Confidencialidad de datos en monitores CRT a examen: Experimento TEMPEST

Antonio Cebrián <acebrian@eln.upv.es>; José Millet <jmillet@eln.upv.es>;
David Moratal Pérez <damope0@eln.upv.es>; Francisco Castells <fracasra@eln.upv.es>

Departamento de Ingeniería Electrónica, Universidad Politécnica de Valencia

La mayoría de usuarios es inconsciente de que la información que se representa en la pantalla de su monitor puede reproducirse en otro equipo a partir de las radiaciones electromagnéticas.

Es algo bien conocido que los equipos electrónicos emiten radiaciones electromagnéticas que pueden producir interferencias en el funcionamiento de otros equipos electrónicos, es lo que se conoce como interferencias electromagnéticas (EMI). En la actualidad todos los equipos electrónicos, para obtener el marcado CE, deben pasar unas pruebas de compatibilidad electromagnética (EMC). Uno de los objetivos de dichas pruebas, es asegurar que las emisiones electromagnéticas de los equipos electrónicos se encuentran por debajo de unos límites definidos en la norma.

Los ordenadores personales así como los sistemas de la tecnología de la información en general, son herramientas indispensables en el mundo laboral y la sociedad actual. La mayoría de usuarios es inconsciente de que la información que se representa en la pantalla de su monitor puede reproducirse en otro equipo a partir de las radiaciones electromagnéticas. A estas emisiones electromagnéticas que pueden comprometer la confidencialidad de la información, se las engloba bajo el acrónimo TEMPEST (*Transiet ElectroMagnetic Pulse Emanation STandard*).

El estudio de las emisiones TEMPEST ha estado históricamente relegado al ámbito militar, siendo por tanto la bibliografía disponible más bien escasa. No obstante, cabe destacar una pequeña excepción asociada a las emisiones TEMPEST producidas en los monitores basados en tubos de rayos catódicos (CRT). Dichas emisiones merecen especial atención por la relativa facilidad con la que puede extraerse información de las mismas. Por esta razón, dichas emisiones son bien conocidas desde los años ochenta, prueba de ello es la aparición en esa misma década de uno de los primeros artículos en el cual se estudia y se describe la extracción de información de la emisión TEMPEST producidas por un monitor de vídeo [1].

Transcurridas casi dos décadas desde la aparición pública de un experimento con TEMPEST en monitores, cabe preguntarse si dicho experimento sigue gozando de validez. Los monitores han evolucionado notablemente en las últimas dos décadas. Se ha pasado de monitores monocromo en fósforo verde con señales de control digital (TTL) a monitores color con señales de control analógicas (RGB) de bajo nivel. Además, las normas de compatibilidad electromagnética se han vuelto más restrictivas reduciendo, por tanto, los niveles de emisión electromagnética permitidas en los equipos.

El objetivo del presente artículo es la reproducción de un experimento con TEMPEST en monitores CRT actuales que demuestre si el TEMPEST sigue siendo un concepto de actualidad. Siguiendo la filosofía del experimento original [1], se intentarán utilizar, en la medida de lo posible, elementos comerciales de bajo coste para reproducir el experimento. No se realizará un estudio teórico sobre las causas que producen la emisión TEMPEST ni sobre sus características, puesto que dicho estudio puede encontrarse como apéndice técnico en [1] y sigue siendo perfectamente válido en la actualidad.

Descripción del experimento

La realización del experimento de TEMPEST con monitores CRT se ajusta al diagrama de bloques de la figura 1. La información visualizada en la pantalla del sistema bajo test se reproducirá en un monitor distante. Para tal efecto se dispone de un sistema de prueba TEMPEST compuesto por: una antena receptora, un amplificador, un equipo receptor, un adaptador de señal de vídeo y un generador de sincronismos.

A continuación, se van a describir cada una de las partes integrantes del experimento:

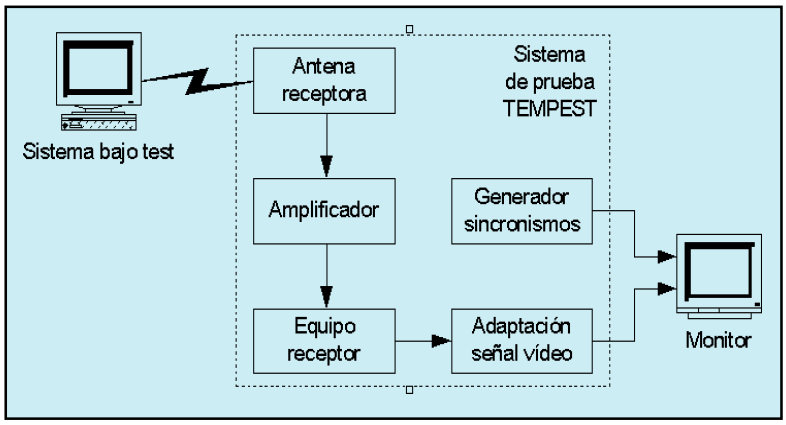

Figura 1. Diagrama de bloques del experimento de TEMPEST.

Sistema bajo test

Como sistema bajo test se ha utilizado un ordenador personal con un monitor CRT color de 17" en el cual se muestra la frase "PRUEBA TEMPEST" ocupando prácticamente toda la pantalla (figura 2). Tal y como se ha comentado, el objetivo del experimento consistirá en reproducir la pantalla visualizada en el sistema bajo test en otro monitor, sin utilizar ningún tipo de conexión física entre

Figura 2. Sistema bajo test.

ambos (origen y destino), mediante el uso de una antena receptora situada a unos metros de distancia del sistema bajo test (figura 3).

Antena receptora y amplificador

La antena receptora permite captar las débiles radiaciones electromagnéticas producidas por el monitor del sistema bajo test. Debe cumplir con dos requisitos fundamentales: debe ser de banda ancha y debe poseer una elevada directividad.

Dado que a priori no es posible saber a qué frecuencia se encontrará el máximo en la recepción de la radiación electromagnética producida por el monitor del sistema bajo test, es necesario disponer de una banda de recepción lo más ancha posible que permita realizar un barrido en la recepción en busca del citado máximo.

Por otra parte, dado el bajo nivel de las radiaciones electromagnéticas producidas por el monitor del sistema bajo test, es importante evitar la recepción de otras fuentes de radiación (fuentes interferentes) que podrían llegar a enmascarar totalmente la radiación electromagnética proveniente del monitor. Una elevada directividad de la antena receptora permitirá minimizar la captación de radiaciones electromagnéticas interferentes.

Para cumplir con los requisitos de banda ancha y elevada directividad, pero manteniendo la premisa inicial de componentes comerciales de bajo coste, se ha recurrido a las antenas empleadas en la recepción de señal de televisión terrestre. Se ha utilizado una antena receptora (figura 4) que cubre las bandas de VHF (canales del 5 al 12) y UHF (canales del 21 al 69) con una ganancia de 8,5dB y 16dB respectivamente y con una elevada directividad.

No obstante y aún con una antena receptora con unas características como las mencionadas, la señal recibida sigue siendo demasiado débil para poder extraer información de ella y es necesario, por tanto, realizar una amplificación de la misma. Dicha amplificación previa a la extracción de información se conseguirá insertando un amplificador a continuación de la antena receptora.

En la selección del amplificador se ha recurrido nuevamente al campo de la recepción de señal de televisión terrestre, utilizándose un amplificador de mástil (figura 4) de banda ancha (VHF y UHF) y con una ganancia ajustable máxima de 25dB.

Figura 3. Antena receptora respecto a sistema bajo test.

Figura 4. Antena receptora y amplificador.

Equipo receptor

Disponiendo ya de un nivel de señal recibida suficiente, es necesario extraer la información contenida en ella. Para ello se precisa de un equipo receptor que integre un sintonizador y un demodulador de AM. Entre las características que idealmente se debería exigir al equipo receptor podemos citar: un amplio rango de barrido de frecuencias (canales) en la sintonización, un ancho de banda del canal ajustable en la demodulación y una elevada sensibilidad.

Siguiendo la tónica de utilizar elementos adscritos al ámbito de la recepción de señal de televisión terrestre, se ha recurrido al uso del sintonizador y del demodulador de un antiguo vídeo VHS (figura 5) que permite la sintonización manual de los canales. Los canales que se están sintonizando no se corresponden con emisoras de TV convencionales, es por ello que no es posible utilizan un sintonizador con búsqueda automática y se recurre al uso de un antiguo sintonizador manual.

Si bien en este caso el equipo receptor se aparta sustancialmente del receptor ideal descrito, presenta la ventaja de ser un equipo receptor ampliamente disponible y de bajo coste.

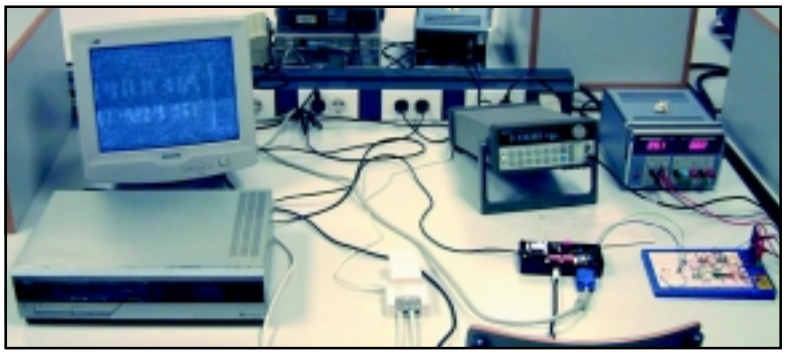

Figura 5. Equipo receptor, generador de sincronismos

Monitor

Como elemento de visualización para la recepción se ha utilizado un monitor CRT de características similares a las del monitor utilizado en el sistema bajo test. Como mínimo, se debe cumplir que ambos monitores soporten las mismas frecuencias de refresco, lo cual permitirá sincronizar adecuadamente la misma imagen en ambos monitores.

Dado que nuestro equipo receptor proporciona una señal de vídeo compuesto monocroma y que, en cambio, el monitor requiere una señal de vídeo RGB a su entrada, será necesario realizar una adaptación de la señal de vídeo proveniente del equipo receptor antes de introducirla en el monitor. Dicha adaptación comprende un ajuste del nivel de la señal y un triplicado de la misma para obtener una imagen monocroma en el monitor.

Por otra parte, si bien por definición la señal de vídeo compuesto contiene los sincronismos horizontal y vertical, en nuestro caso no será así. Se precisará del uso de un generador externo que proporcione los sincronismos necesarios al monitor para la correcta visualización de la imagen recibida.

Generador de sincronismos

Si bien existen técnicas para extraer la información de sincronismo del propio sistema bajo test [1], en nuestro experimento se ha optado por la utilización de un generador de sincronismo externo totalmente independiente del sistema bajo test.

El generador de sincronismos (figura 6) está formado por un oscilador controlador de onda cuadrada de alta precisión (en nuestro caso,

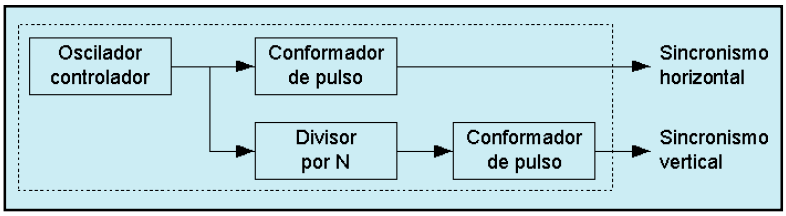

Figura 6. Diagrama de bloques del generador de sincronismos.

será un generador de funciones de precisión), el cual se ajusta para obtener la frecuencia de sincronismo horizontal. A partir de esta frecuencia de referencia se genera, por una parte, el pulso de sincronismo horizontal (conformador de pulso) y por otra, el pulso de sincronismo vertical (conformador de pulso) previo paso por un divisor que será función del número de líneas visualizadas.

Con el generador de sincronismos propuesto (figura 7) obtenemos las señales de sincronismo horizontal y vertical perfectamente sincronizadas (correladas) entre ellas, pero totalmente independientes (incorreladas) de los sincronismos originales. Para poder minimizar los efectos de la incorrelación existente entre sincronismos originales y generados, es necesario disponer de un ajuste muy fino (del orden de los mHz) del oscilador controlado. Este ajuste fino permitirá aproximarse suficientemente a la frecuencia original exacta, lo que se traducirá en la visualización en el monitor de una imagen estable.

Figura 7. Detalle del generador de sincronismos.

Resultados del experimento

Con un sistema de prueba TEMPEST tal y como el que se ha descrito, se ha conseguido reproducir de forma reconocible la imagen visualizada en el monitor del sistema bajo test.

En la figura 8 se puede apreciar un detalle de la pantalla del monitor con la imagen recibida. Por tratarse de una fotografía de una pantalla en funcionamiento, la calidad no es especialmente alta, aún así, es posible reconocer el patrón de la imagen original (figura 2).

La imagen reproducida presenta gran cantidad de ruido (nieve), lo cual suele asociarse a un nivel de señal insuficiente a la entrada de nuestro equipo receptor. Entre otras po-

Figura 8. Detalle de la imagen recibida en el monitor.

sibles causas que justifiquen la deficiente calidad de la imagen recibida, podemos mencionar la falta de sensibilidad del equipo receptor y el excesivo ancho de banda del canal utilizado en la demodulación (filtrado insuficiente).

No obstante, y a pesar del elevado nivel de ruido de la imagen recibida, con el presente experimento se ha demostrado que el TEMPEST sigue siendo un concepto de actualidad en los monitores CRT.

Conclusiones

Se ha reproducido y adaptado un experimento de TEMPEST aplicado a monitores CRT actuales, demostrándose que el TEMPEST sigue siendo un concepto de actualidad.

Con objeto de mantener la filosofía del experimento original, se han utilizado componentes comerciales de bajo coste en la medida de lo posible. Esta decisión ha limitado, en cierta medida, la calidad de los resultados obtenidos. Mención especial merece el hecho de haber utilizado un vídeo VHS como equipo receptor, puesto que sus características en cuanto a sensibilidad y ancho de banda del canal demodulado se apartan bastante de las características ideales requeridas.

Para obtener resultados de mayor calidad es necesario recurrir al uso de sistemas de prueba comerciales para emisiones TEMPEST (figura 9) que permiten obtener unos resultados muchos más satisfactorios que los obtenidos en este experimento. Podemos citar como ejemplo el sistema de medidas TEMPEST DSI-9000A comercializado por la empresa *Dynamic Sciences Inc* [4].

Destacar también la existencia de monitores CRT especialmente fabricados para minimizar las radiaciones electromagnéticas de TEMPEST, lo cual corrobora de nuevo la afirmación de la actualidad del concepto de TEMPEST. Generalmente, minimizar las emisiones TEMPEST de un monitor equivale a reducir las radiaciones electromagnéticas del mismo. Esto se consigue mediante un apantallamiento efectivo que minimice las radiaciones electromagnéticas. Además de las técnicas hardware de reducción de las emisiones TEMPEST (apantallamientos), podemos encontrar algunos estudios sobre técnicas software orientadas a minimizar la cantidad de información contenida en las emisiones TEMPEST. Un interesante ejemplo de estas técnicas software basado en el uso de fuentes gráficas de caracteres filtradas lo podemos encontrar en [2].

Por todo lo visto, podemos concluir que las emisiones TEMPEST siguen estando de actualidad y constituyen en sí mismas un amplio campo de estudio [3]. ❑

Referencias

[1] Wim van Eck, “Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?”, Computers & Security 1985 (vol. 4)

[2] Markus G. Kuhn and Ross J. Anderson, “Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations”, Springer-Verlag Berlin Heidelberg 1998

[3] Joel McMamara, “The Complete, Unofficial TEMPEST Information Page”, http://www.eskimo.com/~joelm/tempest.html

[4] “EMC, EMI, TEMPEST”, http://www.idm-instrumentos.es/Medidores/EMC.htm