Ataques de Canais Laterais Eletromagnéticos Ameaçam Seções Eleitorais Eletrônicas? Cenários e Recomendações

Lucas Brito[1], Leonardo Teodoro[1], Pedro Tomaz[1], Alyson Isaluski[1], Leandro Hyeda[1], Antonio Oliveira-Jr[2,3], Saulo Queiroz[1]

[1] Federal University of Technology – Paraná (UTFPR)
Ponta Grossa – PR – Brasil

{lbrito, lteodoro, pedrotomaz,

alysonisaluski, leandrohyeda}@alunos.utfpr.edu.br,

antoniojr@ufg.br, sauloqueiroz@utfpr.edu.br

[2]Federal University of Goiás (UFG)
Goiânia – GO – Brasil.

[3]Fraunhofer Portugal AICOS, Porto 4200-135, Portugal.

Abstract. *This paper investigates the threat of violating the secrecy of the Brazilian electronic voting machine through electromagnetic side-channel attacks, also known as TEMPEST attacks. In such attacks, screen information can be remotely reconstructed by intercepting electromagnetic emanations associated with the graphical signal of the target device. This work is motivated by the decision of electoral court in Brazil, in revoking a councilman's mandate due to the ballot secrecy violation based on electronic equipment. Based on publicly available information of the electoral process, attack scenarios against electronic polling stations are proposed. Experiments using software-defined radio demonstrate that the effectiveness of TEMPEST attacks is strongly conditioned by the absence of monitoring due to public unawareness of the threat Finally, awareness guidelines are proposed for voters, poll workers, and party representatives in order to mitigate attack risks in the context of an electronic polling station.*

Resumo. *Este artigo investiga a ameaça de violação do sigilo do voto da urna eletrônica brasileira (UEB) por meio de ataques de canais laterais eletromagnéticos, também conhecidos como ataques TEMPEST. Nesses ataques, informações de tela podem ser reconstruídas remotamente pela interceptação de emanações eletromagnéticas associadas ao sinal gráfico do dispositivo-alvo. O trabalho é motivado por uma recente decisão de um tribunal eleitoral brasileiro relacionada à tentativa de violação do sigilo do voto com equipamentos eletrônicos. Com base em informações publicamente disponibilizadas sobre o sistema eleitoral, são propostos cenários de ataque contra seções eleitorais. Experimentos com rádio definido por* software *evidenciam que a efetividade de ataques TEMPEST está fortemente condicionada à ausência de fiscalização por desconhecimento público da ameaça. Por fim, são propostas diretrizes de conscientização destinadas a eleitores, mesários e agentes partidários visando mitigar riscos do ataque no contexto de uma seção eleitoral.*

1. Introdução

Recentemente, o Tribunal Regional Eleitoral do Pará (TRE-PA) cassou o mandato de um vereador no município de Ourilândia do Norte (Pará) em decorrência da cooptação de eleitores para utilização de óculos com microcâmeras embutidas visando à violação do sigilo do voto da Urna Eletrônica Brasileira (UEB) [Tribunal Regional Eleitoral do Pará 2026]. Em perspectiva correlata, este trabalho investiga a ameaça de violação do sigilo do voto sob a ótica de ataques de canais laterais eletromagnéticos, também conhecidos como ataques TEMPEST [Ahmed Leghari et al. 2025].

Em um ataque TEMPEST contra um sistema gráfico, um adversário emprega um Rádio Definido por Software (*Software Defined Radio*, SDR) para interceptar as emanações eletromagnéticas inerentes ao trânsito do sinal de vídeo através dos componentes do sistema (e.g., cabos, conectores, circuitos, *display*). Com o devido processamento do sinal captado, um ataque bem sucedido é capaz de reconstruir a imagem de vídeo contida no sinal. Ressalta-se que esse ataque não compromete a integridade nem a disponibilidade do sistema, apenas sua confidencialidade. Considerando que a imagem precisa ser exibida de forma humanamente inteligível, métodos tradicionais de criptografia de dados não mitigam diretamente esse tipo de ameaça.

A primeira demonstração de um ataque TEMPEST descrita na literatura acadêmica ocorreu na década de 1980, ficando conhecida como "van Eck *phreaking*" em homenagem ao seu autor [van Eck 1985]. À época, o aumento da resolução dos *displays* impunha obstáculos naturais à exploração da ameaça, uma vez que tanto a complexidade computacional quanto a taxa de amostragem requerida eram proporcionais à taxa de pixels do *display*-alvo. Além disso, inexistiam SDRs comerciais compatíveis com os requisitos de aquisição e processamento do ataque. Superadas essas limitações tecnológicas, ataques TEMPEST passaram a ser investigados sob diferentes técnicas, cenários e dispositivos, incluindo sistemas multi-vídeo [Choi et al. 2024], *smartphones* [Cheng et al. 2025] e abordagens baseadas em aprendizado profundo [Fernández et al. 2024].

Considerando sistemas eleitorais eletrônicos, [Danilo André Jorge Patrício 2012] faz referência a um experimento TEMPEST baseado em canais laterais acústicos envolvendo o teclado da UEB, enquanto [Rohr 2009] menciona evidências de espionagem eletromagnética relacionadas a um modelo de urna distinto do brasileiro. Em ambos os casos, tratam-se de relatos sem detalhamento técnico suficiente para assegurar a reprodutibilidade dos experimentos. Em [Teodoro et al. 2026], os autores investigam assinaturas espectrais inerentes a sinais TEMPEST associados à interface gráfica da UEB mas não consideram cenários operacionais de ataque, nem discutem potenciais vulnerabilidades inerentes a uma seção eleitoral brasileira, como realizado neste estudo.

2. Sinal de Video

O sinal VGA, considerado por pelo menos dois modelos de UEB em operação[1], adota uma modulação por amplitude de pulso (*Pulse Amplitude Modulation*, PAM), na qual a informação dos pixels modula a amplitude de pulsos retangulares deslocados no tempo. Nessa modulação, cada pixel discreto $x[n]$ modula a amplitude de um pulso retangular $p(t)$ de duração T_p, produzindo um sinal contínuo modelado por

[1] `https://www.tre-sc.jus.br/eleicoes/urna-eletronica/modelos/`.

$$x(t) = \sum_{n=-\infty}^{\infty} x[n]p(t - nT_p), \tag{1}$$

onde $x(t)$ representa o sinal contínuo transmitido no instante de tempo t, e T_p representa o período temporal associado a cada pixel dado por

$$T_p = \frac{1}{P_x P_y f_v} \quad \text{segundos}, \tag{2}$$

sendo, P_x, P_y e f_v correspondentes ao número total de pixels por linha do quadro de tela, ao número de linhas por quadro e à taxa de atualização de quadros, respectivamente. A taxa de pixels correspondente é dada por $f_p = 1/T_p$ (comumente denotada em Hertz, Hz). É digno de nota que P_x e P_y incluem também os chamados *blank pixels*, empregados para sincronização entre a placa de vídeo e o monitor e que não representam conteúdo visível. A quantidade desses pixels para cada resolução é definida pelo padrão VESA [Video Electronics Standards Association (VESA) 2013].

A aplicação da transformada de Fourier ao sinal em (1) resulta em

$$X(f) = \mathcal{F}\{x(t)\} = P(f) \sum_{n} x[n] e^{-j2\pi f n T_p}, \tag{3}$$

em que

$$P(f) = \mathcal{F}\{p(t)\} = T_p sinc(f T_p) \tag{4}$$

corresponde à transformada de Fourier do pulso retangular, enquanto termo do somatório corresponde à Transformada de Fourier de Tempo Discreto (DTFT) da sequência de pixels. O espectro do sinal apresenta componentes espectrais espaçadas pela taxa de pixels $\Delta f = f_p = 1/T_p$ Hz, moduladas pelo envelope espectral $P(f)$. Embora a função $sinc$ apresente zeros exatamente em múltiplos inteiros de f_p – i.e., frequências em que um SDR apresenta chances de realizar um ataque TEMPEST –, na prática, limitações de largura de banda, tempos de subida de pulso não instantâneos e distorções introduzidas pelo canal eletromagnético alteram o formato ideal dos pulsos retangulares. Consequentemente, o sinal TEMPEST ainda apresenta energia observável em regiões próximas a tais frequências, permitindo ao adversário explorar essas componentes espectrais para reconstrução da imagem. Detalhes técnicos adicionais sobre o ataque TEMPEST podem ser encontrados em [Lee et al. 2025]. [Ahmed Leghari et al. 2025],[Larroca et al. 2022].

3. Cenários de Ataque e Experimentos

De acordo com informações atuais do TSE, o sistema eleitoral eletrônico brasileiro opera por meio dos modelos de UEs UE2013, UE2015, UE2020 e UE2022. Cada UE é instalada em cabines individuais de votação no interior das seções eleitorais. Durante o período de votação, diferentes agentes possuem acesso físico ao ambiente da seção, incluindo eleitores, mesários e fiscais partidários. Além disso, as seções eleitorais são frequentemente instaladas em prédios, preferencialmente públicos, cedidos temporariamente ao TSE para

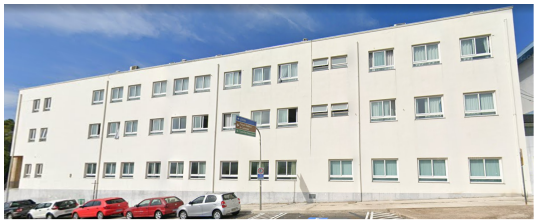

Figura 1. Seção eleitoral compatível com cenários de ataque propostos.

uso como local de votação. Com base nessas características, identificamos dois potenciais cenários de ataque TEMPEST contra uma seção eleitoral brasileira:

- **Cenário 1:** Neste cenário, um adversário com acesso a um espaço adjacente à sala da seção eleitoral (e.g., outra sala, corredor ou via pública) instala um conjunto SDR-computador capaz de operar local ou remotamente, caso o computador esteja conectado à Internet. O ataque explora o fato das cabines de votação serem frequentemente posicionadas próximas a paredes como forma de dificultar a visualização do voto por terceiros. Nessas condições, a proximidade física pode favorecer a captação do vazamento eletromagnético.
- **Cenário 2:** Neste cenário, um agente com acesso legítimo à sala da seção eleitoral pode ser cooptado para portar, durante o período de votação, um SDR portátil alimentado por bateria e capaz de armazenar sinais brutos para posterior análise *off-line*. Exemplos de SDRs adequados a esse cenário incluem Ettus USRP E312 e USRP-LW E3xx. Se executado adequadamente, esse ataque pode contornar a distância mínima de 0,5 metro a partir da qual a atenuação eletromagnética esperada nos modelos UE2020 e UE2022 inviabilizam um ataque TEMPEST [Tribunal Superior Eleitoral 2020].

A Fig. 1 ilustra a seção eleitoral n. 47 da 14a zona eleitoral em Ponta Grossa, Paraná, como um exemplo real de seção compatível com os cenários 1 e 2 descritos neste trabalho. Na imagem, observam-se salas adjacentes entre si e em relação à via pública, evidenciando que a cabine de votação pode estar separada desses ambientes por apenas uma parede de alvenaria.

Em todos os testes, foram adotadas as resoluções $1280 \times 768@60$ (i.e., $f_p = 74.25$ MHz), em conformidade com os modelos UE2013 e UE2015[2], e $1920 \times 1080@60$ ((i.e., $f_p = 148.5$ MHz, *Full HD*), como resolução superior à mínima exigida para os modelos UE2020 [Tribunal Superior Eleitoral 2019]. Até o melhor conhecimento dos autores, não há documentos públicos com informação de resolução do modelo UE2022. Nesses casos, a estimativa pode ser realizada a partir de algoritmos de autocorrelação discreta baseados na Transformada Rápida de Fourier (FFT) e abordagens derivadas [Lee et al. 2019], [Queiroz et al. 2025].

No cenário 1, considerou-se o SDR posicionado a aproximadamente 1 metro da UEB e separado desta por uma parede de alvenaria. No cenário 2, considerou-se uma distância inferior a 0,5 metro entre o SDR e a UEB, condição potencialmente favorável à realização de ataques TEMPEST contra os modelos UE2020 e UE2022. Para

[2]`https://www.justicaeleitoral.jus.br/tps/arquivos/2021/apresentacao-7-tps-2021-cotel-urna-eletronica.pdf`.

a interceptação dos sinais de vídeo, utilizou-se um rádio Ettus USRP B200 conectado a uma antena de TV digital e sintonizado em uma frequência harmônica da taxa de pixels de cada experimento. As amostras do SDR foram processadas por um *notebook* de 16 GB de RAM com processador Intel i7 da 12a geração. Note que, nos experimentos práticos, o cenário 2 foi representado pela proximidade física entre o SDR e o monitor-alvo, visto que o modelo empregado não dispõe de capacidade de armazenamento interno de amostras para processamento posterior. Para diferentes experimentos, foram identificados sinais visualmente legíveis nas harmônicas 3, 6 e 7 utilizando taxa de amostragem $f_s = 54$ MHz no SDR. Os sinais coletados foram posteriormente resincronizados com base nas resoluções conhecidas e convertidos em imagens por meio do módulo GNU Radio gr-tempest [Larroca et al. 2022].

Conforme se pode verificar nas Figs. 2a e 2b, em ambos os cenários do experimento foi possível identificar o número do candidato exibido nos respectivos monitores-alvo. Resultados similares também foram obtidos variando-se as imagens da UEB, o tipo de sinal (VGA/HDMI), e a resolução. Por limitações de espaço, uma síntese dos resultados, bem como os artefatos necessários à reprodução dos experimentos, encontram-se disponíveis no repositório do autor principal[3]. Adicionalmente, foram investigados cenários com mais paredes de separação e maiores distâncias entre o SDR e o monitor-alvo. Nesses casos, não foi possível reconstruir imagens visualmente inteligíveis devido à elevada distorção do sinal captado. Dessa forma, os resultados obtidos evidenciam que o risco de violação do sigilo do voto da UEB por meio de ataques TEMPEST eletromagnéticos está fortemente condicionado à proximidade física entre o adversário e a seção eleitoral. Assim, recomenda-se que mesários, eleitores e agentes partidários sejam orientados tanto sobre a existência de ataques TEMPEST quanto acerca de características estéticas e operacionais típicas de dispositivos SDR, visando reforçar a fiscalização e inibir esse tipo de ameaça.

(a) Cenário 1: ≈ 1 metro com parede. **(b) Cenário 2: menos de 0,5 metro sem obstáculos.**

Figura 2. Imagens resultantes de ataque TEMPEST através de parede de alvenaria (esquerda) e sem obstáculos (direita).

4. Conclusões e Recomendações

Este trabalho investigou a possibilidade de violação do sigilo do voto da Urna Eletrônica Brasileira (UEB) por meio de ataques de canais laterais eletromagnéticos baseados em

[3] `https://github.com/kewlzin/sbseg-ueb`.

Rádios Definidos por *Software* (SDR). Foram propostos dois cenários de ataque avaliados experimentalmente por meio de um monitor VGA reproduzindo características visuais da interface da UEB. No primeiro cenário, considerou-se um adversário com acesso a um ambiente adjacente à sala da seção eleitoral (e.g., outra sala, corredor ou via pública), localizado a aproximadamente 1 metro da UEB, e separado desta por uma parede de alvenaria. No segundo cenário, assumiu-se a cooptação de um agente com acesso legítimo à seção eleitoral (e.g., fiscal partidário, eleitor ou mesário) para portar um dispositivo de rádio compacto, alimentado por bateria e capaz de armazenar sinais para posterior análise *off-line*.

Em todos os cenários considerados foi possível inferir informações exibidas no monitor-alvo. O mesmo não foi verificado para distâncias maiores e/ou na presença de obstáculos adicionais. De forma geral, conclui-se que o risco associado a ataques TEMPEST contra a UEB está fortemente condicionado à proximidade física entre o adversário e a seção eleitoral, evidenciando a importância de ações de conscientização voltadas ao fortalecimento do processo de fiscalização. Especificamente para o primeiro cenário, recomenda-se evitar o posicionamento da UEB junto a paredes adjacentes a ambientes com reduzidas condições de fiscalização ou monitoramento. Quanto ao segundo cenário, conclui-se que o risco de violação do sigilo do voto por meio de SDRs apresenta semelhanças operacionais com casos envolvendo outros dispositivos eletrônicos portáteis, como o episódio relacionado ao uso de *smart glasses* que culminou na cassação de um vereador em Ourilândia do Norte (Pará). Nesse contexto, o desconhecimento público acerca de SDRs e da ameaça representada por ataques TEMPEST pode favorecer a atuação insuspeita de um adversário. Dessa forma, recomenda-se que mesários, eleitores e agentes partidários sejam orientados tanto sobre a existência de ataques TEMPEST quanto acerca de características estéticas e operacionais típicas de dispositivos SDR. Por fim, acredita-se que este trabalho possa estimular futuras discussões sobre segurança eletromagnética, transparência pública e mitigação de ataques baseados em canais laterais no contexto eleitoral brasileiro.

Agradecimentos

Este trabalho foi parcialmente financiado pelo projeto *Advanced Multimodal Sensing* (AIMS), apoiado pelo *Advanced Knowledge Center in Immersive Technologies* (AKCIT), com recursos financeiros do PPI IoT do MCTI, convênio nº 057/2023, firmado com a EMBRAPII. Os autores também agradecem à Fundação de Amparo à Pesquisa do Estado de Goiás (FAPEG) pelo apoio financeiro concedido a esta pesquisa (Projeto n. 64448878/2024).

Referências

Ahmed Leghari, M., Mei Pralle, S., Peik, S. F., Luetje, S., and Henkel, W. (2025). Waveform classification from TEMPEST attacks. *IEEE Access*, 13:167405–167423.

Cheng, Y., Zhu, S., Ou, C., Han, X., Li, Y., and Zheng, S. (2025). Capacitive touchscreens at risk: Recovering handwritten trajectory on smartphone via electromagnetic emanations. Aceito em ACM/IEEE Des. Autom. Conf. (DAC). Preprint. Acesso em: 26 maio 2026.

Choi, D.-H. et al. (2024). Analysis of leaked electromagnetic waves in multi-video systems with common clock and vertical synchronization. *IEEE Access*, 12:146818–146829.

Danilo André Jorge Patrício (2012). EMSEC (Emissors Security - Tempest): Uma forma alternativa de invasão de sistemas. `https://ric.cps.sp.gov.br/handle/123456789/1634`. Repositório Institucional do Conhecimento do Centro Paula Souza (RIC-CPS). Acesso em: 28 maio 2026.

Fernández, S., Martínez, E., Varela, J., Musé, P., and Larroca, F. (2024). Deep-tempest: Using deep learning to eavesdrop on hdmi from its unintended electromagnetic emanations. In *Proc. 13th Latin Amer. Symp. Dependable Secure Comput. (LADC)*.

Larroca, F., Bertrand, P., Carrau, F., and Severi, V. (2022). gr-tempest: an open-source GNU Radio implementation of TEMPEST. In *2022 Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*, pages 1–6.

Lee, E., Choi, D.-H., Nam, T., Kim, I., Yu, Y., and Yook, J.-G. (2025). Complete coherent demodulation and recovery of spread spectrum clocking-based electromagnetic information leakage: Theory and demonstration. *IEEE Trans. Inf. Forensics Security*, 20:3804–3818.

Lee, H. S., Choi, D. H., Sim, K., and Yook, J.-G. (2019). Information recovery using electromagnetic emanations from display devices under realistic environment. *IEEE Trans. Electromagn. Compat.*, 61(4):1098–1106.

Queiroz, S., Vilela, J. P., and Monteiro, E. (2025). Fast computation of the discrete fourier transform square index coefficients. *IEEE Signal Process. Mag.*, 42(2):88–92.

Rohr, A. (2009). Pesquisador diz ser possível 'espionar' urna eletrônica. `https://g1.globo.com/Noticias/Tecnologia/0,,MUL1274579-6174,00.html`. G1 Tecnologia. Acesso em: 23 mai. 2026.

Teodoro, L., Vieira, K. L., and Queiroz, S. (2026). Pre-Characterization of Electromagnetic Side-Channel Leakage Using Publicly Available Information: A Case Study on E-Voting Interfaces. Disponível em: `https://2026.ieeeicassp.org/industry_program/#DMOS_530`. *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.(ICASSP), Show & Tell Demo Session.*

Tribunal Regional Eleitoral do Pará (2026). Recurso eleitoral n 0600629-58.2024.6.14.0074. TRE-PA, 1ª Sessão Plenária Ordinária, 05 Abr 2025.

Tribunal Superior Eleitoral (2019). Audiência Pública UE2020: Especificações Técnicas de Hardware (Anexo II). Acesso em: 26 maio 2026.

Tribunal Superior Eleitoral (2020). UE2020 – Especificações Técnicas de Segurança (Anexo IV). Acesso em: 27 maio 2026.

van Eck, W. (1985). Electromagnetic radiation from video display units: An eavesdropping risk? *Computers & Security*, 4(4):269–286.

Video Electronics Standards Association (VESA) (2013). Industry Standards and Guidelines for Computer Display Monitor Timing (DMT), ver. 1.13, 2013. Acesso em: 22 maio 2026.