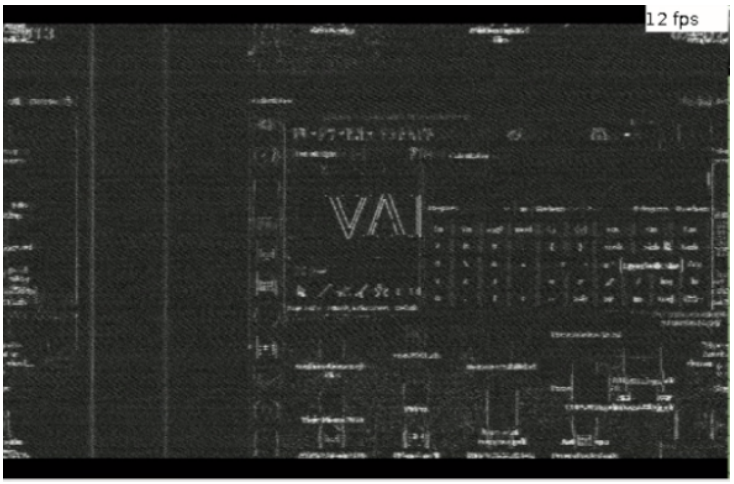


Figura 3.10: Segundo escenario, la ventana de la aplicación "Calculadora" de Ubuntu se puso frente a la ventana del texto, tapándolo parcialmente, $f_s = 40MHz$.

La posición de escritura dentro del editor de texto, indicada por el parpadeo de una línea vertical también se aprecia, al igual que los caracteres que se van escribiendo, siempre que estos sean grandes.

Al menos en las pruebas hechas en el escenario descrito, los íconos de la barra de herramientas del editor, o del escritorio del usuario, no se distinguen. Solo se ven como un espacio borroso.

La frecuencia fundamental de la emisión de este escenario corresponde a 38,3 MHz, ya que la cantidad de píxeles del monitor, para una resolución de 800x600 @60Hz, es, agregándole los píxeles de relleno y sincronización [36], de 1024x624 esto es 638976 por trama. Siendo la frecuencia de las tramas de 60 por segundo f_0, de acuerdo a la ecuación (2.3), resulta 1024x624x60=38338560 Hz. La sintonización del SDR se hizo en la frecuencia fundamental y en varios armónicos, no existiendo diferencia significativa hasta el quinto armónico inclusive.

Se pudieron captar emanaciones para otras resoluciones más altas, por ejemplo: 1024x768 @ 60Hz, pero a los propósitos de la comparación con las simulaciones resulta más práctico hacerlo con baja resolución ya que los tiempos de procesamiento, sobre todo de Octave, se incrementan sustancialmente con el aumento de la resolución.

La diferencia en la nitidez de las dos imágenes captadas no guarda relación directa con el hecho de que una aplicación aparezca delante de la otra, sino a que la orientación de la antena cambió con todas seguridad levemente de una captura a la otra.

Se puede concluir entonces que las simulaciones del espionaje donde la señal es generada con Octave (y procesada con GNU Radio) se parece mucho a lo que se ve en espionaje de emanaciones reales. Esto se convierte en una herramienta que habilita la generación de señales de manera offline para trazar estrategias de procesamiento de la señal sin necesidad de lidiar con las dificultades de captación con antenas. Ensayar y mejorar dichas estrategias en el ambiente simulado, para luego trasladarlas al escenario real.

3.5.1. Efecto Blurring en VGA

En esta sección se discutirán los efectos que impone el filtro pasabajos del SDR cuya expresión quedó plasmada en la ecuación (3.7):

$$x_R(nT_s) = \left[x(t)e^{-j2\pi f_p t}\right] * h_{lpf}(t)\Big|_{t=nT_s}.$$

Para ello se parte de la expresión de x_R en la ecuación (3.14),

$$x_R(nT_s) = \sum_{i=-\infty}^{\infty} x_i g(nT_s - iT_p),$$

donde se aprecia que cada muestra que entrega el hardware SDR, si bien contiene la información del valor del píxel x_i, está contaminada por los valores de otros píxeles ponderados por $g(t)$.

El efecto más notorio sobre la recuperación de la imagen es la falta de nitidez, pues el píxel recuperado no representará su valor original sino un "promedio" de los valores de los píxeles adyacentes. La adyacencia espacial a la que se hace referencia se da a lo largo de cada línea de la trama. Es decir, dada la forma de conformación de la imagen como se mencionó en la sección 3.1, dos píxeles pueden ser adyacentes en tanto están en la misma columna pero se transmitirán separados

un tiempo igual $p_H T_p$, por lo tanto no serán adyacentes temporalmente. Cosa que si ocurre con dos píxeles que sean adyacentes y estén en la misma fila. Por lo tanto, el "promedio" es entre píxeles de la misma fila[5].

En la Figura 3.11 se representa un muy grosero esbozo de la forma de la parte real e imaginaria de $g(t)$ calculado a partir de la ecuación (3.11) y para dos valores de frecuencia de corte del LPF ($rect(f/f_{cutoff})$), donde se puede ver que hay una gran cantidad de puntos en torno al centro que contribuyen a la sumatoria de forma significativa cuanto más pequeño sea el ancho de banda del LPF (i.e f_{cutoff}).

Sin perder de vista que $g(t)$ es una señal compleja, por lo tanto con fase, que introduce aún más errores que los que se pueden percibir en la figura, en especial en la componente imaginaria de $g(t)$ producida por el filtro de menor ancho de banda.

En la señal de esa figura usada como ejemplo, y para el filtro cuyo módulo de respuesta en frecuencia se representa con negro, el 3,3 % de los píxeles que más contribuyen lo hacen con el 31 % del peso total de la sumatoria de los valores absolutos de g de la ecuación (3.14), mientras que el caso de la respuesta representada en verde, se necesitan el doble de puntos (6,7 %) para alcanzar el mismo porcentaje de peso sobre el total.

En el área de procesamiento de imágenes por computadora a este efecto, a veces provocado mediante técnicas de filtrado, se lo conoce como *blur* o *blurring*. El efecto perseguido mediante esas técnicas es justamente lo que acá causa la pérdida de definición, por ejemplo para detectar bordes, ya que aplicando técnicas de blurring se reducen las cantidades de bordes quedando solo los que tienen mayores diferencias de luminiscencia, o para minimizar la percepción de ruido.

[5]Salvo lo primeros (o últimos) píxeles de cada fila que se promediarán con los píxeles de relleno.

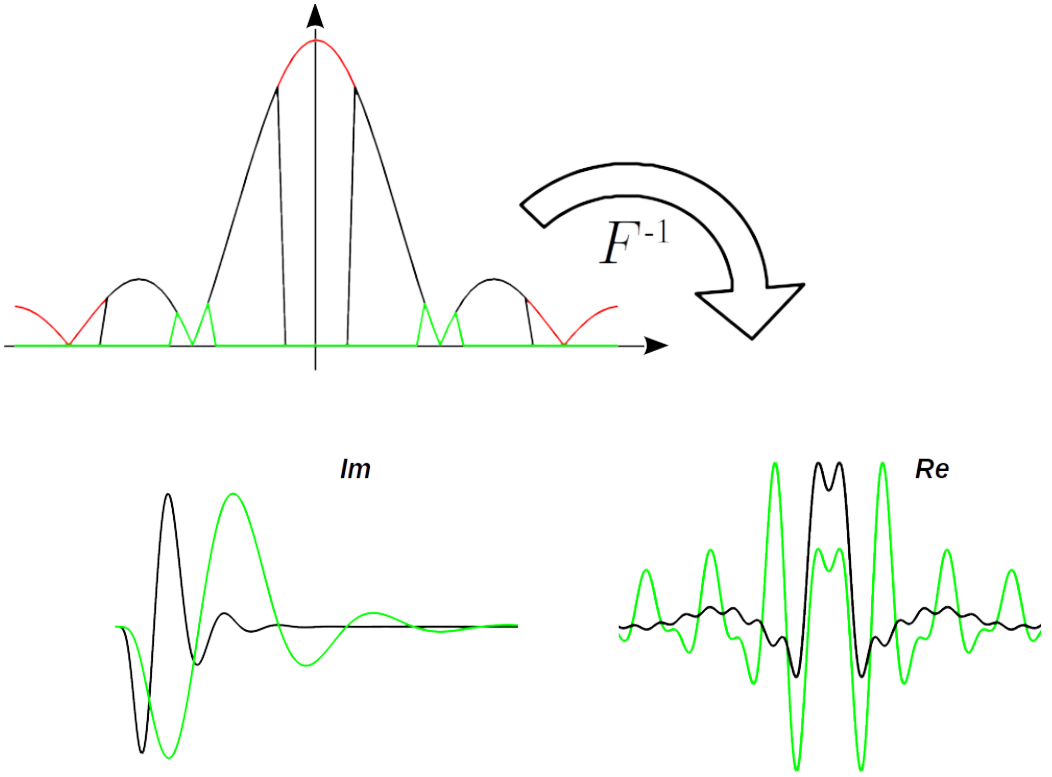


Figura 3.11: Arriba: espectros de $P(f)$ en rojo, y dos versiones de $P(f - f_p)rect(f/f_{cutoff})$ en negro para un $f_{cutoff} = 25MHz$ y en verde para $f_{cutoff} = 10MHz$, resolución de pantalla 800x600 @60Hz. Abajo las respectivas $\mathbb{R}e(g(t))$ e $\mathbb{I}m(g(t))$ normalizadas.

Nota: La imagen es ilustrativa también en el sentido que se mencionan LPF y en realidad la porción de espectro que se muestra es en el primer armónico. Lo correcto es decir que luego de la modulación (punto (5) en la Figura 3.2), el espectro se trasladará, quedando los espectros allí representados en banda base, esto es: el primer corte por cero en f_p del espectro original quedará en $f = 0$ y una vez ahí se pasa por el LPF.

El mismo efecto, esta vez no deseado, se ve también en capturas de secuencias de imágenes donde la transición de un movimiento de una trama a otra es rápida.

Este efecto, y en línea con lo mencionado en referencia a la detección de bordes, es justamente lo que hace el filtro pasaaltos que en definitiva es $g(t)$. Es por eso que las imágenes de TempestSDR y sus simulaciones muestran predominantemente bordes, i.e: letras huecas. Teniendo en cuenta que el promedio se hace en sentido horizontal, por lo tanto se comporta como un detector de bordes verticales. Y en el caso de líneas genéricas[6]: detecta su componente vertical, el borde vertical de las mismas.

Una prueba muy sencilla, cuyo análisis comienza aquí y culminará en la sección 4.3 cuando se vea la ecualización, consiste en analizar la visualización de una imagen con rectángulos negros sobre fondo blanco, y uno con una transición negro→gris→blanco (Figura 3.12).

[6]Ni horizontales ni verticales.

Es notoria la detección de los bordes verticales, y la desaparición, por lo menos a simple vista, de los bordes horizontales (Figura 3.13). En el caso de la segunda línea vertical, al ser muy fina, los dos bordes verticales detectados se confunden en uno solo.

Esto se explica por la forma de $g(t)$ que incide en el peso relativo de los puntos sucesivos horizontales (recordando que los puntos adyacentes en el tiempo son adyacentes en el sentido horizontal).

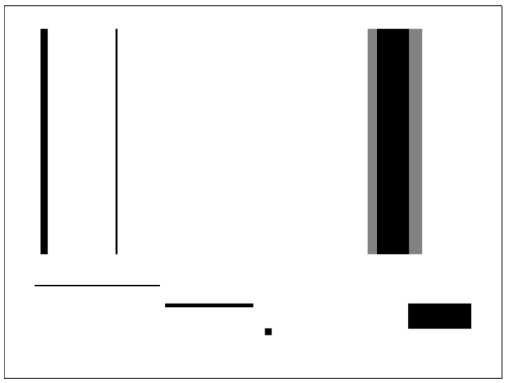


Figura 3.12: Imagen patrón para analizar la detección de bordes.

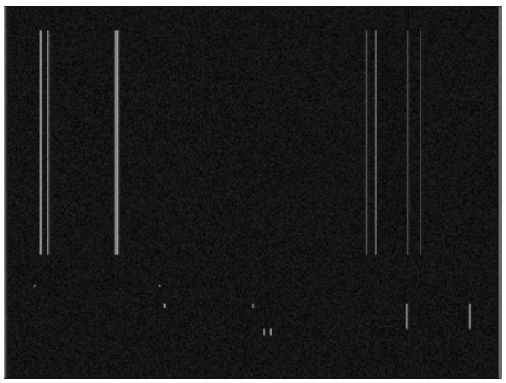


Figura 3.13: Detección simulada de la Figura 3.12 en TempestSDR con una frecuencia de corte en el LPF de $f_{cutoff} = 10MHz$.

Hacer una simulación con un filtro que tuviera una frecuencia de corte exageradamente alta para los valores que maneja el hardware SDR que se ha utilizado, llevaría a ver más detalles de la imagen cuyo análisis no sería realista, por lo menos en el escenario de este trabajo.

3.5.2. Efecto del corrimiento de frecuencia

Para realizar las operaciones que llevaron a deducir la ecuación (3.14), se asumió que la frecuencia a la cual se sintoniza el receptor superheterodino situado entre los puntos (3) a (5) de la Figura 3.2 era igual a $1/T_p$. Pues bien, esto no siempre tiene que ser necesariamente el caso, ya que no sólo el SDR carece de un reloj extremadamente preciso, sino que además se deben considerar las propias tolerancias que la norma VESA [36] contempla.

Por lo tanto, se tratarán aquí los efectos de una sintonización imperfecta. Esto se tiene en cuenta considerando un corrimiento de frecuencias Δf, que cambia la frecuencia de sintonización a $1/T_p + \Delta f$.

Primero que nada recordar que lo que ingresa al LPF, punto (5) de la Figura 3.2, es la señal de la ecuación (3.9) sin el *rect* que representa justamente al LPF, es decir:

$$x_{in-lpf}(t) = \mathcal{F}^{-1}\Big\{P(f - f_p)Xs(f)\Big\}. \tag{3.15}$$

Contemplando el error de frecuencia Δf en la sintonización, lo que ingresará al LPF es:

$$x_{in-lpf}^{'}(t) = \mathcal{F}^{-1}\Big\{P(f - f_p - \Delta f)Xs(f - \Delta f)\Big\}. \tag{3.16}$$

De las ecuaciones (3.15) y (3.16) se deduce que:

$$\boxed{x_{in-lpf}^{'}(t) = x_{in-lpf}(t)e^{-j2\pi\Delta ft}}. \tag{3.17}$$

Esta ecuación indica que al LPF ingresa una señal que estará girando en el plano complejo, o sea, se verá como un giro de las muestras de x_R en dicho plano, lo que se agrega a la ISI vista en la sección anterior. Sin embargo y en tanto el software TempestSDR toma $\left|x_R(nT_s)\right|$, estos corrimientos no lo afectan.

La ecuación (3.17) permite seguir operando si se asume que $2\pi\Delta ft$ varía lentamente. Continuando entonces bajo esa hipótesis se tiene que:

$$x_R{}'(nT_s) = \left\{x_{in-lpf}(t)e^{-j2\pi\Delta ft}\right\} * \mathcal{F}^{-1}\Big\{rect(f/f_{cutoff})\Big\}\Big|_{t=nT_s}. \tag{3.18}$$

Pudiendo "sacar" la exponencial fuera de la convolución bajo la hipótesis mencionada [37]:

$$x_R{}'(nT_s) = e^{-j2\pi\Delta ft}\left\{x_{in-lpf}(t) * \mathcal{F}^{-1}\Big\{rect(f/f_{cutoff}\Big\}\right\}\Big|_{t=nT_s}, \tag{3.19}$$

y usando las ecuaciones (3.14) y (3.15) se obtiene:

$$\boxed{x_R{}'(nT_s) = e^{-j2\pi\Delta ft}x_R(nT_s)} \tag{3.20}$$

Esta ecuación, si bien tiene la misma consideración del giro en el campo complejo de la señal respecto al caso sin corrimiento de fase que la ecuación (3.17), lo refleja a la salida del SDR.

Como se vio en la sección 3.3.2, el software TempestSDR toma el módulo de las muestras recibidas, y de acuerdo a la ecuación (3.20), los errores de frecuencia le son indiferentes ya que $|x_R{}'(nT_s)| = |x_R(nT_s)|$.

3.5.3. Pulso conformador de píxeles

El pulso conformador con el cual se analizó la señal en la sección 3.1 es un pulso NRZ ideal. En la práctica el pulso dista bastante de ser ideal. El pasaje de niveles bajos a altos de voltaje no será instantáneo sino que será un valor medible y cuyos límites están establecidos por la norma, llamado *rise time*, lo mismo que el tiempo de bajada del voltaje (*fall time*), podría tener *overshooting* (y/o *undershooting*) y éste a la vez puede demorar en desaparecer, entre otras cosas que lo apartan de lo ideal.

Sobre las formas del pulso y sus TF

La norma [36] establece tolerancias para esos valores medidos en el peor caso: pasando del nivel más bajo de voltaje de la señal PAM al más alto y viceversa. Algunos de los valores, en tanto son tiempos, dependerán en términos absolutos de la resolución con la que se trabaje, por lo tanto para evitar ambigüedades se expresan en términos relativos. Por ejemplo: el *rise time* (medido desde el 10 % del voltaje mínimo estable hasta el 90 % del voltaje máximo estable) debe demorar menos que el 25 % de la duración del píxel, el *overshooting* y el *undershooting* no deben superar el 12 % medidos desde el voltaje máximo y mínimo estables respectivamente, y deben "desaparecer" antes de transcurrido el 30 % del tiempo de duración del píxel. Este apartamiento del pulso ideal se analizó en forma práctica midiendo la forma de los mismos directamente en la interfaz VGA como se puede ver en la Figura 3.14, que representa un único pulso, cuya respuesta temporal se obtuvo con una imagen de un píxel blanco sobre fondo negro. Los dos pulsos observados (rojo y azul en la figura), fueron captados en un osciloscopio directamente desde el cable VGA usando un adaptador VGA⇔BNC.

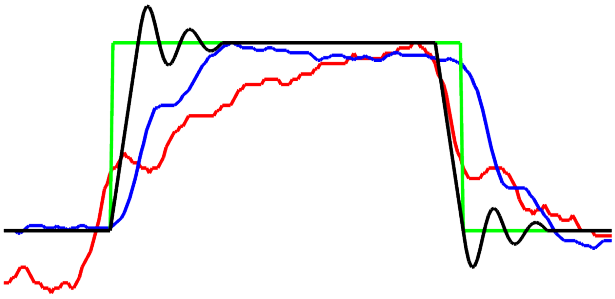


Figura 3.14: Representaciones de diferentes pulsos de conformación. En azul y rojo tomados de la interfaz VGA de sendas PC, ambas con tarjeta de video on board, Intel®y genérica respectivamente.

El osciloscopio permitió grabar los valores de los pulsos en formato csv, los cuales se cargaron en Octave para graficarlos y ver sus componentes de frecuencia. Para poder permanecer dentro del rango de frecuencias de respuesta del osciloscopio (Tektronix®TDS2000C, ancho de banda de 200MHz) se trabajó con una resolución de 800 x 600 @ 60Hz. Además se representan en la figura el pulso ideal en verde y en negro un pulso con over y under shooting.

Se puede percibir casi sin hacer medida alguna que el pulso rojo demora mucho en alcanzar el valor máximo, si es que lo alcanza, por lo que su *rise time* no cumple con las tolerancias impuestas por la norma, sin embargo a simple vista la imagen en el monitor no mostraba deterioro. Pero vale resaltar que al intentar elevar la resolución usando la misma configuración de cables y tarjeta de video que generó el pulso rojo, no fue posible, indicio que la configuración estaba al límite de rendimiento aún con la resolución tan baja.

En la Figura 3.15 se muestra otro ejemplo del apartamiento de la forma del pulso conformador ideal. Esa figura es una impresión de la pantalla del osciloscopio. Se nota el *overshooting* al comienzo del último píxel blanco, el *undershooting* al final del mismo. Se nota claramente también que ambos demoran en terminar, *rise time* y *fall time*, tienen mucho ruido, etc.

Algunos fabricantes de tarjetas de video, trabajan con una solución de compromiso entre un *rise time* rápido a costa de un mayor *overshooting*, a los efectos de mejorar la definición de las imágenes, efecto conocido como Corrección de Aper-

tura [42] .

Se nota también en la Figura 3.15 que la tarjeta de video ha conformado de diferente forma la transición negro→blanco. En la primera transición no hay overshooting, mientras que en la segunda sí lo hay. Hay un pico invertido en los niveles altos de voltaje en el medio de dos píxeles blancos sin explicación coherente aparente. Todo esto se expone aquí para tener presente que el pulso no es uniforme, se conforma en forma diferente según el hardware, pero aún así las imágenes se ven muy bien. Esto en parte a la robustez de los monitores y a veces a la falta de capacidad de discernimiento del ojo humano.

Figura 3.15: Señal R del cable VGA correspondiente a 2 píxeles blancos seguidos por un píxel negro seguido de un píxel blanco, para una resolución de 800x600 @60Hz.

Dados estos alejamientos del comportamiento ideal, importa entonces tener una cierta idea de qué tanto afecta este alejamiento observado en el dominio de las frecuencias. Con ello se podrá inferir qué tanto podrían variar o apartarse ciertos comportamientos, en especial los referentes a propagación, respecto a aquellos con los cuales se trabajó en las secciones precedentes y las propuestas del capítulo 5. Para ello se grafican las TF de las cuatro señales de la Figura 3.14 y se muestran en la Figura 3.16.

Si bien se puede percibir un leve corrimiento en frecuencia, se destaca la atenuación que sufren los pulsos no ideales en los armónicos, los que se propagan. El primero de estos efectos podría considerarse análogamente a como se como se hizo en la sección 3.5.2 con el corrimiento en frecuencia de la sintonización. Mientras que el segundo repercute en una menor potencia (área bajo las gráfica) en particular en torno al primer armónico, qué es lo que se estuvo captando. Por lo tanto hay menos potencia de transmisión, pero ninguno hace perder las generalidades tomadas en las simulaciones.

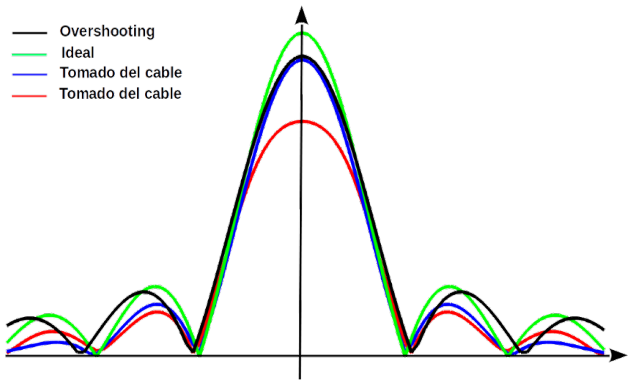


Figura 3.16: TF de los pulsos de la Figura 3.14 respetando los mismos colores usados, y recortando la visualización a los primeros lóbulos.

Al mismo tiempo cabe resaltar que las formas del pulso, sobre todo los simu-

lados no siempre se conservan pues dependen fuertemente de los valores de las transiciones de luminiscencia: $|x_i - x_{i+1}|$. Esto es: si ese valor es pequeño en comparación con el máximo (0.7V) es probable que no haya overshooting. Tampoco habrá undershooting si $x_i \leq x_{i+1}$.

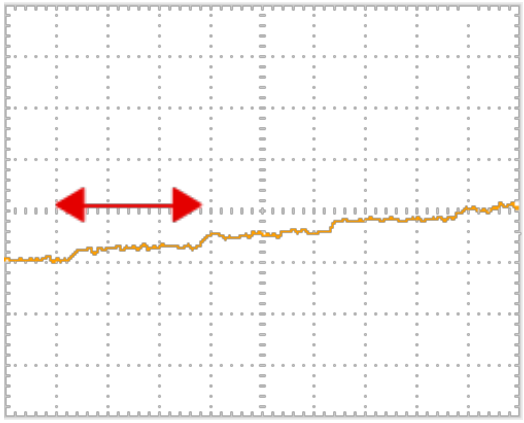


Figura 3.17: Progresión de la luminiscencia en VGA vista en el osciloscopio, donde la flecha roja indica la duración de un píxel.

En la Figura 3.17 se muestra la señal VGA en el caso de un aumento progresivo de los niveles de blanco, donde se ven tres píxeles enteros, y se nota que no hay undershooting, lo que es razonable, pero la presencia de overshooting es confusa, pareciendo que lo hay en unas transiciones y no en otras.

Resta tener en cuenta las mismas consideraciones que se hicieron en la sección 3.5.1 respecto a la forma de $g(t)$ en la ecuación (3.14) para estos pulsos, recordando que los pulsos deben "pasar" por el LPF del SDR.

Entonces se toman las respectivas respuestas en frecuencias de los pulsos ilustradas en la Figura 3.16, se las filtra con diferentes pasabajos, lo que dará idea de esas formas y cómo éstas hacen pesar los valores de los píxeles adyacentes.

En la Figura 3.18 se muestra la forma de los pulsos de la Figura 3.14 luego de haber sido detectados, bajados a banda base y haber pasado por el LPF de $10MHz$ en recepción, respetando los mismos colores.

Si bien son muchas las conclusiones que se pueden sacar de esas representaciones, vale destacar la falta de simetría de los pulsos. En todos pesan mucho los píxeles inmediatamente adyacentes. El pulso ideal, junto con el representado por el color azul, son quienes menos peso relativo proporcionan a la muestra del propio píxel, actuando entonces en forma más "promediadora", si cabe el término, que el resto de los pulsos. Al mismo tiempo se percibe que los cruces por cero se separan bastante más que en el caso de los pulsos sin filtrar.

Se repite la estimación anterior pero con un filtro LPF con mayor ancho de banda, el doble que el anterior donde el comportamiento (ver Figura 3.19 a)) en los tiempos adyacentes al píxel es bastante similar salvo una pronunciada asimetría en el pulso rojo, y también se aprecia que el peso de las componente más alejadas se va separando.

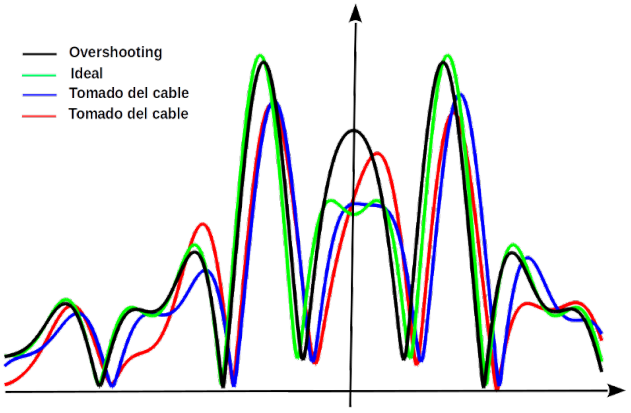


Figura 3.18: Diferentes $g(t)$ para una $f_{cutoff} = 10MHz$.

En la misma figura, esta

vez en la imagen b), se compara el mismo pulso, que ha sido representado con azul en la parte a) de esta y en la Figura 3.18, esta vez en cyan. Allí se ve el mayor peso de los píxeles más cercanos, y una "separación" de los adyacentes.

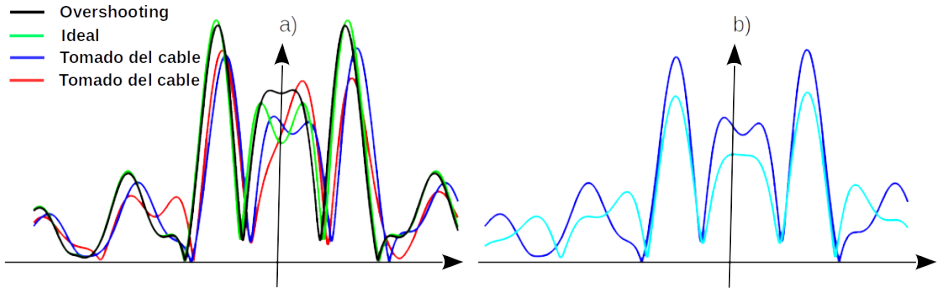


Figura 3.19: a) Diferentes $g(t)$ para una $f_{cutoff} = 20MHz$, b) Comparación del mismo pulso, azul en a), para $10MHz$ en cyan y $20MHz$ en azul.

Visualización del impacto de los pulsos

En la sección anterior se hicieron algunas conjeturas en referencia a las formas de los pulsos en base a las observaciones hechas en el osciloscopio y a las tolerancias de la norma.

Ahora bien, y como se mencionó también anteriormente, no se puede afirmar que una tarjeta de video, por lo menos las observadas, tengan una conformación única del pulso para todos los valores de píxeles, o mejor expresado para todos las diferencias entre píxeles adyacentes: $|x_i - x_{i+1}|$. No se puede siquiera asegurar que existiendo una superación de ese valor absoluto de un umbral haya por ejemplo siempre overshooting (ver Figura 3.17).

Si ese fuera el caso, existe un impulso tentador a escribir el pulso conformador como algo de la forma:

$$p(t) = rect(t/T_p)\Big\{1 + (V_{os}/V_{max})(x_{i+1} - x_i)e^{-at}cos(2\pi(4/T_p)t)\Big\}. \qquad (3.21)$$

Donde para contemplar la norma debería ser $a \approx 0{,}184$ para que el overshooting baje una vez transcurridos el 25 % de T_p, $V_{os} = 0{,}12$ para que no se supere el 12 % de overshooting, etc.

Incorporar esta forma de $p(t)$ no solo implicaría un procesamiento más potente en la detección pues hay que estar constantemente adquiriendo el píxel siguiente para volver a estimar el actual o volver a calcular el actual en base al píxel anterior, por lo que la hace impracticable. Del mismo modo usar un pulso con overshooting para conformar todos los píxeles tampoco sería lo más ajustado a la realidad como ya se mencionó.

Por lo tanto, se propone un escenario de simulación que sea un compromiso entre lo realizable con tiempos de procesamiento similares a cuando se consideró el pulso ideal, y que contemple alguna de las características más interesantes o vulnerables a los efectos del espionaje. Con esa premisa se simula una detección con pulsos con overshooting como el representado con color negro de la Figura 3.14, sabiendo que es altamente probable que esté presente solamente en saltos grandes de luminiscencia como en bordes.

Los resultados se ven en la Figura 3.20, donde se muestran porciones de capturas del patrón de la imagen 3.12. Allí las figuras superiores son las generadas con pulsos con overshooting y abajo con un pulso rectangular. Las diferencias son imperceptibles para el escenario E1, Figura a) (simulación en Octave), y con líneas apenas más definidas en el caso del escenario E2, Figura b).

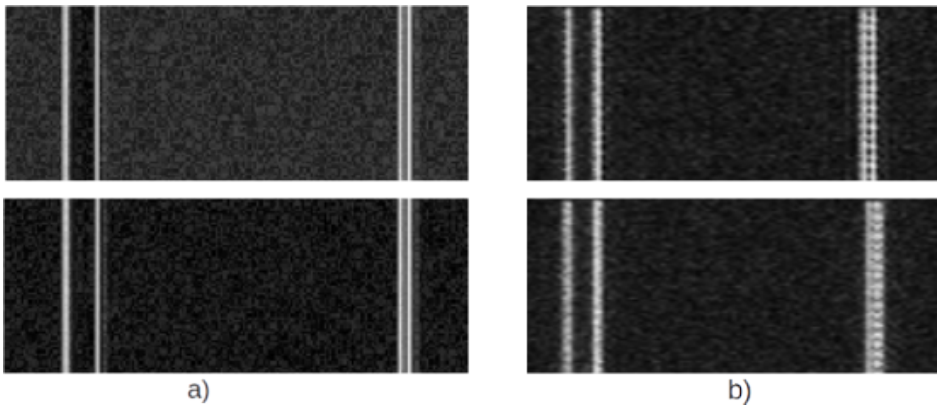


Figura 3.20: Comparación del efecto del overshooting en escenario E1 en a) y escenario E2 en b). Las dos imágenes superiores corresponden al pulso con overshooting, mientras que las dos de abajo al pulso rectangular.

Este comportamiento es esperable, dado el LPF con bajo ancho de banda como el que se usó ($f_{cutoff} = 10MHz$), lo que habilita a estimar comportamientos con los pulsos de la Figura 3.18, donde se ve que el peso relativo para el pulso negro (con overshooting) del píxel iT_p es mayor que el mismo peso relativo para el pulso verde (pulso ideal).

3.6. Representatividad de las simulaciones por software

Más allá de las certezas en la representatividad formal o matemática de las simulaciones hechas por software, es decir: en tanto las ecuaciones son claras y la construcción de bloques de software que reflejen el comportamiento del hardware SDR es casi lineal, vale la pena en este punto apreciar y comparar, por lo menos subjetivamente, las simulaciones de las secciones 3.4.1 y las detecciones reales de la sección 3.5.

Junto con tales certezas y la similitud de las imágenes obtenidas en ambos casos, se abre la posibilidad de continuar en el próximo capítulo con las propuestas de mejora y comprensión más cabal de las señal, que se podrán tangibilizar en las pruebas de software.

Por ejemplo, TempestSDR toma el módulo de las señales recibidas, esto es, $|x_R|$ cuando se podría realizar un proceso de ecualización como se muestra en la Figura 3.2 entre las señales de los puntos marcados como (7) y (8) de la misma. Ésta y otras consideraciones son las que se verán en el capítulo siguiente. Algunas serán mostradas en ecuaciones y en otras se complementará con simulaciones en software.

Esta página ha sido intencionalmente dejada en blanco.

Capítulo 4

Contribuciones

Este capítulo extiende a la interfaz HDMI el análisis de los resultados vistos hasta ahora, a partir de las ecuaciones que representan las señales de video desarrolladas en el capítulo 3 para el caso VGA.

Se verán las limitaciones en el muestreo y sus efectos, y al igual que en el capítulo anterior, blurring, errores en frecuencia y se proponen algunas mejoras.

Cabe también resaltar que las imágenes obtenidas a partir del espionaje de la interfaz HDMI, como la de la Figura 4.1, fueron obtenidas utilizando el software TempestSDR, que está concebido para obtener imágenes VGA. Esto es, el software hace la reconstrucción de la imagen a partir del módulo de las componentes digitales en cuadratura $x(kT)$ e $y(kT)$, i.e. $\sqrt{x(kT)^2 + y(kT)^2}$ de la Figura 2.11. Ese módulo es quien representa el nivel de intensidad del píxel, lo que para las señal VGA es aceptable (con las salvedades que se verán más adelante).

Una explicación analítica, validada por resultados empíricos, de como a pesar de esa característica y considerando que sin modificaciones en ese software se pueden visualizar emanaciones de señales codificadas, se plasma también en este capítulo.

4.1. Extensión del espionaje a señales HDMI

Utilizando las mismas herramientas descritas para el caso VGA en la sección 3.4, y siguiendo el mismo esquema de pruebas de la Figura 3.4, se extienden los escenarios de simulación y espionaje para el caso HDMI.

Se presentan entonces en esta sección los resultados, evitando repetir las consideraciones hechas previamente para el caso VGA, que alentaron la descripción analítica de la sección 4.2 que terminan ayudando a comprender qué se ve en ambos escenarios.

4.1.1. Detección de emisiones de señales de video HDMI

La primera y simple extensión del espionaje trata de captar la misma imagen que en el caso VGA (Figura 3.5) pero esta vez usando la interfaz HDMI de

una notebook (Lenovo™ Ideapad™ 100v) conectada a una televisión Philips™ 32PFL5604/77.

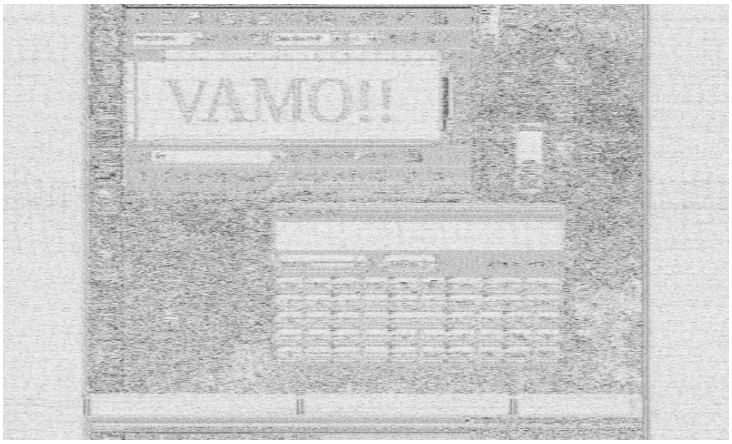


Figura 4.1: Captura de imagen transmitida por la interfaz HDMI en el primer armónico, tomada con la opción de inversión de color de TempestSDR.

Habiendo utilizado el mismo hardware, incluida la misma antena de la Figura 3.3 c) y misma frecuencia de muestreo (40Mhz), y el mismo software TempestSDR, otra vez los resultados fueron muy alentadores, lográndose ver muy bien el texto como se aprecia en la Figura 4.1. Cabe resaltar que el texto se captó en forma más nítida que en el caso VGA. Sin embargo la distancia donde se ubicó la antena no fue superior a los 80cm, distancia que una vez superada degradó sustancialmente la captación, lo que a los efectos de un ataque no es ni práctico y muchos menos eficiente.

4.1.2. Simulación de recepción de emisiones de señales HDMI

Las simulaciones E1 y E2 incorporan la codificación TMDS (sección 2.4) en la etapa (2). Es decir, cuando se guarda el archivo *.dat* que hace las veces de entrada en la recepción, se guarda como la señal que viaja por la interfaz HDMI. Esto trae un incremento de las frecuencias en un factor $n_b = 10$ que deja muy fuera del alcance de las frecuencias de muestreo $1/T_s$ del hardware SDR usado en el espionaje. Por lo tanto, esto se debió considerar en las simulaciones para no falsear los resultados.

Se parte del escenario E2 donde desde TempestSDR se "levanta" el canal simulado en GNU Radio. Recordando que TempestSDR toma el valor absoluto de las muestras recibidas cada T_s segundos luego de pasar por el LPF, y que además los bits se transmiten cada T_s/n_b segundos, ese valor será alguna especie de promedio de los n_b bits del píxel más otros bits de otros píxeles (efecto que se verá en la sección siguiente).

A pesar de ese "caos" de bits, se ve mucha información en la imagen, como se puede apreciar en la Figura 4.2.

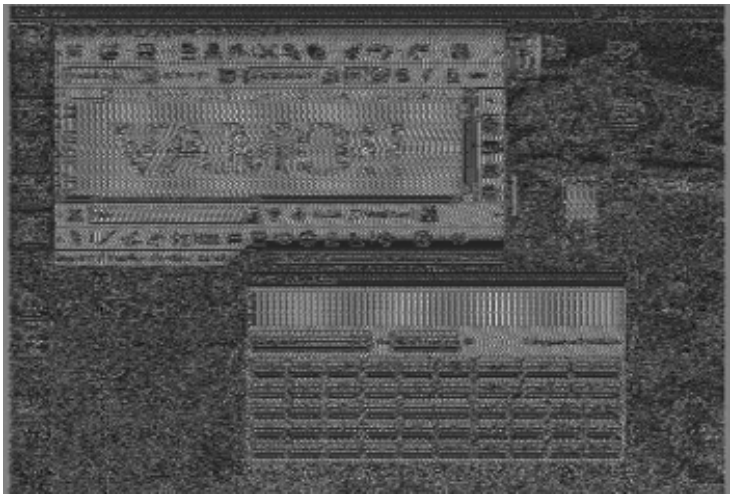


Figura 4.2: Simulación de la imagen HDMI recuperada usando el E2 del esquema de la Figura 3.4.

Es importante notar que a pesar de ese aumento de un orden de magnitud en la frecuencia fundamental de las emanaciones, usando parámetros en recepción (T_s) realistas, aún se aprecian, no sin esfuerzo: el texto, los límites de las ventanas y algunos íconos del escritorio.

Por otro lado, la simulación con el escenario E1 debe contemplar el hecho que en el escenario E2 no haya decodificación TMDS. Pero al mismo tiempo, al ser una simulación en software, puede trabajar con las frecuencias apropiadas, lo que le permite recupera los bits, ya no solo un valor cada T_s.

Se buscó una forma de contemplar estas dos contradicciones, y como en principio no se sabe cual es la forma del promedio mencionado en el caso del escenario E1, se optó en esta etapa por hacer un promedio de los n_b bits para obtener el valor de un píxel. Esto a sabiendas que los resultados no reflejarían el escenario real. Esto se corrige en las secciones siguientes (4.2) una vez se obtiene la expresión analítica de la señal recibida.

Se debe resaltar que en las simulaciones se usa un filtro pasabajos que simula el LPF del SDR (ver Figura 2.11) que recorta a 40MHz (como lo haría el hardware) una señal que tiene una frecuencia, para su resolución más baja, de algunos cientos de Megahertz.

Atendiendo a que lo que se puede ver en el escenario E2 es más fiel inclusive que la simulación del escenario E1, y vista la simplificación burda del promedio descrita, surge la imperiosa necesidad de corregirla en la sección siguiente.

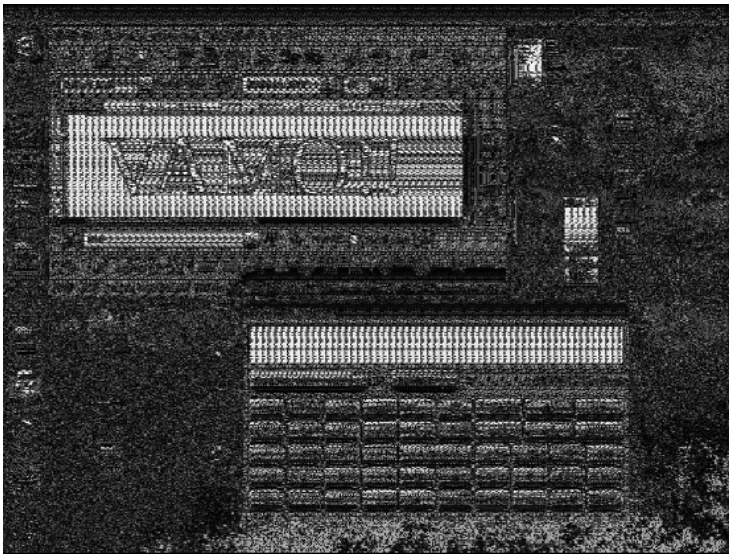


Figura 4.3: Simulación de una imagen HDMI recuperada usando el E1 del esquema de la Figura 3.4, con una f_cutoff para el LPF de 40MHz.

Nota: Del mismo modo se hizo para el caso VGA, en los dos escenarios de simulación de esta sección se trabajó con resoluciones de 800x600 @60Hz, también para optimizar los tiempos de ejecución de los scripts. Con una diferencia no menor en este caso, trabajar en resoluciones más altas impide el desarrollo de las simulaciones usando computadoras de escritorio, pues el tiempo de procesamiento insumido es excesivamente grande.

4.2. Más sobre la recepción de la señal HDMI

De la misma forma que se procedió en el caso de la señal VGA en la sección 3.2.1, lo que deja la libertad de saltear algunos de los pasos allí recorridos, se opera aquí con la señal HDMI.

Partiendo en este caso de la ecuación análoga a la ecuación (3.7) y considerando que en la señal de video TMDS representada en la ecuación (3.5), b_i solo puede tomar dos valores (ver Figura 2.10), esto es:

$$b_i(t) = \begin{cases} AV_{cc} \\ AV_{cc} - V_{swing} \end{cases} \quad \text{ó} \quad b_i(t) = \begin{cases} V_{swing} \\ -V_{swing} \end{cases} \tag{4.1}$$

Primero se replantea la ecuación (3.5) considerando los n_b (diez) bits con que se codifica cada píxel:

$$x^{HDMI}(t) = \sum_{k=-\infty}^{\infty} \sum_{i=0}^{n_b-1} {b_i}^k p_b(t - iT_b - kT_p), \tag{4.2}$$

donde ${b_i}^k$ es el i-ésimo bit dentro del k-ésimo píxel. Esta ecuación representa la sumatoria de n_b señales, una por cada bit donde además $T_p = n_b T_b$.

Haciendo la TF de la ecuación (4.2):

$$X^{HDMI}(f) = P_b(f) \sum_{k=-\infty}^{\infty} \sum_{i=0}^{n_b-1} {b_i}^k e^{-j2\pi(iT_b+kT_p)f}, \tag{4.3}$$

la señal a la salida de los LPF, punto (7) en la Figura 3.2 será:

$${x_R}^{HDMI}(nT_s) = \mathcal{F}^{-1}\Big\{ X^{HDMI}(f - mf_b) rect(f/f_{cutoff}) \Big\}\Big|_{t=nT_s}. \tag{4.4}$$

Considerando que:

$$X^{HDMI}(f - mf_b) = X_s^{HDMI}(f - mf_b)P_b(f - mf_b) = X_s^{HDMI}(f)P_b(f - mf_b),$$

donde además se usó la periodicidad de $X_s^{HDMI} \Rightarrow$

$${x_R}^{HDMI}(nT_s) = \Big[\sum_{k=-\infty}^{\infty} \sum_{i=0}^{n_b-1} {b_i}^k \delta(t - iT_b - kT_p) \Big] * g_d(t)\Big|_{t=nT_s}, \tag{4.5}$$

donde tomando $m = 1$:

$$g_d(t) = \mathcal{F}^{-1}\Big\{ P_b(f - f_b) rect(f/f_{cutoff}) \Big\} \tag{4.6}$$

se obtiene:

$$\boxed{{x_R}^{HDMI}(nT_s) = \sum_{k=-\infty}^{\infty} \sum_{i=0}^{n_b-1} {b_i}^k g_d(nT_s - iT_b - kT_p)} \tag{4.7}$$

Teniendo en cuenta la similitud de $g(t)$ de la ecuación (3.11) para el caso VGA y $g_d(t)$, valen las mismas consideraciones hechas en la sección 3.2.1. Se le agrega a la interferencia entre píxeles del caso VGA, la combinación lineal, dada por la sumatoria en i, de los n_b bits de cada píxel. Esto es, cada muestra será una combinación lineal de los n_b bits del píxel, más la interferencia de las combinaciones lineales de los bits de los píxeles adyacentes.

4.2.1. Efecto Blurring en HDMI y la decodificación

A pesar de la combinación lineal de diferentes bits de diversos píxeles que refleja la ecuación (4.7), las imágenes HDMI captadas con TempestSDR permiten visualizar información útil como se vio en las secciones 4.1.2 y 4.1.1.

Lo que se vio en el caso VGA (Figura 3.11), donde se presentaron diferentes formas de $g(t)$ y que son igualmente válidas para $g_d(t)$, constituye un escenario muy apropiado para explicar porqué a pesar de la mezcla de bits que representa la ecuación (4.7) hay información valiosa en el espionaje HDMI.

En esta sección se agregan formas de $g_d(t)$ que se muestran en la Figura 4.4, donde se aprecian dos formas adicionales para una $f_{cutoff} = 50MHz$ y para $f_{cutoff} = 200MHz$. Ambas referidas al ancho T_b marcado con la forma del pulso rectangular en color rojo. Las dos formas de $|g_d(t)|$ se grafican normalizadas, ya que lo importante es hacer notar el peso relativo de los bits "contaminantes" y no la diferencia entre las magnitudes de los pulsos.

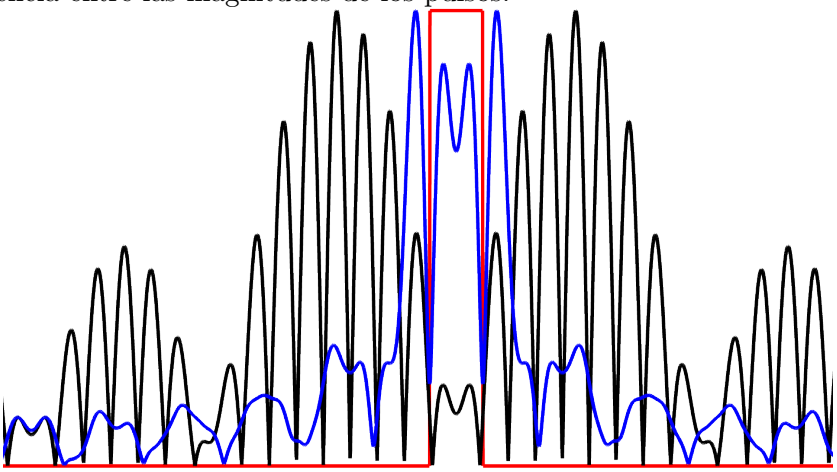


Figura 4.4: $|g_d(t)|$ para una $f_{cutoff} = 50MHz$ en negro y para $f_{cutoff} = 200MHz$ en azul, ambos casos normalizados.

La imagen muestra que cuanto mayor sea f_{cutoff} más se concentrará el cálculo del promedio en el propio bit. Esto es, $g_d(t)$ tendrá más peso relativo en iT_b en la ecuación (4.7) que en el resto de los bits (los otros sumandos en i) y que en el resto de los bits de los otros píxeles (los otros sumandos en k).

A esta altura hay suficiente evidencia analítica para sustituir el brusco promedio de la sección 4.1.2, que se uso como una primera aproximación, por el real surgido de $g_d(t)$. Los resultados se muestran en la Figura 4.5.

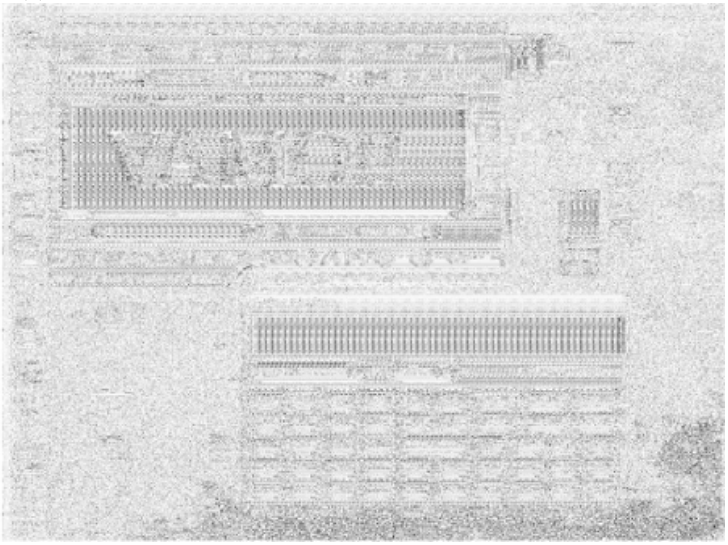


Figura 4.5: Simulación E1, esta vez usando el promedio ponderado por $g_d(t)$,$f_{cutoff} = 50MHz$. Para compararla con la tomada de TempestSDR, Figura 4.1, también toman colores invertidos.

Viendo los resultados, se puede afirmar que la simulación de Octave, con el promedio correcto surgido de aplicar $g_d(t)$, refleja con cierta verosimilitud lo que hace TempestSDR. Esto es: muchos bits dentro del mismo píxel contribuyendo al promedio, sumandos en i en la ecuación (4.7), y bits de píxeles adyacentes contribuyendo también, sumandos en k en dicha ecuación.

Ahora bien, el esfuerzo de usar un filtro que "acierte más" al bit iT_b, que básicamente consiste en usar un SDR generalmente más caro, en tanto tenga más ancho de banda, no reditúa mucho en calidad de la imagen recuperada si no se hace una decodificación. Repetir el ensayo que lleva a obtener la Figura 4.5 con un LPF con más ancho de banda no es útil.

Otro escenario de simulación: incorporación de la decodificación

El siguiente ensayo a realizar, como forma de mejorar la detección, consiste en hacer una decodificación TMDS en el escenario simulado. Esto implica detectar cada uno de los $n_b = 10$ bits de cada píxel. En un escenario real esto implicaría aumentar la frecuencia de muestreo n_b veces, lo que es inalcanzable con el hardware usado en este trabajo.

Por lo tanto, lo que se simula ahora es que se están muestreando cada uno de los bits, y una vez detectados se procede a la decodificación para generar el valor del píxel. Esta forma de detección se refleja en la Figura 4.6, que claramente muestra mejores detalles que las obtenidas con TempestSDR (Figura 4.1) en el espionaje o en la simulaciones de las figuras 4.1 y 4.5.

Lo descrito parece lógico pues el promedio brusco que refleja TempestSDR pierde mucha información al omitir la decodificación no lineal usada en HDMI.

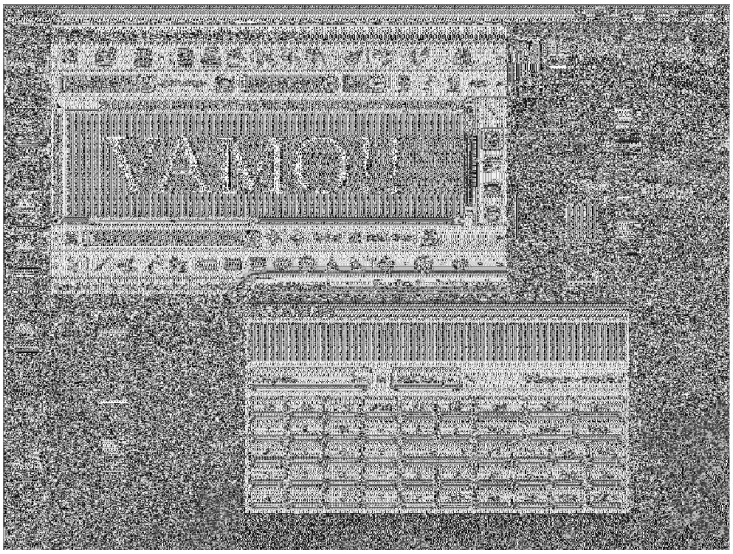


Figura 4.6: Decodificación TMDS muestreando cada T_b con $f_{cutoff} = 50MHz$.

Un ensayo adicional consiste en repetir la simulación pero con el filtro de 200MHz de la Figura 4.4, donde habrá menos bits adicionales a iT_b tanto del propio píxel como de píxeles adyacentes contribuyendo al promedio de forma significativa.

Si bien el hecho de, como se mencionaba antes de "acertar más" al bit iT_b, redunda en una decodificación más fiel, viendo la Figura 4.7 donde se ve el texto con un fondo más uniforme y aparecen más definidos los "botones" de la calculadora, comparada con la Figura 4.6, no es una mejora sustancial que pueda influir en la decisión de invertir en un hardware con mejor respuesta que el usado, por lo menos del análisis de estas dos figuras.

Por lo tanto, para profundizar en cuanto al beneficio de usar un LPF con más ancho de banda en un entorno más objetivo, se compara la respuesta del esquema de simulación a la imagen patrón ya usada de la Figura 3.12.

Figura 4.7: Decodificación TMDS a partir de un LPF con $f_{cutoff} = 200Mhz$.

Previo a extraer conclusiones de carácter general, vale la pena repasar lo expresado en unos párrafos anteriores al concluir sobre la forma de los pulsos de la Figura 4.4. Se observa allí que para el caso del pulso filtrado con $50MHz$, cuyo módulo de su espectro está representado en negro, el peso relativo de los demás bits (fuera del rectángulo rojo del pulso ideal) dependerá mucho de donde se tomen los valores dentro de T_b, i.e. si estos se toman en el centro su peso relativo será casi nulo, en cambio si se toman un poco corridos (fuera de sincronismo) su peso será sustancial.

En suma: En términos generales se puede afirmar que tener un LPF con mayor $f_{cutoff} \Rightarrow$ tener una pulso $g_d(t)$ que se acerca a los resultados que se obtendrían con pulso ideal (son pocos los bits que pesarán significativamente en la suma de la ecuación (4.7) además del "bueno") $\Rightarrow$ cada bit se puede decodificar (entre $\pm V_{swing}$) con más fidelidad. Por lo tanto, se podrá hacer mejor la decodificación TMDS.

Otro aspecto a considerar es el sincronismo (ver capítulo 8 de [37]). Puede darse el caso que tener un buen sincronismo traiga buenos resultados con hardware de menor costo (menos ancho de banda), a costa del mayor procesamiento en recepción que éste implique.

En la Figura 4.8 se percibe esto último. En donde en a) y b) se representan las figuras decodificadas en base a señales con buen sincronismo para frecuencias f_{cutoff} de 50 y $200MHz$ respectivamente, y en c) y d) las mismas recuperaciones pero con errores de sincronismo. Donde, si bien el sincronismo mejora la recepción para ambos casos: a) vs. c) y b) vs. d), el LPF con menor ancho de banda y buen sincronismo muestra resultados comparables al LPF con mayor ancho de banda y mal sincronismo: a) vs d).

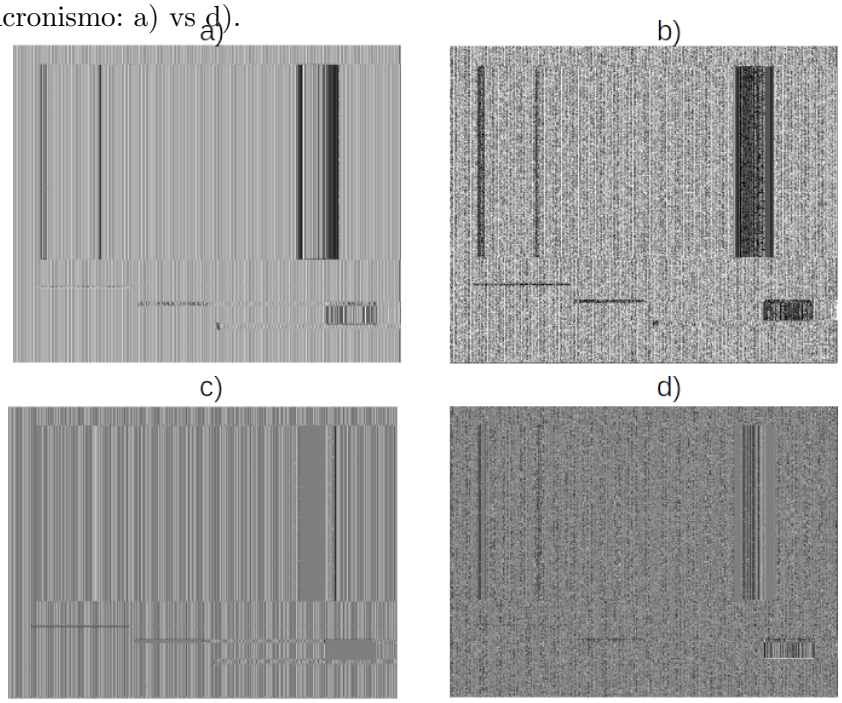


Figura 4.8: Sincronización temporal a) Sin error, $f_{cutoff} = 50MHz$ b) Sin error, $f_{cutoff} = 200MHz$ c) Con error, $f_{cutoff} = 50MHz$ d) Con error, $f_{cutoff} = 200MHz$.

Vale reiterar que este resultado no es alcanzable con el hardware SDR usado en las pruebas de campo, dada la respuesta en frecuencia del LPF muy inferior a 200MHz.

El beneficio reflejado en las Figuras 4.6 y 4.7 de decodificar las señales y no quedarse con el "promedio" que genera g_d, no se hizo en TempestSDR, entre otras cosas atendiendo a la restricción del hardware que no puede muestrear a las frecuencias requeridas. Quedando como una oportunidad de mejora para trabajos futuros.

4.3. Ecualización de la señal a la salida del SDR

En la Figura 3.2 aparece sugerida la utilización de un filtro ecualizador a la salida del SDR entre los puntos marcados como (7) y (8).

Se comenzará con un análisis del caso VGA para extenderlo luego al caso HDMI, con la presentación de resultados simulados. Lo que se busca compensar es el efecto que introduce el producto $P(f - f_p)rect(f/f_{cutoff})$ en la ecuación (3.9)

que termina atenuando en forma diferente a las componentes de frecuencia que se recuperan en la detección.

Recordando que ese producto es la TF de $g(t)$, lo que se busca es que el filtro resultante sea un pulso de Nyquist para evitar la ISI, esto es:

$$\mathcal{F}\{g(t)\}(f)H_{eq}(f) \tag{4.8}$$

debe cumplir con el criterio de Nyquist. Esto es:

$$g(t) * \mathcal{F}^{-1}\{H_{eq}(f)\}\Big|_{t=nT_s} = \begin{cases} 1 & \text{si } n = 0 \\ 0 & \text{si } n \neq 0 \end{cases}.$$

Eligiendo al pulso resultante sin exceso de ancho de banda [37], el ecualizador tendrá la siguiente forma:

$$H_{eq}(f) = \frac{1}{\mathcal{F}\{g(t)\}(f)}. \tag{4.9}$$

La ecualización no se puede hacer en el cruce por cero de $\mathcal{F}\{g(t)\}(f)$ por la restricción de existencia de la expresión de la ecuación (4.9). Esto impide la compensación de la atenuación, y se termina perdiendo información.

$H_{eq}(f)$ es el inverso, cuando existe, de la transformada del pulso conformador en la porción del espectro ($1/2T_p$, $3/2T_p$). Agregando este ecualizador a lo hecho en la sección 3.4.1 donde se hizo la simulación de la recepción de emisiones, a la salida del SDR, se obtiene una imagen como se aprecia en la Figura 4.9, donde se toma $|x_R^{eq}|$.

Figura 4.9: Simulación de la imagen recuperada usando $|x_R^{eq}|$ si se ecualizara a la entrada con el filtro de (4.9), $f_{cutoff} = 10MHz$.

En la Figura 4.10 se muestra la corrección del ecualizador en el domino de las frecuencias.

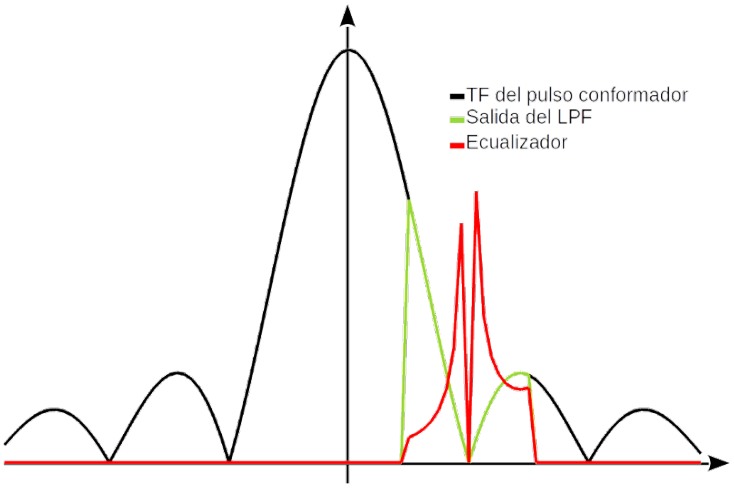


Figura 4.10: Respuesta en frecuencia del ecualizador de la ecuación (4.9).

Para comparar resultados de este agregado con la opción sin ecualización, más allá de la evidente mejora en los caracteres, se toma la misma porción de ambas figuras (3.6 y 4.9), una parte de la ventana de la aplicación Calculadora y una porción de la barra de íconos favoritos del escritorio, ambos de Ubuntu, se las amplía y se muestra en la Figura 4.11.

Resulta evidente que la recuperación con el filtro ecualizador de la ecuación (4.9) tiene mejor definición (en algunas zonas que son particulares de la imagen espiada). Basta ver que los números son visibles en una imagen y en la otra se distinguen con dificultad. Mientras que los íconos se distinguen muy bien en la imagen ecualizada y vagamente en la imagen no ecualizada.

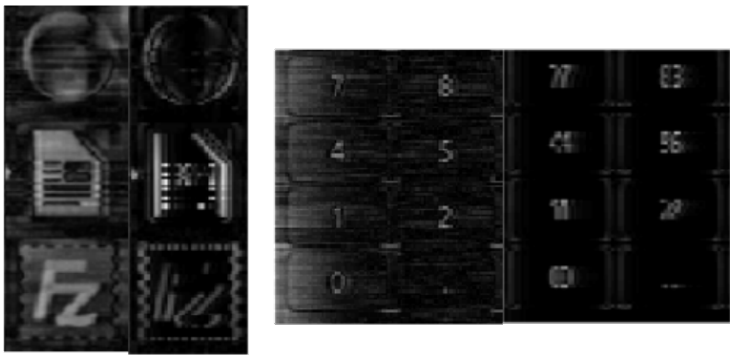


Figura 4.11: Dos comparaciones de sendas porciones de la misma imagen, donde la recuperación sin ecualizar se ve sobre la derecha y usando el ecualizador de la ecuación (4.9) a la izquierda.

Una forma de ver la razón de esta mejora se plasma en la Figura 4.12, donde se comparan las dos formas de $g(t)$: la "original" en verde (pulso ideal filtrado con un LPF con $f_{cutoff} = 10MHz$ como se vio en la sección 3.5.1), y la que resulta de ecualizar. Esta última concentra el peso en los píxeles cercanos a la vez que atenúa los píxeles del entorno más alejado.

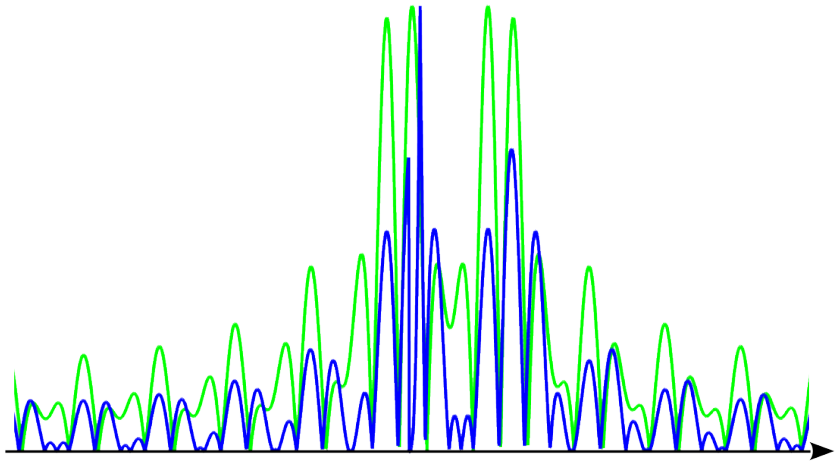


Figura 4.12: Comparación entre $g(t)$ de la ecuación (3.14). En verde, la misma que se muestra en la Figura 3.11 y en azul la que resulta de ecualizar con la ecuación (4.9).

La ecualización también introduce más cortes por cero. Recordar que se construyó el H_{eq} para que el filtro resultante sea de Nyquist. Además se hizo sin exceso de ancho de banda por lo tanto, los ceros de $g(t)$ ecualizada serán ceros en cada múltiplo del tiempo de muestreo, siempre que haya sincronismo ideal.

En la sección 3.5.1, al analizar el blurring, se mostraron los efectos sobre la detección de bordes y en consecuencia porque las letras se ven huecas, a partir del patrón de pruebas de la Figura 3.12. Se analiza entonces cualitativamente el efecto que el filtro ecualizador (4.9) tiene sobre los bordes.

Comparando las dos figuras (3.13 y 4.13), se ve que los resultados son coherentes con los análisis primarios y las conclusiones ya expresadas, la recuperación sin ecualización detecta mejor los bordes verticales. Esto se percibe en los bordes verticales de las barras horizontales finas (se confunden en el caso ecualizado). Esto al mismo tiempo sugiere que en la imagen ecualizada, el efecto de ver las letras rellenas, es debido al blurring, una especie de "arrastre" que da la sensación de relleno cuando hay dos bordes verticales próximos, y deja en evidencia que no es un verdadero relleno cuando los bordes verticales están separados.

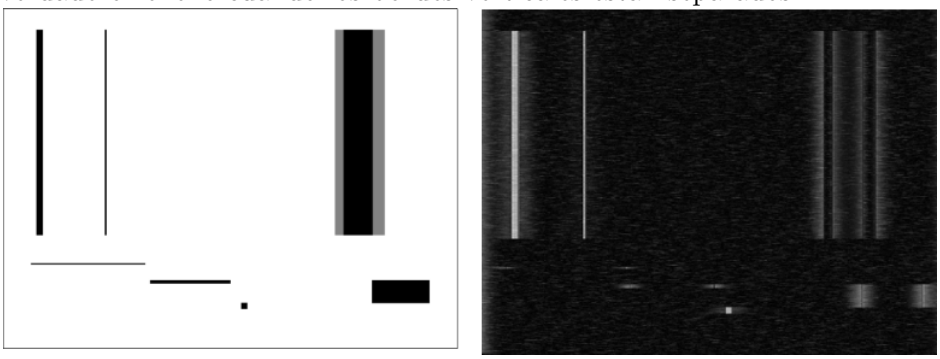


Figura 4.13: Detección simulada, sobre la derecha, usando un ecualizador a la salida del SDR, del patrón de la izquierda.

Esta aparente contradicción entre la mejor percepción de la Figura 4.11 y lo

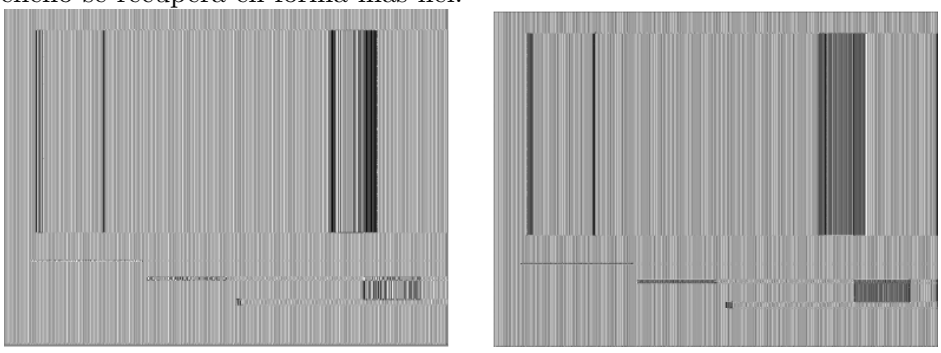
expresado en el párrafo anterior, no es tal: solo es mejor la opción sin ecualizar detectando solo bordes verticales.

Del mismo modo se puede compensar con un ecualizador la señal HDMI de la ecuación (4.7), resultando en un filtro ecualizador con la siguiente respuesta en frecuencia:

$$H_{eq}^{HDMI}(f) = \frac{1}{F(g_d(t))(f)}. \tag{4.10}$$

El camino seguido para HDMI es esencialmente el mismo que para VGA, salvo que el pulso es más corto, por lo tanto, el ancho de banda del ecualizador es mayor.

En la Figura 4.14 se muestra el resultado de la ecualización usando la ecuación (4.10) y decodificando TMDS (b), comparado con la decodificación sin ecualizar (a). Es notoria la mejora en las rectas horizontales finas, basta ver que en la ecualizada y en la resolución de la figura aparece mientras que casi no aparece en la que no usa ecualización. También las líneas verticales aparecen más definidas, y el relleno se recupera en forma más fiel.



a) b)

Figura 4.14: Comparación del espionaje HDMI del patrón de la Figura 3.12 a) sin ecualización, b) ecualizando.

Valen también las mismas consideraciones que en el caso VGA en cuanto a la forma del pulso ($g_d(t)$ en este caso), remarcando que la decisión es entre los dos valores posibles de la codificación TMDS, i.e. $\pm V_{swing}$ y aplicando el ecualizador se reducen sustancialmente los errores.

4.4. Otras posibles mejoras en la recepción

Dentro de las muchas oportunidades de mejora adicionales a las ya mencionadas se describen dos campos que pueden mejorar no solo la recepción sino la percepción visual de la recepción y el espionaje en general.

Una consiste en introducir mejoras en el procesamiento en tiempo real, tanto en las simulaciones como en el escenario real, como por ejemplo usar la parte real de la señal recibida y corregir los errores de frecuencia, y la otra describe algunas técnicas de post procesamiento.

4.4.1. Uso de la parte real

Como se mencionó en la sección 3.5.2 el software TempestSDR toma el módulo de la señal en la recepción ($|x_R|$), lo que tiene la ventaja que lo hace inmune a los errores de frecuencia.

Ahora bien, el uso de un filtro ecualizador como el de la sección 4.3 junto con la utilización de $\mathbb{R}e(x_R^{eq})$, redundan en una mejor nitidez de la imagen recibida como se ve el primer ensayo que se hizo en la simulación por Octave, cuyo resultado se muestra en la Figura 4.15. Se aprecia allí que:

- La mejora en la nitidez es muy notoria.
- El texto en el editor se lee mejor.
- Los demás textos: los nombres de los íconos y en la calculadora se leen mejor.
- En la barra de tareas se diferencian sin ninguna dificultad los íconos).
- Aparecen las formas en la imagen de fondo de pantalla: edificios, el follaje.
- Los íconos dentro del editor de texto se distinguen.

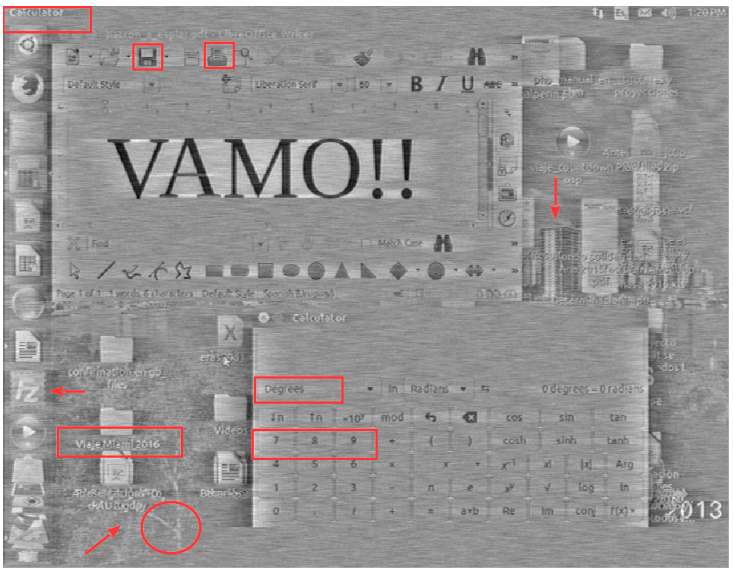


Figura 4.15: Recuperación simulada de una imagen VGA si se ecualizara a la entrada con el filtro de la ecuación (4.9) y se tomara $\mathbb{R}e(x_R^{eq})$ con $f_{cutoff} = 10MHz$.

El efecto del ecualizador visto en el plano complejo (Figura 4.16) muestra un mejor comportamiento respecto al caso sin ecualizar: la dispersión de la señal ecualizada es menor en referencia a la no ecualizada, la señal se parece más a un recta. Resta hacer una corrección adicional en frecuencia, no hecha en este trabajo, que no resultará fácil de hacer en este contexto (con señales tan débiles, y con un canal que introduce muchas distorsiones, desconocido, etc.).

Queda planteado entonces, que además del uso del ecualizador, es recomendable el uso de un PLL en la recepción. En [37] hay una profunda base teórica acerca de la sincronización en fase y frecuencia por lo que esta sección solo se remite a ella.

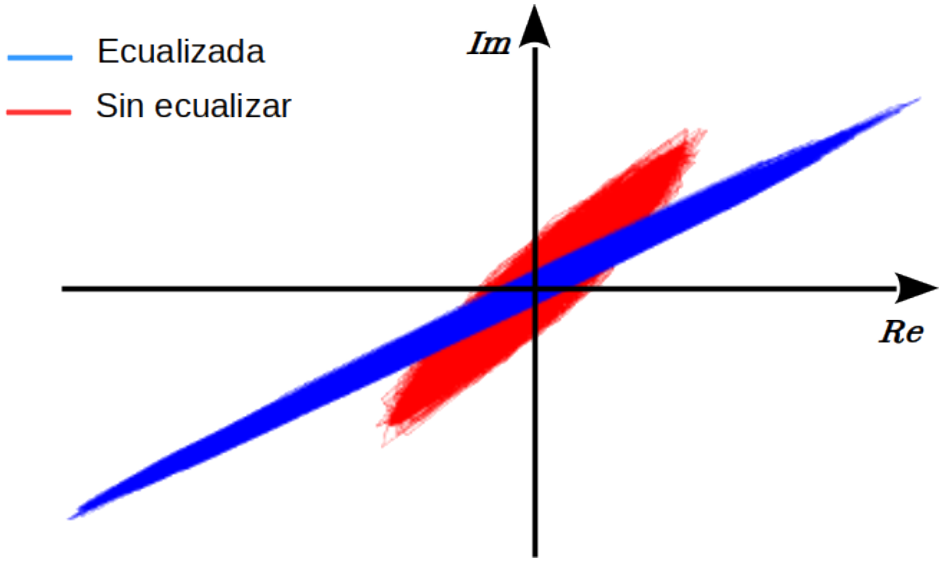


Figura 4.16: Efecto del ecualizador en la recuperación de una señal VGA visto en el plano complejo.

En el caso de las señal HDMI, el algoritmo que decodifica la señal recibida es muy simple:

$$\mathbb{R}e(x_R^{eq}) \leq 0 \quad ? \quad x_R^{eq} = -V_{swing} : x_R^{eq} = V_{swing}.$$

Por lo tanto, en el caso HDMI no existe una posibilidad de mejora adicional como tal si se toma la parte real, pues el algoritmo de decodificación la tiene ya incorporada.

Efecto del error de frecuencia en la ecualización

La ecualización resultante en la Figura 4.15 de la simulación fue hecha asumiendo que no hay errores de frecuencia, cuyo análisis se hizo en la sección 3.5.2.

A los efectos de mostrar la importancia de considerar y corregir estos errores, si se fuera a ecualizar, se muestra en la Figura 4.17 el caso de la recuperación de la señal, ecualizando y con un error de frecuencia $\Delta f = 100Hz$. Allí se marcan las diferencias más notorias respecto a la Figura 4.15 con recuadros o flechas rojas.

Siendo el error considerado apenas del 0,00026 % de la frecuencia fundamental $1/T_p$, las diferencias son sustanciales.

Figura 4.17: Recuperación simulada de una imagen VGA, ecualizando y con un error $\Delta f = 100Hz$.

4.4.2. Procesamiento offline

Si bien es un tema amplio y muy ambicioso de abordar en una sola sección, se debe considerar que el espionaje no se limita al análisis meramente visual y en tiempo real de las emanaciones captadas. Por el contrario, se puede recurrir a post-procesamiento tanto de la señal RF en su totalidad, sus partes o de imágenes captas puntualmente.

Este último tipo de procesamiento se enmarca dentro de los métodos de recuperación de imágenes que trabajan con imágenes estáticas. Por ejemplo: realce de bordes, trabajar con las curvas de la imagen (ecualización de histogramas), métodos de filtrado de ruido, clasificación y/o detección de patrones (más específicamente: reconocimiento de caracteres), deep learning, etc.

Una práctica muy fácil de llevar a cabo, ya que está presente en muchas aplicaciones de código abierto de edición de imágenes, consiste en ecualizar el histograma de la imagen. Recordando que no se genera más información con este método, es más: se puede perder información (si la transformación que lleva de una imagen a otra no es estrictamente creciente[43]), pero teniendo presente que la percepción de una imagen no está basada en el valor absoluto de la intensidad o niveles de grises, sino más bien en el contraste local.

En la Figura 4.18 se compara una porción de la figura ecualizada que se mencionó en la sección anterior, contra la misma porción con un aumento del contraste. No aparecen elementos nuevos ni se leen caracteres que no se leían en la imagen original, pero la lectura es más directa. En otras casuísticas se podría dar el caso que sí se leyeran caracteres antes imperceptibles si es que el contraste fuera más pobre que el del ejemplo.

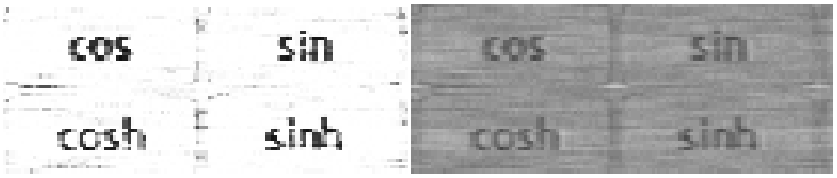


Figura 4.18: Comparación de una porción de la imagen 4.15 consigo misma cambiando el contraste en GIMP de Ubuntu.

El paquete *image* de Octave contiene un conjunto de funciones para filtrado y transformación, y de operaciones morfológicas de imágenes muy amplio que también se pueden utilizar como apoyo para el post-procesamiento de imágenes.

Esta página ha sido intencionalmente dejada en blanco.

Capítulo 5

Conclusiones y propuestas sobre trabajos futuros

Contar con equipamiento SDR accesible que pueda captar las emanaciones provenientes de interfaces VGA y HDMI, complementado con herramientas de software de código abierto, ya sean de propósito general como Octave o GRC, o de aplicación específica como TempestSDR, dejan abierta la posibilidad para trabajos analíticos como el que se plasmó en este documento. Se ha tratado de conjugar la captación real de emanaciones acompañada con una explicación teórica de los resultados vistos y los que se podrían llegar a ver en trabajos futuros.

La captación de las emanaciones provenientes de interfaces de video no resulta fácil. Desde la parte de radiofrecuencia hasta el muestreo de las componentes en fase y cuadratura este trabajo se pudo realizar, con las restricciones presupuestales planteadas, gracias al desarrollo de SDR. Por otro lado, la conformación de imágenes a partir de esas muestras fue posible a partir del muy buen trabajo de Marinov. Explicar qué se está viendo, porqué, cuales son las oportunidades de mejora y los límites o restricciones propios de los diferentes escenarios de espionaje, ha sido el aporte principal en este trabajo de tesis.

La documentación de la NSA, entre otras muchas fuentes, que va quedando disponible, solo hace aumentar el entusiasmo de quienes se dedican a encontrar vulnerabilidades en diferentes sistemas de información. Sin embargo, el campo de las emanaciones espurias no parece tener tanta atención como las vulnerabilidades que se han visto a lo largo de este trabajo han mostrado que debería [13].

En este capítulo se mencionará un caso particularmente sensible: el voto electrónico. Junto con algunas recomendaciones de seguridad generales, para terminar con algunas conclusiones y propuestas de trabajo futuro que complementan las ya vistas.

5.1. Un ejemplo sensible

Si bien el escenario descrito en esta sección no necesariamente se ajusta a la realidad, a los efectos de mostrar algunas vulnerabilidades y como paliarlas resulta

práctico. Rop Gonggrijp et al. [44], han estudiado las vulnerabilidades de las urnas electrónicas usadas por el 90 % de los votantes holandeses, que también se usan, con modificaciones menores, en algunas partes de Francia y Alemania. Siendo una de sus preocupaciones las emanaciones que pueden ser captadas a unos cuantos metros y de esa forma ser usadas para espiar lo que está siendo votado.

En la Figura 5.1 se muestra un modelo de boleta electoral electrónica como las que se pudieran presentar en la pantalla de una urna de voto electrónico, esto es: la imagen que se le presenta al elector una vez ha seleccionado el candidato de la fila 3 columna 5[45]. Allí aparece la foto del candidato con una sombra abajo y a la derecha. En la imagen b) se muestra como se ve esa imagen captada en TempestSDR (interfaz VGA), donde aparece una línea vertical que corresponde al final de la sombra. Mientras que las fotos c) y d) son resultados de ecualizaciones simuladas sin y con ruido respectivamente.

En todos los casos es posible identificar la posición del candidato seleccionado. Cabe resaltar que si la posición es fija en todas las instancias de voto, se puede inferir el candidato seleccionado. Las posturas de los candidatos y corbatas si las tuvieran pueden identificarse en todos los casos.

También se pueden identificar caracteres grandes, banderas si fueran de formas diferentes unas de otras y en particular si tuvieran bastones verticales.

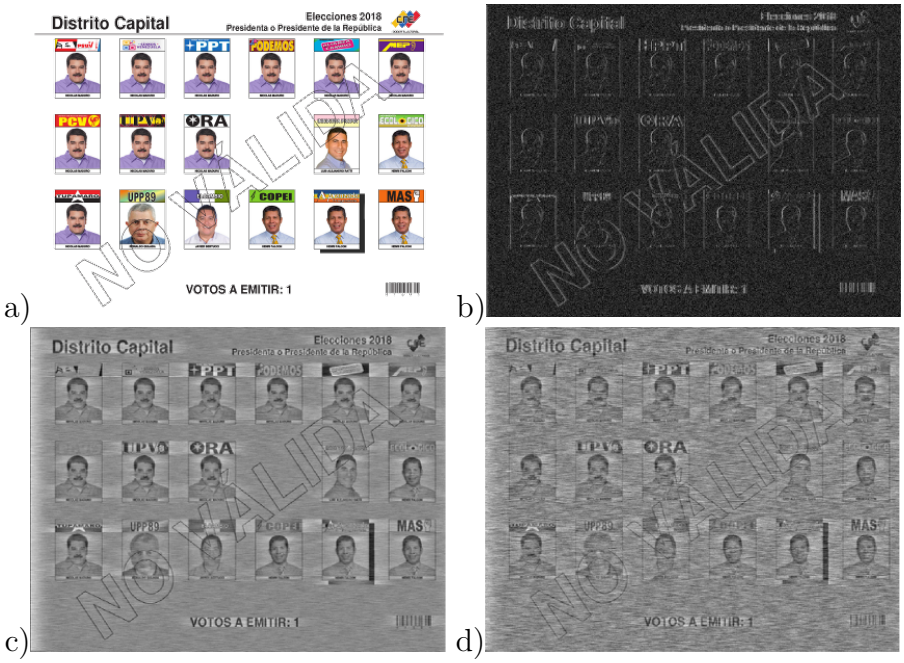


Figura 5.1: Voto electrónico.

Ecualizando y tomando parte real, aparecen adicionalmente características particulares de los candidatos, tales como bigotes prominentes, se puede distinguir candidatos calvos, las corbatas aparecen más definidas, identificar si el candidato está de frente o de perfil (y hacia donde apunta), etc.

Se muestra entonces con este ejemplo la vulnerabilidad del secreto del sufragio si no se toman algunas precauciones en el diseño de las hojas de votación digitales.

Esas precauciones pueden ser algunas de las siguientes[1]:

a) Evitar que un candidato u opción en general se "marque" de alguna forma en la pantalla, particularmente si eso implica la aparición de líneas verticales.

b) Dentro de lo posible evitar diferencias sustanciales entre candidatos, por ejemplo que uno tenga corbata y los otros no.

c) Ubicar los candidatos en forma aleatoria dentro de la matriz de votación de un sufragio a otro.

d) Posicionar a todos lo candidatos de igual forma en la foto, y guardando relaciones relativas al tamaño lo más uniforme posible.

e) Procurar que todas las instancias tengan la misma cantidad de rectángulos. Esto es, si una vez hecha la primera elección de candidato a Presidente, se pasa a una pantalla donde para cada partido tenga diferente número de candidatos al parlamento, se podrá diferenciar entre partidos en la segunda selección.

f) Evitar los contrastes que generen bordes pronunciados.

g) Distinguir a los candidatos preferentemente por colores, recordando que lo que se recupera es un falso color.

h) Colocar más de una urna (pantalla) por circuito para que se interfieran mutuamente las emanaciones.

5.2. Recomendaciones sobre seguridad

Una máxima popular reza que una cadena es tan débil como el más débil de sus eslabones. En materia de seguridad informática y en espionaje en general muchas veces resulta difícil encontrar tal eslabón. Yendo específicamente al tema de las $eEMR$, resulta trivial decir que diseñar un equipo electrónico que no tenga emanaciones electromagnéticas con riesgo de ser captadas es casi imposible. Sin embargo se pueden tomar muchas medidas, de diferente grado de dificultad y costo, que minimicen los riesgos.

Siguiendo la línea que se trazó en el capítulo 1 en cuanto a utilizar definiciones de la NSA norteamericana, o considerando el complejo entramado de agencias gubernamentales de ese país y en base a documentación que paulatinamente se va liberando (descalificando) de esos entes estatales, se pueden encontrar numerosas guías y recomendaciones con puntillosas pruebas de equipos y requerimientos de aceptación para sistemas que manejen información (NSI, National Security Information). Esos documentos cuando se liberan son en general obsoletos y su

[1]El resto de las precauciones que refieren a las emanaciones propiamente dichas son análogas al resto de los sistemas.

liberación muchas veces es parcial. Sin embargo constituyen una guía muy detallada de verificación a tener en cuenta en las etapas de diseño o de aceptación de equipos. Por ejemplo el NSTISSAM[2] TEMPEST/2-95, contiene incluso consideraciones locativas además de las propias de diseño de los equipos. O la especificación Nº 94106 de la NSA en referencia al blindaje o apantallamiento electromagnético de recintos.

Ahora bien, cumplir todas esas exigencias, dependerá de factores circunstanciales tales como el presupuesto disponible, tiempo de desarrollo, y sobre todo si la información que se maneja lo amerita. De todas formas sin caer en consideraciones extremas tales como: "Si no quiere que lo espíen: conviértase en un ermitaño", se describen a continuación algunas medidas de seguridad a tener en cuenta:

a) **Separación de cables rojos y negros**: El concepto es bien conocido en ambientes militares y en seguridad en general: los cables o equipos rojos procesan información sensible sin encriptar mientras que los negros llevan información encriptada o desclasificada (lo que hace casi irrelevante el hecho que sea vista).

   La medida implica la separación de estos cables de forma que no se induzcan señales no encriptadas hacia caminos que puedan emanar y luego ser captadas, i.e. que señales que circulan por cables rojos se induzcan en cables negros. Por ejemplo el memorándum TEMPEST 2-95 de la NSTISS [3], establece distancias mínimas entre cables rojos y negros de 5 cm, y de 25 cm entre equipos que procesen señales rojas y equipos o cables negros.

   Claramente tanto el cables VGA como el HDMI son cables rojos, llevan información sensible no encriptada, por lo tanto, una medida adicional de seguridad es convertirlos en cables negros usando en ambos extremos encriptadores.

b) **Apantallamiento**: Por apantallamiento (*shielding* en inglés) se entiende al que se le practica a los cables o equipos y al que se le puede realizar a locaciones enteras. Una vez identificados cuales son los cables rojos se deberían apantallar, recordando que la gran mayoría de los cables VGA están apantallados por un revestimiento muy fino de aluminio, entre cada par de cables y luego el grupo entero de cables, que no impide la emanación por lo menos en las circunstancias en que se desarrolló este trabajo.

   De la misma forma, si la información que se maneja lo amerita, el local entero debería estar apantallado. (*facilty shielding*).

c) **Interferencia positiva (masking)**: esto es, emitir una señal con la misma frecuencia portadora, sea $1/T_p$ o $1/T_b$ según sea VGA o HDMI, con potencia mayor que la que pueda emitir la señal del monitor (aunque esto no es necesariamente imperativo). Es esperable que en la mayoría de las situaciones ésta sea la señal captada.

[2]National Security Telecommunications and Information Systems Security Advisory Memorandum.

[3]National Security Telecommunications and Information Systems Security de EEUU.

Se debe tener la precaución de transmitir también en los armónicos, y tener presente que muchas veces no es suficiente para evitar algún tipo de lectura.

Una forma de llevar a cabo esta interferencia consiste en emitir una señal equivalente a la producida por una imagen trasmitida a través de la interfaz VGA (o HDMI) usando un transmisor de RF. Esa equivalencia refiere a que la interferencia será una señal PAM con el mismo timing, i.e: T_s, blanking y f_t, e incluso puede ser producto de la modulación de una imagen muy similar a la imagen del contexto con el cual se esté trabajando, y que se quiere proteger, en el monitor que se llamó en su momento "inadvertido". El esquema de defensa se muestra en la Figura 5.2.

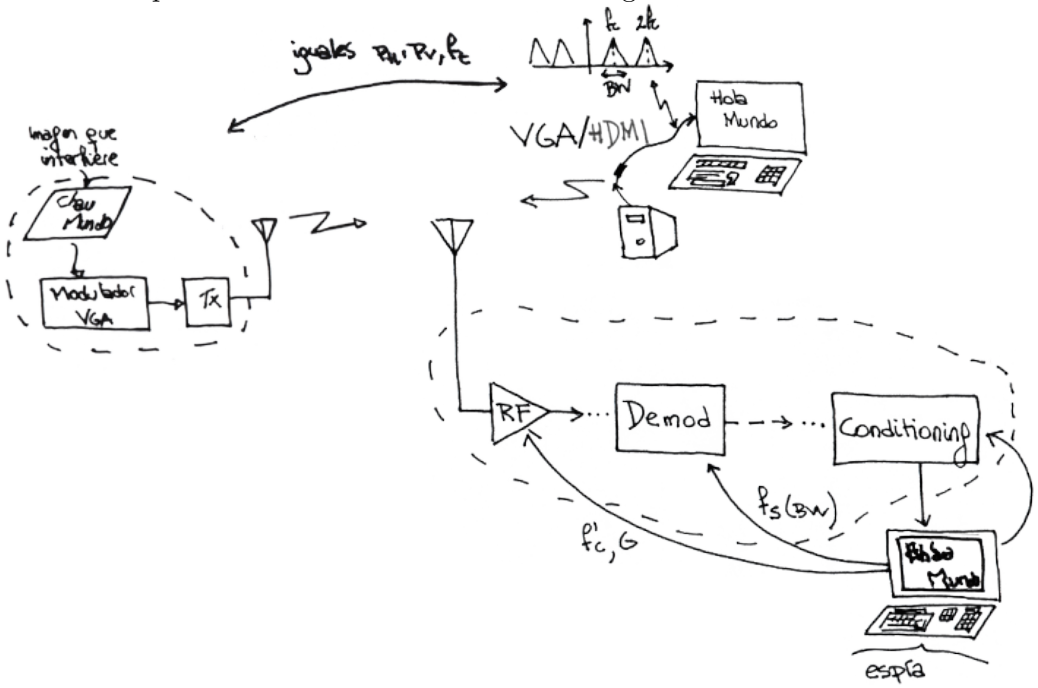


Figura 5.2: Esquema de una interferencia positiva.

En la Figura 5.3 se muestra una imagen que es usada como interferencia positiva, es decir, se transmite (emana) a propósito, al mismo tiempo y con las mismas características que la imagen que se quiere proteger. Es la misma imagen que se está espiando (Figura 3.5), donde se ha cambiado el texto en el editor de texto Writer. Luego se muestran tres diferentes escenarios donde se fue modificando el porcentaje de potencia con que se irradia la interferencia en referencia a la potencia de la imagen a proteger: iguales potencias arriba, 25 % más para la interferencia (abajo a la izquierda) y 100 % más para la interferencia en la otra imagen.

d) **Combinación de color de fondo y fuente**: Se trata de encontrar una combinación de colores entre el fondo sobre donde se escribe el texto y el propio texto, que permita la lectura medianamente cómoda en el procesador de texto, pero que dificulte el espionaje.

Figura 5.3: Interferencia positiva.

La Figura 5.4 muestra la modificación hecha a la imagen objetivo, cambiando el color de fondo del editor de texto a negro y los caracteres a verde oscuro, y al lado la detección de la interfaz VGA donde el texto ha desaparecido casi completamente.

e) **Sospechar de cualquier posibilidad**: Contemplar en las políticas de seguridad el tema de las *eEMR* parece ser de perogrullo, pero muchas veces estos temas se obvian por completo en las reglas de seguridad. El mero ingreso a lugares sensibles con dispositivos de uso popular (i.e. teléfonos celulares, pero también otros) que puedan actuar como receptores y retransmisores o que registren las emanaciones para post procesamiento debería ser restringido per se.

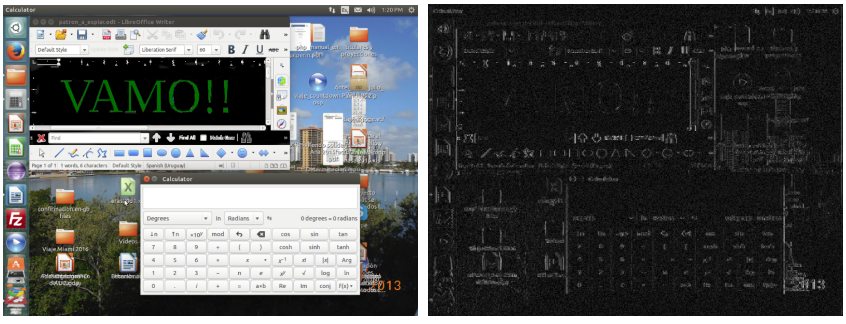


Figura 5.4: Contraste defensivo VGA.

Las medidas enumeradas, que si bien son efectivas, no son infalibles, conviene que sean consideradas desde el inicio del desarrollo de un proyecto que maneje información sensible. Este concepto que se conoce, sobre todo en el ambiente de

desarrollo de software, como *Secure by design*, seguridad por diseño, e implica que los sistemas son diseñados desde el inicio mismo para ser lo más seguros posible. Las prácticas de espionaje son consideradas un hecho y se toman todas las precauciones posibles para minimizar el impacto de las prácticas maliciosas y anticipar las vulnerabilidades de seguridad del sistema.

5.3. Conclusiones

Los principales desafíos de este trabajo fueron, por un lado el hecho de lidiar con emisiones electromagnéticas que, al ser no intencionales, no están acondicionadas para propagarse y en consecuencia recibirse en las mejores condiciones. Por otro, comprender cabalmente las expresiones analíticas detrás de ellas. Mientras que en un sistema típico de comunicaciones, la transmisión se diseña para que la señal llegue de la mejor forma posible a la recepción, eligiendo en consecuencia el pulso conformador, la codificación, la frecuencia portadora, etc., este espionaje tiene que poder recibirlas a pesar de no tener todo ese acondicionamiento.

La primera conclusión es que a distancias razonables, con equipo *off the shelf* y como se hubo mostrado en [1] y [3], se pueden detectar emisiones provenientes de la interfaz VGA y se puede mejorar la recepción con intervenciones en el software de recepción como se sugiere en las secciones 4.3 y 4.4. Caben también mejoras incorporando elementos de hardware con mejores prestaciones, esto es: SDR con mejor respuesta en frecuencia y, antenas con más ganancia y selectividad de frecuencias a los equipos usados.

Por otro lado, y no menos importante es que el espionaje se puede extender a la interfaz HDMI (o DVI dado que tienen las mismas características), no sin dificultades en cuanto a la distancia. Repasando cronológicamente, las primeras capturas en base a emanaciones espurias se hicieron por [2] sobre monitores CRT cuyos voltajes son órdenes de magnitud más grandes que los visto en este trabajo. Luego se pasó a espiar sobre monitores VGA y algunas notebooks con interfaces digitales pero escasos trabajos se han publicado sobre HDMI, y menos aún con base analítica.

Las expresiones analíticas para ambas interfaces, ecuaciones 3.14 y 4.7 dejan el punto de partida para considerar las mejoras, tanto las ya propuestas en el capítulo 4 como algunos de los trabajos futuros propuestos en la sección siguiente. Se entiende entonces que esas bases analíticas junto con las demás consideraciones que en ellas se sustentan y que explican los efectos de blurring, sobre los pulsos conformadores y ecualización son una aporte en si mismos.

Por otro lado, el hecho de mostrar probables falencias en aplicaciones tan sensibles como la que se describió en la sección 5.1 en referencia al voto electrónico, no puede ser considerado un aporte en si mismo pero agrega un nuevo elemento a tener en cuenta para preservar el carácter secreto del sufragio.

5.4. Trabajos futuros

Además de las oportunidades de mejora enumeradas en las secciones 4.3 y 4.4, sobre todo la ecualización, las cuales fueron ensayadas en software, y resta implementarlas en ambientes de espionaje real, existen otros desafíos para trabajos futuros en especial relativos al espionaje de señales emanadas de interfaces HDMI.

Primero que nada se debe mejorar la distancia de ubicación de la antena respecto a la interfaz, recordando que no se lograron distancias superiores a un metro, con una antena que si bien tiene una respuesta en frecuencia que abarca el rango de frecuencias de las resoluciones bajas, no presenta una respuesta adecuada para las resoluciones altas. De todas formas no se puede alentar a priori una mejora sustancial con el uso de una mejor antena, pues las frecuencias de trabajo son altas y la potencia de trabajo baja, un mínimo de 275mW[4], por lo tanto a pocos metros la caída de la señal RF será drástica como para poder ser captada más allá de unos pocos metros con una antena pasiva o de baja ganancia. Algunos valores de potencia recibida: Para una resolución de 800x600 @ 60Hz $\Rightarrow 1/T_b = 383MHz$ que con una $P_t^{max} = 350mW$, a un metro y con una buena antena habrá una potencia de recepción:

$$P_r = P_t G_r G_t \left(\frac{\lambda}{4\pi d} \right)^2 \leq 150\text{mW},\ L \approx 7\text{dB}$$

donde G_r y G_t son las ganancias de las antenas de transmisión y recepción respectivamente, usando sus máximos valores [5] y L es la pérdida. Mientras que a cinco metros (distancia razonable, para un espía ubicado en una habitación contigua al objetivo) se tendrá $P_r \leq 4\text{mW}$ y $L \approx 25\text{dB}$.

Valores que permiten la detección usando antenas con buena G_r o imponiendo el uso de electrónica (filtros y amplificadores) antes que la antena entregue la señal al SDR. Si entre el objetivo y el espía hay mampostería, las consideraciones son otras, entrando en juego la geometría, sobre todo los bordes de las aperturas donde se produce el fenómeno de difracción por borde filoso que permitiría recibir la señal.

Respecto a la ecualización, se puede ver en la Figura 4.12 que $g(t)$ tiene más cruces por cero, por lo tanto abre la posibilidad a la utilización de técnicas de sincronizar temporal en la recepción para que las muestras de los bits sucesivos de todos los píxeles sean tomadas justo en esos cruces (ver referencia [37]). Esta propuesta es análoga al concepto teórico de pulso de Nyquist, pero exige un trabajo de procesamiento en tiempo real no evaluado en este trabajo. Al mismo tiempo, siendo casi imposible que no haya errores de frecuencia en un escenario real, viendo que por muy pequeños que sean introducen distorsiones significativas cuando se ecualiza y se toma la parte real, y resultando muy notorios los beneficios mostrados en la Figura 4.15 se impone la corrección de dichos errores.

[4] La norma [38] establece un mínimo de 55mA y no un máximo para la interfaz. Salvo cables activos para largas distancias no se pueden drenar de la interfaz más de 50mA. Dados estos datos se toma un máximo de 70mA.

[5] $G_t = 1,64$dBi dipolo, y $G_r = 30$dBi asumiendo que la recepción se haga con una parabólica.

El procesamiento *offline* a partir de imágenes grabadas o de las propias emanaciones grabadas abre un abanico de oportunidades muy grande para mejorar la percepción del observador. Desde técnicas de ecualización de histograma hasta filtro de ruido, algunas de las cuales se mencionaron. También el uso de técnicas de reconocimiento de caracteres, tanto sea mediante el uso de correlación espacial u otras.

Por último y sin perder de vista que lo que se trata de espiar es texto, en particular texto que es escrito y/o leído por un ser humano, surgen oportunidades de mejora a partir de la persistencia temporal de ese texto en la pantalla. En la sección 2.2.2 se describió un uso de esa persistencia, pero sin dudas es una característica de las emanaciones que puede ser más explotada en el post-procesamiento. En este trabajo y en los trabajos usados como referencias, [1] y [3], el esfuerzo se centra en obtener los píxeles o los bits y procesarlos. Un rumbo disruptivo para recorrer en futuros trabajos, sería profundizar en la búsqueda de herramientas de reconocimiento de patrones y *deep learning* que permitan desarrollar algoritmos que aprendan la relación entre formas en la pantalla y las muestras.

Las técnicas de reconocimiento de patrones, junto con inteligencia artificial, permitirían construir además, un sistema de espionaje que sea menos vulnerable a los errores de sincronismo temporal, ya que reconocerían las letras aún cuando se vayan desplazando dentro de la pantalla debido a tales errores.

Esta página ha sido intencionalmente dejada en blanco.

Apéndice A

Complemento: fórmulas y desarrollos útiles y normativa

A.1. Ecuaciones de Maxwell

Puede ser inferido a partir de las ecuaciones de Maxwell, que en tanto haya cargas eléctricas en movimiento habrá generación y propagación de campos electromagnéticos. Este es un fenómeno obviamente bien conocido y base en las comunicaciones de radio. De hecho es la base fundamental de la utilización de antenas en sistemas de radio. Por lo tanto, se hará un breve repaso de tal fenómeno en los párrafos siguientes, habiendo una excelente profundización en la teoría electromagnética en la referencia [46].
Partiendo de dos de las ecuaciones de Maxwell:

$$\nabla.\vec{B} = 0, \qquad \text{ley de Gauss para el campo magnético} \tag{A.1}$$

$$\nabla \times \vec{E} = -\frac{\partial \vec{B}}{\partial t}, \qquad \text{ley de Faraday.} \tag{A.2}$$

Sabiendo que la divergencia de un rotor es cero, $\nabla.(\nabla \times \vec{A})$, se introduce el vector potencial magnético $\vec{A}$ de forma tal poder usar dicha propiedad: $\vec{B} = \nabla \times \vec{A}$ definido a menos de un potencial escalar ϕ (potencial eléctrico), pues para todo escalar ϕ: $\nabla \times \nabla\phi = 0$, eligiendo entonces en forma genérica $\vec{A} \rightarrow \vec{A} + \nabla\phi$, la ecuación (A.2) queda:

$$\nabla \times \vec{E} = -\frac{\partial \nabla \times (\vec{A} + \phi)}{\partial t} \Rightarrow \nabla \times (\vec{E} + \frac{\partial \vec{A}}{\partial t}) = 0. \tag{A.3}$$

Siendo que el rotor de la expresión en (A.3) es nulo, queda definido como se vio a menos de un gradiente:

$$\vec{E} + \frac{\partial \vec{A}}{\partial t} = -\nabla\phi. \tag{A.4}$$

Los dos potenciales quedan definidos a menos de una *gauge*, una función escalar *f=f(r,t)*, donde los potenciales $\hat{A} = \vec{A} + \nabla f$ y $\hat{\phi} = \phi - \frac{\partial f}{\partial t}$ también cumplen

(A.4). Esa libertad en la elección de los potenciales permite imponer una condición adicional que facilitará las deducciones:

$$\nabla.\vec{A} + \frac{1}{c^2}\frac{\partial \phi}{\partial t} = 0, \qquad \text{Condición de Lorentz.} \tag{A.5}$$

Usando las restantes ecuaciones de Maxwell:

$$\nabla.\vec{E} = \frac{1}{\epsilon}\rho \qquad \text{Ley de Gauss,} \tag{A.6}$$

$$\nabla \times \vec{B} = \mu\vec{J} + \frac{1}{c^2}\frac{\partial \vec{E}}{\partial t} \qquad \text{Ley de Ampère.} \tag{A.7}$$

Y sustituyendo (A.4) en (A.6) $\nabla.\vec{E} = \nabla.(-\frac{\partial \vec{A}}{\partial t} - \nabla\phi) = -\frac{\partial}{\partial t}(\nabla.\vec{A}) - \nabla^2\phi$ usando (A.5)

$$\nabla.\vec{E} = \frac{1}{c^2}\frac{\partial^2 \phi}{\partial t^2} - \nabla^2\phi = \frac{1}{\epsilon}\rho. \tag{A.8}$$

De forma análoga se trabaja con (A.7)

$$\nabla \times \vec{B} - \frac{1}{c^2}\frac{\partial \vec{E}}{\partial t} = \nabla \times (\nabla \times \vec{A}) - \frac{1}{c^2}\frac{\partial}{\partial t}(-\nabla\phi - \frac{\partial \vec{A}}{\partial t}) \Rightarrow$$

$$\nabla \times \vec{B} - \frac{1}{c^2}\frac{\partial \vec{E}}{\partial t} = \nabla \times (\nabla \times \vec{A}) + \nabla(\frac{1}{c^2}\frac{\partial \phi}{\partial t}) + \frac{1}{c^2}\frac{\partial^2 \vec{A}}{\partial t^2}$$

usando: $\nabla \times (\nabla \times \vec{A}) = \nabla(\nabla.\vec{A}) - \nabla^2\vec{A}$, y Lorentz (A.5) se obtiene:

$$\nabla \times \vec{B} - \frac{1}{c^2}\frac{\partial \vec{E}}{\partial t} = -\nabla^2\vec{A} + \frac{1}{c^2}\frac{\partial^2 \vec{A}}{\partial t^2} = \mu\vec{J} \tag{A.9}$$

(A.8) y (A.9) son las ecuaciones de onda, reescritas a continuación:

$$\boxed{\begin{array}{c} \frac{1}{c^2}\frac{\partial^2 \vec{A}}{\partial t^2} - \nabla^2\vec{A} = \mu\vec{J} \\ \frac{1}{c^2}\frac{\partial^2 \phi}{\partial t^2} - \nabla^2\phi = \epsilon\rho \end{array}}. \tag{A.10}$$

Donde la densidad de carga ρ y la densidad de corriente $\vec{J}$ son las fuentes generadoras de los potenciales ϕ y $\vec{A}$ respectivamente. Entonces si se conocen tales densidades se pueden resolver las ecuaciones (A.10).

Por lo tanto, en el caso de las emanaciones "bastaría" ver que forma tienen tales densidades para estimar como y cuan lejos se podrían propagar los campos generados, ver Anexo A.2.

A.2. Funciones de Green para la ecuación de ondas y solución retardadas

Los valores de ϕ y A se deducen a partir de las funciones de Green para la ecuación de onda, donde las soluciones así llamadas retardadas son:

$$\begin{aligned} \phi(x,t) &= \frac{1}{4\pi\epsilon_0}\int d^3x' \frac{1}{R}[\rho(x',t')]_{ret} \\ A(x,t) &= \frac{\mu_0}{4\pi\epsilon_0}\int d^3x' \frac{1}{R}[J(x',t')]_{ret} \end{aligned} \tag{A.11}$$

donde x y t son la ubicación y tiempo en el lugar de observación y, x' y t' lugar y tiempo donde se genera la carga, $R = x - x'$.

De forma análoga a como se hizo para los potenciales en la sección anterior, las ecuaciones de onda se pueden deducir para los campos, obteniendo:

$$\begin{aligned} \nabla^2 E - \frac{1}{c^2}\frac{\partial^2 E}{\partial t^2} &= -\frac{1}{\epsilon_0}(-\nabla\rho - \frac{1}{c^2}\frac{\partial J}{\partial t}) \\ \nabla^2 B - \frac{1}{c^2}\frac{\partial^2 B}{\partial t^2} &= -\mu_0 \nabla \times J \end{aligned} \tag{A.12}$$

De donde se deducen las siguientes expresiones [1]:

$$E = \frac{q}{4\pi\epsilon_0}\left\{\left[\frac{\hat{R}}{R^2}\right] + \frac{[R]_{ret}}{c}\frac{\partial}{\partial t}\left[\frac{\hat{R}}{R^2}\right] + \frac{\partial^2}{c^2\partial t^2}[\hat{R}]_{ret}\right\} \qquad \text{Feyman} \tag{A.13}$$

$$B = \frac{\mu_0 q}{4\pi}\left\{\left[\frac{v\times R}{k^2R^2}\right]_{ret} + \frac{1}{c[R]_{ret}}\frac{\partial}{\partial t}\left[\frac{v\times\hat{R}}{k}\right]_{ret}\right\} \qquad \text{Heaviside} \tag{A.14}$$

A.3. Normativa sobre EMC

Como parte de la investigación, los equipos que fueron sujeto de evaluación, como por ejemplo en el caso de las figuras 3.9 y 3.10, son equipos certificados con las normas exigidas en los mercados europeos, norteamericano o nacional. Es por ello que se describen, muy brevemente, algunas de esas normas de forma de tener presente cuales son sus exigencias.

Las normas tienen requerimientos en dos sentidos. Por un lado están las consideraciones de un aparato como **emisor** de disturbios electromagnéticos, y por

[1] Ver las secciones 6.4 y 6.5 de la referencia [46], donde se hace la deducción rigurosa.

otro, el aparato **receptor**[2] que es afectado por esos disturbios, los que son percibidos como interferencia. El disturbio es la señal no deseada producida, la causa, que lleva a la degradación de la performance de otro aparato, y que es percibida como interferencia, la consecuencia.

Habrá entonces un aparato que emite interferencia, otro que tendrá una tolerancia (inmunidad o susceptibilidad) a ellas, y entre ellos habrá o no compatibilidad.

En consecuencia aparecen tres conceptos claramente derivados de esa consideración, el **margen de inmunidad** entre el límite de inmunidad y el nivel de compatibilidad, y el **margen de emisión** entre el nivel de compatibilidad y el límite de emisión. De igual forma se define el **margen de compatibilidad** entre el límite de inmunidad y el límite de emisión. Estos conceptos se ilustran en la Figura A.1.

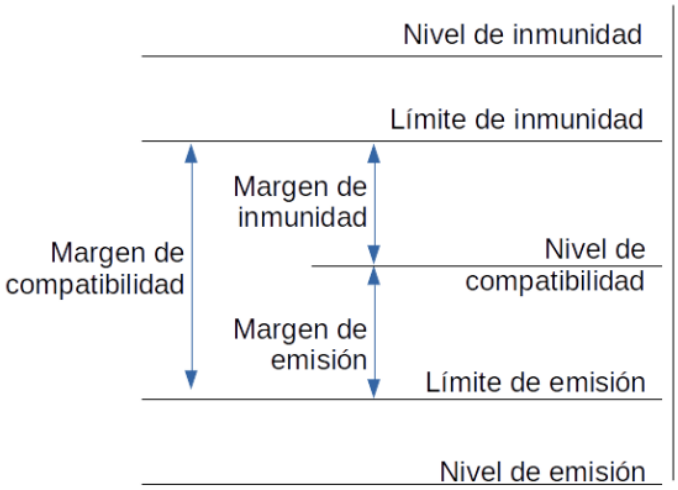


Figura A.1: Diferentes niveles, márgenes, límites de inmunidad y emisión.

A.3.1. Norma EN55022

El prefijo "EN" proviene del inglés: *European Norm*. Las normas así prefijadas pueden ser del Comité Europeo de Normalización (CEN), del Comité Europeo para la Estandarización Electrónica (CENELEC) o del Instituto Europeo de estándares de Telecomunicaciones (ETSI), y en su mayoría son adoptadas por la Unión Europea. En el caso de la norma EN55022, el responsable de su aprobación es CENELEC y toma como base la norma CISRP 22.

La norma [7] tiene por título: *"Information Technology Equipment - Radio*

[2]A veces al aparato que es afectado se lo denomina **susceptor**. A riesgo de inferir confusiones en la traducción desde el inglés, entre susceptor de sensible, y de susceptibilidad como quien absorbe energía electromagnética y la convierte en calor, se prefiere el uso de receptor.

disturbance characteristics - Limits and methods of measurement", y algunos de sus principales aportes pueden resumirse de esta forma:

- Establece las tolerancias de emanaciones de equipos (ITE) que no hayan sido fabricados explícitamente como transmisores o receptores bajos las normas de la ITU, y cuya funcionalidad primaria es guardar, visualizar, obtener, procesar, controlar, etc., datos y mensajes, están equipados con uno o más puertos, y que operan con voltajes (alimentación) inferiores a 600 V.

- Las emanaciones se refieren a señales que van desde 9KHz a 400GHz.

- Define dos clases de ITE: Los equipos Clase B de uso en ambientes domésticos[3] sin lugar fijo de uso, como por ejemplo equipos portátiles alimentados con baterías propias, computadoras personales y sus equipos auxiliares. Mientras que los equipos Clase A satisfacen los límites de su categoría pero no los de la Clase B, que son niveles menos exigentes.

- Determina los métodos y condiciones bajo las cuales se deben hacer las mediciones, distancias, disposición, tiempo y cantidad de medidas, y los límites en dB(μV) y dB(μA) de aceptación por rango de frecuencias. Un ejemplo de tales límites de tolerancia se puede ver en la Tabla A.1.

Frequency range MHz	**Quasi-peak limits** dB(µV/m)
30 to 230	30
230 to 1 000	37
NOTE 1 The lower limit shall apply at the transition frequency. NOTE 2 Additional provisions may be required for cases where interference occurs.	

Tabla A.1: Tomada de la norma EN55022.

Nota: la Tabla A.1 figura como "Table 6 - Limits for radiated disturbance of class B ITE at a measuring distance of 10 m".

A.3.2. Regulación 47 CFR

La parte 15, "Radio Frequency Devices", del capítulo I, título 47 de la FCC de Estados Unidos, es la regulación a través de la cual se deben certificar los equipos electrónicos para poder ser comercializados en ese país.

También define dos tipos de dispositivos, A y B, cuyo alcance es similar al visto en A.3.1, y establece límites superiores de frecuencias de emisión sobre las cuales se harán las pruebas de certificaciones de acuerdo a la Tabla A.2.

[3]La norma refiere a "Ambiente doméstico" como una distancia menor a 10m entre el aparato y receptores de radio y televisión. Esa especificidad puede extenderse a 10m de cualquier otro aparato susceptible a las interferencias.

Highest frequency generated or used in the device or on which the device operates or tunes (MHz)	**Upper frequency of measurement range (MHz)**
Below 1.705	30
1.705-108	1000
108-500	2000
500-1000	5000
Above 1000	5th harmonic of the highest frequency or 40 GHz, whichever is lower.

Tabla A.2: Tabla de frecuencias máximas analizadas en función de las frecuencias de trabajo, tomada de la norma 47 CFR.

Los límites de emanación para dispositivos clase B son los que figuran en la tabla A.3.

Frequency of emission (MHz)	**Field strength (mV/meter)**
30-88	100
88-216	150
216-960	200
Above 960	500

Tabla A.3: Límites a 3m de distancia, tomados de la norma 47 CFR.

Mientras que para dispositivos clase A son los de la tabla A.4.

Frequency of emission (MHz)	**Field strength (mV/meter)**
30-88	90
88-216	150
216-960	210
Above 960	300

Tabla A.4: Límites a 10m de distancia, tomados de la norma 47 CFR.

En su punto §15.9, *Prohibición contra espionaje*, establece:

> *Excepto para la operación de oficiales de la ley encargados de ejercer la autoridad, ninguna persona debe usar, directa o indirectamente, dispositivos operados conforme a la provisión de esta parte (regulación) con el propósito de escuchar o grabar conversaciones privadas de terceros, a menos que tal uso sea autorizado por quienes toman parte de dicha conversación.*

Claramente no menciona la decodificación de señales de video.

A.4. Fórmulas útiles

TF o CTFT	$\rightarrow$	$\mathcal{F}\{x(t)\} = X(f) = \int_{-\infty}^{+\infty} x(t)e^{-j2\pi ft}dt$
inv(TF)	$\rightarrow$	$x(t) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} X(w)e^{-j\omega t}d\omega$
DTFT	$\rightarrow$	$\mathcal{X}(e^{j\Omega}) = \sum_{n=-\infty}^{+\infty} x(n)e^{-j\Omega n}$
DFT	$\rightarrow$	$\mathcal{X}(k) = \sum_{n=0}^{N-1} x[n]e^{-j(2\pi/N)kn}$
SF	$\rightarrow$	$x(t) = \sum_{n=-\infty}^{+\infty} X_k e^{-j\frac{2\pi}{T}kt}$

donde

$$X_K = \frac{1}{T} \int_{-T/2}^{T/2} x(t)e^{-j\frac{2\pi}{T}kt}dt$$

Tabla A.5: Fórmulas útiles.

Referencias

[1] Martin Marinov, **Remote video eavesdropping using a software-defined radio platform.** *University of Cambridge, Computer Laboratory, Cambridge CB3 0FD*, Reino Unido, Junio 11, 2014.

[2] W van Eck. **Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?**, *Elsevier Science Publishers B.V. (North-Holland)*, 0167-4048/85, 1985.

[3] Markus G Kuhn. **Compromising emanations: eavesdropping risks of computer displays.** *University of Cambridge Computer Laboratory, Technical Report,* UCAM-CL-TR-577, 2003.

[4] ITU-T Recomendación P.11, **Efectos de las degradaciones de la transmisión**, *International Telecommunication Union*, 1994.

[5] **TEMPEST: A Signal Problem, NSA FOIA Case #51633**. Approved for Release by *NSA*, EEUU, 2007.

[6] **NACSIM 5000 Tempest Fundamentals**, *National Security Agency*, EEUU, Diciembre 2000.

[7] European EMC standard EN55022, **Information Technology Equipment - Radio disturbance characteristics - Limits and methods of measurement**, *CENELEC*, Setiembre 2006.

[8] Electronic Code of Federal Regulations, **Title 47 Telecommunication, Chapter I, Subchapter A, Part 15: Radio Frequency Devices**, *Office of the Federal Register National Archives and Records Administration*, EEUU, Revisión 2018.

[9] National Security Agency Specification For Shielded Enclosures **Specification NSA No. 94106**, *NSA*, EEUU, Octubre 1994.

[10] **Electromagnetic compatibility, part 1, Section1: Application and interpretation of fundamental definitions and terms**, *International Electrotechnical Commission*, 1992.

[11] **Van Eck phreaking,** Wikipedia, the free encyclopedia.

[12] Sitio web de GNU Radio `http://gnuradio.org/`.

[13] Ross Anderson, **Security Engineering**, *Second Edition, Wiley*, 2008.

[14] M Dillinger, K Madani, N Alonistioti, **Software Defined Radio: Architectures, Systems and Functions Markus**, *John Wiley & Sons, Ltd.* ISBN 0-470-85164-3, 2003.

[15] **Budget of the U.S. National Security Agency in line with the U.S. National Intelligence Program for fiscal years 2011 to 2017**, Statista report, *Statista*, 2018.

[16] Wilson Andrews, Todd Lindeman, **The Black Budget** basado en "FY2013 Congressional Budget Justification Book", *The Washington Post*, Agosto 29, 2013.

[17] Sitio web de NSA Playset `http://www.nsaplayset.org/`.

[18] Milos Prvulovic, **EM Covert Channel Attack from Nearby Desk,** `https://www.youtube.com/watch?v=C4DhFsJthgI`.

[19] Markus G. Kuhn and Ross J. Anderson, **Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations,** *Information Hiding, IH'98, Proceedings, lNCS 1525, Springer-Verlag*, Portland, Oregon, pp. 124-142, Abril 15-17, 1998.

[20] Karman Ali, Alex X. Liu, Wie Wang, and Muhammad Shahzad, **Recognizing Keystrokes Using WiFi Devices,** *IEEE Journal on Selected Areas in Communications*, Vol. 35, No. 5, pp. 1175-1189, Mayo 2017.

[21] Mordechai Guri, Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, Yuval Elovici, **GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies**, *Proceedings of the 24th USENIX Security Symposium*, ISBN 978-1-931971-232, Agosto 12–14, 2015.

[22] NSA/CSS Regulation 90-6: **Technical Security Program. National Security Agency–Central Security Service**, parcialmente descalificado *Fort George G. Meade, Maryland*, 12 pages, 31 Mayo 1999.

[23] Eunchong Lee, Hyunsoo Kim, Ji Won Yoon, **Various Threat Models to Circumvent Air-Gapped Systems for Preventing Network Attack**, *Springer International Publishing*, 2016.

[24] M. Hanspach and M. Goetz, **On Covert Acoustical Mesh Networks in Air**, *Journal of Communications*, vol. 8, 2013.

[25] Blog, Air Gap Computer Network Security, Sitio web: `http://abclegaldocs.com/blog-Colorado-Notary/air-gap-computer-network-security/`.

[26] Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, Yuval Elovici, **Fansmitter: Acoustic Data Exfiltration from (Speakerless) Air-Gapped Computers**, *Ben-Gurion University of the Negev, Cyber Security Research Center*, 2016.

[27] Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, Yuval Elovici, **Acoustic Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard-Drive Noise ("DiskFiltration")**, *Computer Security – ESORICS 2017* pp 98-115, 2017.

[28] A. Barber, **Handbook of Noise and Vibration Control**, *Elsevier Advanced Technology*, 1992.

[29] Sitio web del Proyecto Osmocom `https://osmocom.org/projects/osmo-fl2k`.

[30] **Adaptador USB a VGA como transmisor SDR**, Sitio web RTL-SDR.com, `https://www.rtl-sdr.com/setting-up-and-testing-osmo-fl2k/`.

[31] Steve Markgraf, **osmo-fl2k: Using cheap USB 3.0 VGA adapters as SDR transmitter** `https://media.ccc.de/v/HWVZPK`.

[32] GBPPR, **Overview of the NSa's RAGEMASTER Radar Retro-Reflector** `https://www.youtube.com/watch?v=Eu9QzagshbY`.

[33] Michael Ossmann, **The NSA Playset RF Retroreflectors**, *DEFCON 22 Hacking Conference*, Las Vegas, EEUU, Agosto 7-10, 2014.

[34] Sitio web del curso **Tratamiento de Imágenes por Computadora**, *Instituto de Ingeniería Eléctrica, Facultad de Ingeniería, UdelaR*, `https://eva.fing.edu.uy/course/view.php?id=520`.

[35] Michael Robin, Michel Poulin **Digital Television Fundamentals**, *Second Edition, Mcgraw-Hill,* ISBN 0-007-135581.2, 2000.

[36] VESA Coordinated **Video Timings (CVT) Standard**, *VESA*, Version 1.2, Febrero 8, 2013.

[37] Pablo Belzarena, Federico Larroca, **Comunicaciones Inalámbricas, Notas del Curso**, *Facultad de Ingeniería, Universidad de la República*, 2017.

[38] **Digital Visual Interface**, *Digital Display Working Group*, Revision 1.0, 1999.

[39] Sitio en Wikipedia con lista de principales equipos de SDR: `https://en.wikipedia.org/wiki/List_of_software-defined_radios`.

[40] Sitio web de GNU Octave `https://www.gnu.org/software/octave/`.

[41] Sitio web de Ettus `https://www.ettus.com`.

[42] Tektronix®Application Note, **VGA Interface Testing with the VM5000**, Tektronix, 2006.

[43] Rafael Gonzalez, Richard Woods, **Digital Image Processing**, *Third Edition, Prentice Hall*, ISBN-10: 9780133356724, 2008.

[44] Rop Gonggrijp, Willem-Jan Hengeveld, **Studying the Nedap/Groenendaal ES3B voting computer, a computer security perspective**, *We do not trust voting computers foundation*, Holanda, 2006.

[45] Consejo Nacional Electoral de la República Bolivariana de Venezuela, http://www.cne.gov.ve/divulgacion_asamblea_2015/index.php?e=00&m=00&p=00&c=00&t=00&ca=00&v=00.

[46] John David Jackson, **Classical Electrodynamics,** *Third Edition, McGraw-Hill*, ISBN 0-07-135581-2, 1998.

Glosario

API	Application Programming Interface
CENELEC	European Committee for Electrotechnical Standardization
CFR	Code of Federal Regulation
CISRP	Comité International Spécial des Perturbations Radioélectriques
CPU	Central Processing Unit
CRT	Cathode Ray Tube
CSI	Channel State Information
CSV	Comma Separated Values
CTFT	Continous Time Fourier Transform
CTTA	Certified TEMPEST Technical Authority
DDC	Display Data Channel
DDWG	Digital Display Working Group
DMT	Display Monitor Timings
DFT	Discrete Fourier Transform
DTFT	Discrete Time Fourier Transform
DVI	Digital Visual Interface
eEMR	Radiación EM espurias
EMC	ElectroMagnetic Compatibility
EN	European Norm
ETSI	European Telecommunications Standards Institute
FCC	Federal Communication Commission
FFT	Fast Fourier Transform
FT	Fourier Transform
GNU	GNU is Not Unix
GRC	GNU Radio Companion
HDMI	High-Definition Multimedia Interface
I^2C	Inter-Integrated Circuit
IEC	International Electrotechnical Commission
ITE	Information Technology Equipment
ITU	International Telecommunications Unit
LCD	Liquid Crystal Display
LPF	Low Pass Filter
MOVNTDQ	Move Double Quadword Non-Temporal
MSB	Most Significant Bit
NRZ	Non Return to Zero
NSA	National Security Agency, EEUU
PAM	Pulse Amplitude Modulation
PLL	Phase Local Loop
PNG	Portable Network Graphics
RAM	Random Access Memory
RFID	RadioFrequency IDentification
RPM	Revoluciones Por Minuto
RZ	Return to Zero

SDR	Software Defined Radio
SIMD	Single Instruction Multiple Data
SMA	SubMiniature version A
SNR	Signal to Noise Ratio
SSE	Streaming SIMD Extension
TMDS	Transition-Minimized Differential Signaling
TIC	Tecnologías de la Información y las Comunicaciones
UHF	Ultra High Frequency
VESA	Video Electronic Standars Associaton
VGA	Video Graphic Array
VHF	Very High Frequency
WBFM	WideBand Frequency Modulation

Esta página ha sido intencionalmente dejada en blanco.

Índice de tablas

Esta página ha sido intencionalmente dejada en blanco.

Índice de figuras

Esta es la última página.
Compilado el jueves 20 diciembre, 2018.
http://iie.fing.edu.uy/