*URSI GASS 2023, Sapporo, Japan, 19 – 26 August 2023*

# Fundamental Study on TEMPEST Under Limited Measurement Performance

Taiki Kitazawa(1), Hiroyuki Kubo (2), and Yuichi Hayashi(1)
(1) Nara Institute of Science and Technology, Ikoma, Japan; e-mail: kitazawa.taiki.kq8, yu-ichi@is.naist.jp
(2) Chiba University, Chiba, Japan; e-mail: hkubo@chiba-u.jp

TEMPEST, a threat used for eavesdropping screen information through electromagnetic (EM) emissions from video display units (VDUs), is traditionally executed remotely using an expensive non-portable setup [1], [2]. However, recent research has shown that it is possible to perform similar attacks in the proximity of the target using a low-cost portable setup [3]. However, the limitations of the measurement instruments impact the acquisition of pixel information from leaked EM waves at each screen frame, missing many pixels and being unable to sample arbitrary pixels. In this paper, we propose a method to reconstruct images with sufficient quality to restore screen information overcoming the existing limitations of measurement instruments.

As VDUs typically update their screens at regular intervals (e.g., at approximately 60 Hz), an attacker can observe multiple frames carrying identical information if the screen content does not change frequently. However, a sampling rate of the instrument lower than the clock frequency that transmits each pixel in the VDU may result in missing pixel information at each frame. Additionally, a low gain and high noise floor may obscure some pixel information. In such cases, averaging over multiple frames, which is a conventional method used to improve information restoration, may yield unstable results owing to the significant variance of each pixel. Therefore, we propose a method that extracts sufficient pixel information needed to recover screen data by estimating a plausible image using an optimization problem.

We consider an observation signal $b$ measured at $M$ samples over multiple frames. We define this signal as a function of the screen information $x$ to be restored at a certain time window, as follows: $b = \int a(t)x(t)\,dt$, where $a$ represents the response function. Using this formulation, the following non-negative least-squares optimization problem is solved to restore the screen image.

$$\underset{x(t)}{\operatorname{argmin}} \sum_{i}^{M} \left\| b_i - \int a_i(t)x(t)dt \right\|_2^2 + \alpha E_{smooth} + \lambda E_{sparse},$$
$$\text{s.t. } x(\mathrm{t}) \geq 0, E_{smooth} = \|\nabla \tilde{x}\|_2^2, E_{sparse} = \|\tilde{x}\|_1 , \quad (1)$$

where the regularization terms $E_{smooth}$ and $E_{sparse}$ are added, weighted by the respective coefficients $\alpha$ and $\lambda$, to further improve the restored image, promoting smoothness and sparseness. The variable $\tilde{x}$ represents the two-dimensional screen information obtained by flattening $x$.

We compared the images reconstructed by the conventional averaging method with those obtained by the proposed approach using an actual display as the experimental target. The measurement device used in the experimental environment was the HackRF One [4]; it can be easily purchased for several hundred of US dollars. Figure 1 shows a part of the attack target and reconstructed images. We confirmed that the reconstructed image using the proposed method clearly improves visibility compared to the conventional method.

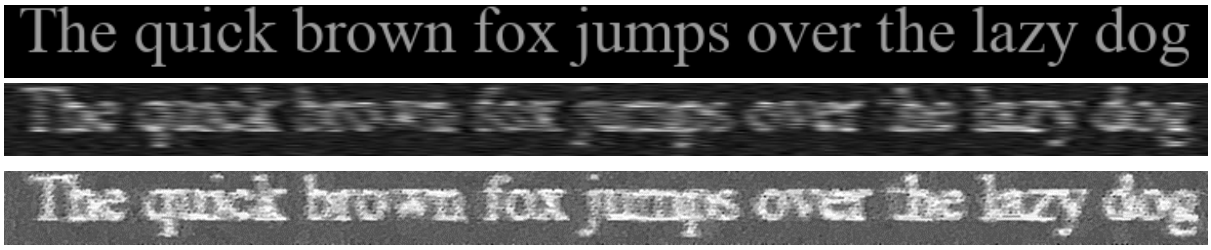


**Figure 1** A target image (top), a reconstructed image using conventional (middle) and proposed (bottom)

[1] T. Kitazawa, et al., *IEEE Trans. Electromagn. Compat.*, vol. 64, no. 6, pp. 1941–1948, Dec. 2022.
[2] D.-H. Choi, et al., *IEEE Electromagnetic Compatibility Magazine*, vol. 11, no. 3, pp. 77–83, 2022.
[3] Y. Hayashi, et al., *2014 ACM SIGSAC Conference on CCS*, pp. 954–965, 2014.
[4] "Great Scott Gadgets, HackRF One." https://greatscottgadgets.com/hackrf/one/ (accessed Jan. 2023).