

Estimação Rápida de Taxa de Quadros em Ataques de Canais Laterais Eletromagnéticos de Sistemas Públicos

Alyson Isaluski¹, Leonardo Teodoro¹, Kleber V. Cardoso², Antonio Oliveira-Jr^{2,3},
Saulo Queiroz¹

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

{alysonisaluski, lteodoro}@alunos.utfpr.edu.br,

{kleber, antoniojr}@ufg.br,

sauloqueiroz@utfpr.edu.br

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

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

Abstract. *Frame refresh rate estimation is a fundamental step for the identification of compromising harmonic frequency in electromagnetic side-channel attacks. Methods based on Discrete Linear Auto-correlation (DLA) provide robustness across a wide range of scenarios, requiring a computational complexity of $O(N \log N)$ for a signal containing N samples. This work proposes a reduction of this complexity to $O(N)$ by exploiting prior knowledge of the target system's display resolution, as is the case for certain models of the Brazilian electronic voting machine. Experiments based on software-defined radios show that the proposed method preserves the accuracy of the conventional approach in the evaluated scenarios.*

Resumo. *A estimativa da taxa de atualização de quadros é uma etapa fundamental para identificação de frequência harmônica comprometedora em ataques de canais laterais eletromagnéticos. Métodos baseados em autocorrelação linear discreta (DLA, do inglês Discrete Linear Auto-correlation) apresentam robustez em diferentes cenários, exigindo complexidade computacional $O(N \log N)$ para um sinal de N amostras. Este trabalho propõe uma redução dessa complexidade para $O(N)$ explorando o conhecimento prévio da resolução gráfica do sistema-alvo, como ocorre em modelos da urna eletrônica brasileira. Experimentos baseados em rádios definidos por software mostram que o método proposto mantém a precisão da abordagem convencional nos cenários avaliados.*

1. Introdução

Ataques de Canais Laterais Eletromagnéticos (e-SCAs, do inglês *Electromagnetic Side-Channel Attacks*) referem-se a uma classe de ameaças de segurança nas quais informações sensíveis são inferidas a partir de emissões eletromagnéticas não intencionais produzidas pela movimentação de cargas elétricas. Tais ataques são comumente conhecidos

como ataques TEMPEST [Ahmed Leghari et al. 2025]. Neste trabalho, adotamos o termo TEMPEST para designar especificamente os e-SCAs voltados a dispositivos de vídeo.

Um desafio crítico em ataques TEMPEST é a estimação da Taxa de Atualização de Quadros (FRR, do inglês *Frame Refresh Rate*) a partir do sinal vazado, necessária para reconstruir a imagem interceptada e auxiliar na identificação de uma frequência harmônica comprometedora. Diferentes métodos para estimação da FRR têm sido considerados pela literatura [Nam et al. 2025], [Fernández et al. 2024], [Meynard et al. 2011]. Dentre esses, a auto-correlação linear discreta (DLA, do inglês *Discrete Linear Auto-correlation*) destaca-se como método popular entre bibliotecas TEMPEST práticas devido à sua eficiência de estimativa para cenários variados [Larroca et al. 2022], [Marinov 2014].

Este trabalho propõe um método para reduzir a complexidade computacional da DLA de $O(N \log N)$ para $O(N)$ em cenários nos quais a resolução gráfica do sistema-alvo é conhecida previamente, como observado por [Teodoro et al. 2026] em relação a alguns modelos da Urna Eletrônica Brasileira (UEB) em uso. O método proposto é validado a partir de sinais TEMPEST reais, obtidos em experimentos baseados em rádio definido por *software* (SDR, do inglês *Software-Defined Radio*).

2. Modelo do Sinal TEMPEST

Esta seção introduz a fundamentação teórica do trabalho. Primeiramente, na subseção 2.1, apresentamos os parâmetros do sinal TEMPEST necessários ao método proposto. Então, na subseção 2.2, apresentaremos o método DLA, a ser otimizado neste trabalho quanto ao quesito complexidade computacional.

2.1. Parâmetros TEMPEST Básicos

O sinal VGA assumido neste trabalho pode ser modelado por uma soma de pulsos retangulares:

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

onde $x(t)$ representa o sinal contínuo real no instante de tempo t . O período (i.e., tempo de duração) T_p de cada pixel (pulso) no cabo depende da resolução e taxa de atualização da tela (*frame rate*). T_p pode ser definido como:

$$T_p = \frac{1}{P_x P_y f_v} \text{ s}, \quad (2)$$

onde P_x , P_y e f_v representam o número de pixels em uma linha (incluindo pixels de sincronização, i.e., *blanking pixels*), o número de linhas em um quadro de tela e a taxa de atualização, respectivamente. A possibilidade de ataques TEMPEST decorre das distorções inerentes aos componentes analógicos do sistema de vídeo responsáveis por causar vazamentos em frequências harmônicas múltiplas da taxa de pixels [Ahmed Leghari et al. 2025], [Lee et al. 2025], [Lee et al. 2019]. Um adversário que sintonize um SDR em uma dessas frequências pode recuperar a imagem nela contida.

2.2. Estimativa FRR com o Método DLA

Após a obtenção do sinal bruto por meio de um SDR em um ataque TEMPEST, torna-se necessário estimar a taxa de atualização de quadros f_v . O método DLA baseia-se na

identificação do pico dominante da função de autocorrelação. Para um sinal complexo discreto $x[n]$ contendo N amostras, a autocorrelação no *lag* τ é dada por

$$R_{xx}(\tau) = \sum_{n=\tau}^{N-1} x[n]x^*[n-\tau], \quad 0 \leq \tau < N, \quad (3)$$

onde $x^*[n]$ denota o conjugado complexo de $x[n]$. Para uma taxa de amostragem f_s , a estimativa da FRR é obtida por

$$f_v \approx f_s / \tau_{\max}, \quad (4)$$

em que $\tau_{\max}$ corresponde ao *lag* associado ao maior pico de (3).

Uma implementação direta da DLA avalia a autocorrelação para todos os *lags* de interesse, resultando em complexidade $O(N^2)$. Para reduzir esse custo, ferramentas TEMPEST amplamente utilizadas [Larroca et al. 2022], [Marinov 2014] recorrem ao teorema de Wiener–Khinchin, segundo o qual a autocorrelação pode ser obtida a partir da transformada inversa de Fourier do espectro de potência do sinal. Assim, com base no algoritmo da transformada rápida de Fourier (FFT, do inglês *Fast Fourier Transform*) e sua inversa (IFFT), o método DLA opera em tempo $O(N \log N)$. Embora eficiente no caso geral, o custo computacional associado ao processamento de sinais com milhões de amostras – como os sinais TEMPEST considerados neste trabalho – pode tornar-se um fator limitante em aplicações críticas sujeitas a restrições temporais rigorosas, como demonstrado em [Queiroz et al. 2022].

3. O Método *Fast DLA* (F-DLA)

O método proposto, denominado F-DLA (*fast DLA*), reduz a complexidade computacional do método convencional DLA explorando cenários TEMPEST nos quais os parâmetros P_x e P_y podem ser conhecidos *a priori*. Embora essa seja uma premissa forte em cenários TEMPEST em geral, a hipótese de desconhecimento dos parâmetros do sistema-alvo pode ser relaxada em contextos pautados por princípios de transparência, como ocorre no sistema eleitoral brasileiro. Especificações públicas estabelecem resoluções de 1280×768 para os modelos UE2013/UE2015 [Tribunal Regional Eleitoral de Santa Catarina 2026] e de, no mínimo, 1280×720 para o modelo UE2020 [Tribunal Superior Eleitoral 2019]. Assim, mesmo sem conhecimento prévio do modelo em uso, o padrão VESA restringe o conjunto de FRRs candidatas a apenas $R = 4$ valores para as resoluções dadas: 60, 75, 85 e 120 Hz [Video Electronics Standards Association (VESA) 2013]. Logo, o primeiro pico significativo de autocorrelação é esperado em um dos *lags* $\{f_s/60, f_s/75, f_s/85, f_s/120\}$, sendo $R = O(1)$ em relação a N .

A correta operação do método DLA pressupõe que as distorções introduzidas pelo canal não desloquem o pico dominante da autocorrelação para além do intervalo associado à FRR correta. Caso contrário, mesmo o método DLA convencional produziria uma estimativa incorreta. Portanto, nos cenários em que o DLA convencional opera corretamente, o deslocamento δ deve permanecer limitado por uma constante independente de N . Consequentemente, apenas os *lags* situados em uma vizinhança de δ amostras ao redor dos R candidatos precisam ser avaliados. Assim, como $R = O(1)$ e $\delta = O(1)$, o

conjunto $\mathcal{T}$ de *lags* candidatos cujos valores de auto-correlação precisam ser avaliados possui tamanho

$$|\mathcal{T}| = (2\delta + 1)R = O(1). \quad (5)$$

À semelhança da Eq. (4), o método F-DLA estima a FRR como

$$f_v \approx \frac{f_s}{\tau_{F-DLA}}, \quad (6)$$

em que $\tau_{F-DLA} \in \mathcal{T}$ é o *lag* que maximiza a função de autocorrelação

$$R_{xx}(\tau_{F-DLA}) = \max_{\tau \in \mathcal{T}} R_{xx}(\tau) \quad (7)$$

Como cada *lag* em $\mathcal{T}$ é avaliado em tempo $O(N)$ (3), e essa lista possui tamanho constante (5), a complexidade final do método F-DLA é

$$T_{F-DLA}(N) = |\mathcal{T}|N = O(N), \quad (8)$$

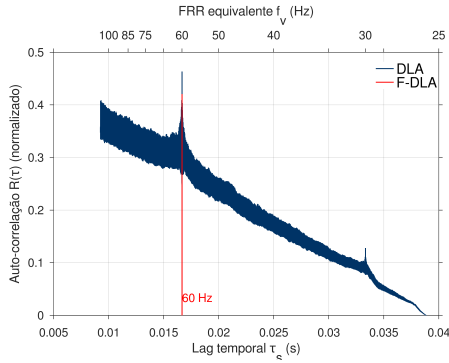
portanto, inferior à complexidade $O(N \log N)$ do método DLA convencional. Sob degradação severa do canal, a premissa de $\delta = O(1)$ pode deixar de ser válida, comprometendo a estimativa de FRR tanto pelo DLA quanto pelo F-DLA. Como este trabalho busca validar o F-DLA como alternativa ao DLA em ao menos um cenário real, a avaliação em canais degradados é deixada para trabalhos futuros.

4. Resultados Preliminares

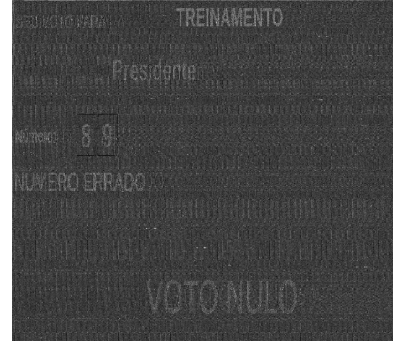
Nesta seção, o método F-DLA proposto é comparado ao método DLA convencional em termos de tempo de execução e precisão da estimativa de f_v , utilizando sinais obtidos em um experimento TEMPEST real baseado em SDR. Nos experimentos, foi utilizado um monitor VGA exibindo a interface da UEB (disponível em [Tribunal Superior Eleitoral 2026]), configurado com FRR $f_v = 60$ Hz e resolução gráfica de 1280×720 , compatível com o modelo UE2020. Para essa configuração, obtêm-se $P_x = 1650$ pixels e $P_y = 750$ linhas por quadro, de acordo com o padrão VESA [Video Electronics Standards Association (VESA) 2013]. Para mais detalhes sobre os resultados apresentados nesta seção, bem como outros resultados omitidos por limitações de espaço, solicitamos ao leitor que consulte o repositório do autor principal¹.

O sinal TEMPEST do vídeo foi capturado por um SDR Ettus USRP B200 conectado a uma antena de TV digital posicionada a ≈ 20 cm do monitor e operando com taxa de amostragem $f_s = 54$ MHz. Foram consideradas $N = 2^{21}$ amostras para ambos os métodos. Esse número é suficiente para capturar a quantidade mínima de dois quadros consecutivos, correspondente a $2(f_s/f_v) = 1,8 \times 10^6$ amostras no cenário considerado. Como referência para o método DLA convencional, foi utilizada a função `xcorr` do pacote *signal* do GNU Octave. Para o método proposto F-DLA, o menor valor δ capaz de produzir a estimativa correta de f_v nos experimentos foi igual a 1. Embora preliminares, os resultados experimentais corroboram os ganhos teóricos discutidos na Seção 3. Em

¹<https://github.com/AlysonIsa/SBSeg-FDLA>.



(a) Gráfico da função de auto-correlação.



(b) Imagem TEMPEST reconstruída dos experimentos.

Figura 1. F-DLA (proposto) e DLA (convencional): identificação de FRR em um canal TEMPEST experimental. O pico de autocorrelação em $\tau_s \approx 0,016667$ s obtido por ambos os métodos em (a) corresponde à FRR correta de 60 Hz da imagem reconstruída em (b).

uma versão expandida deste trabalho, pretende-se realizar uma avaliação experimental mais abrangente.

A Fig. 1a apresenta a função de autocorrelação do sinal TEMPEST cuja imagem reconstruída com base no módulo gr-tempest [Larroca et al. 2022], é exibida na Fig. 1b. O lag temporal τ_s , em segundos, foi obtido pela relação $\tau_s = \tau / f_s$. O pico de autocorrelação identificado pelo método F-DLA (barra vermelha) em $\tau_s = 0,016667$ s coincide com aquele obtido pelo método DLA (curva azul) e corresponde à FRR esperada de $1/\tau_s \approx 60$ Hz. Entretanto, o método F-DLA produziu essa estimativa em aproximadamente 0,30 s, com intervalo de confiança (IC) de $\pm 0,01$ s (95% de confiança), enquanto o método DLA convencional requereu aproximadamente 0,67 s, com IC de $\pm 0,02$ s. A diferença observada reflete constantes de implementação e otimizações da função `xcorr`, não apenas a ordem assintótica dos algoritmos. Esse resultado indica que a restrição do conjunto de lags candidatos a partir do conhecimento prévio de P_x e P_y , como no caso da UEB, permite reduzir o custo computacional da estimação sem comprometer a precisão da FRR no cenário avaliado.

5. Conclusão

Este trabalho apresentou o método *Fast DLA* (F-DLA), uma alternativa de baixa complexidade para a estimação da taxa de atualização de quadros em ataques TEMPEST. O método explora cenários nos quais parâmetros do sistema gráfico alvo podem ser conhecidos *a priori*, restringindo o conjunto de lags candidatos avaliados pela autocorrelação. Sob essa premissa, demonstrou-se que a complexidade computacional pode ser reduzida de $O(N \log N)$ para $O(N)$. Resultados obtidos em um experimento TEMPEST real baseado em SDR mostraram que o método F-DLA preserva a precisão da estimativa de FRR do método DLA convencional, ao mesmo tempo em que reduz o tempo de processamento. Embora preliminares, esses resultados corroboram a análise teórica desenvolvida e indicam o potencial da abordagem para aplicações com requisitos computacionais mais restritivos. Como trabalho futuro, pretende-se ampliar a avaliação experimental para diferentes cenários e parâmetros, bem como considerar técnicas de otimização de complexidade baseadas em FFT esparsas, e.g. [Queiroz et al. 2025].

Agradecimentos

Este trabalho foi parcialmente financiado pelo projeto *Advanced Multimodal Sensing* (AIMS), apoiado pelo *Advanced Knowledge Center in Immersive Technologies* (AK-CIT), com recursos financeiros do PPI IoT do MCTI, convênio nº 057/2023, firmado com a EMBRAPIL. 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.
- 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 Transactions on Electromagnetic Compatibility*, 61(4):1098–1106.
- Marinov, M. (2014). Tempestsdr: Remote video eavesdropping using a software-defined radio platform. <https://github.com/martinmarinov/TempestSDR>. Acessado em: 28 maio 2026.
- Meynard, O., Réal, D., Guilley, S., Flament, F., Danger, J.-L., and Valette, F. (2011). Characterization of the electromagnetic side channel in frequency domain. In *Inf. Security Cryptol. (Inscrypt), LNCS 6584*, pages 471–486.
- Nam, T., Choi, D.-H., Lee, E., and Yook, J.-G. (2025). Integrating Advanced Signal Analysis and Deep Learning in TEMPEST Techniques. In *Proc. IEEE Int. Symp. Electromagn. Compat., Signal & Power Integr. (EMC+SIPI)*, pages 66–71.
- Queiroz, S., Vilela, J. P., and Monteiro, E. (2022). Is FFT Fast Enough for Beyond 5G Communications? A Throughput-Complexity Analysis for OFDM Signals. *IEEE Access*, 10:104436–104448.
- 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.
- 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 de Santa Catarina (2026). Modelos de urna eletrônica. <https://www.tre-sc.jus.br/eleicoes/urna-eletronica/modelos/>. Acesso em: 3 jun. 2026.

Tribunal Superior Eleitoral (2019). Audiência Pública UE2020: Especificações Técnicas de Hardware (Anexo II). Disponível em: <https://www.tse.jus.br/servicos-judiciais/audiencias-publicas/arquivos/ue2020/tse-audiencia-publica-ue2020-especificacoes-tecnicas-hardware>. Acesso em: 26 maio 2026.

Tribunal Superior Eleitoral (2026). Simulador de Votação da Urna Eletrônica Brasileira. Disponível em: <https://www.tse.jus.br/hotsites/simulador-de-votacao/inicioVotacao.html>. Acesso em: 23 maio 2026.

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.