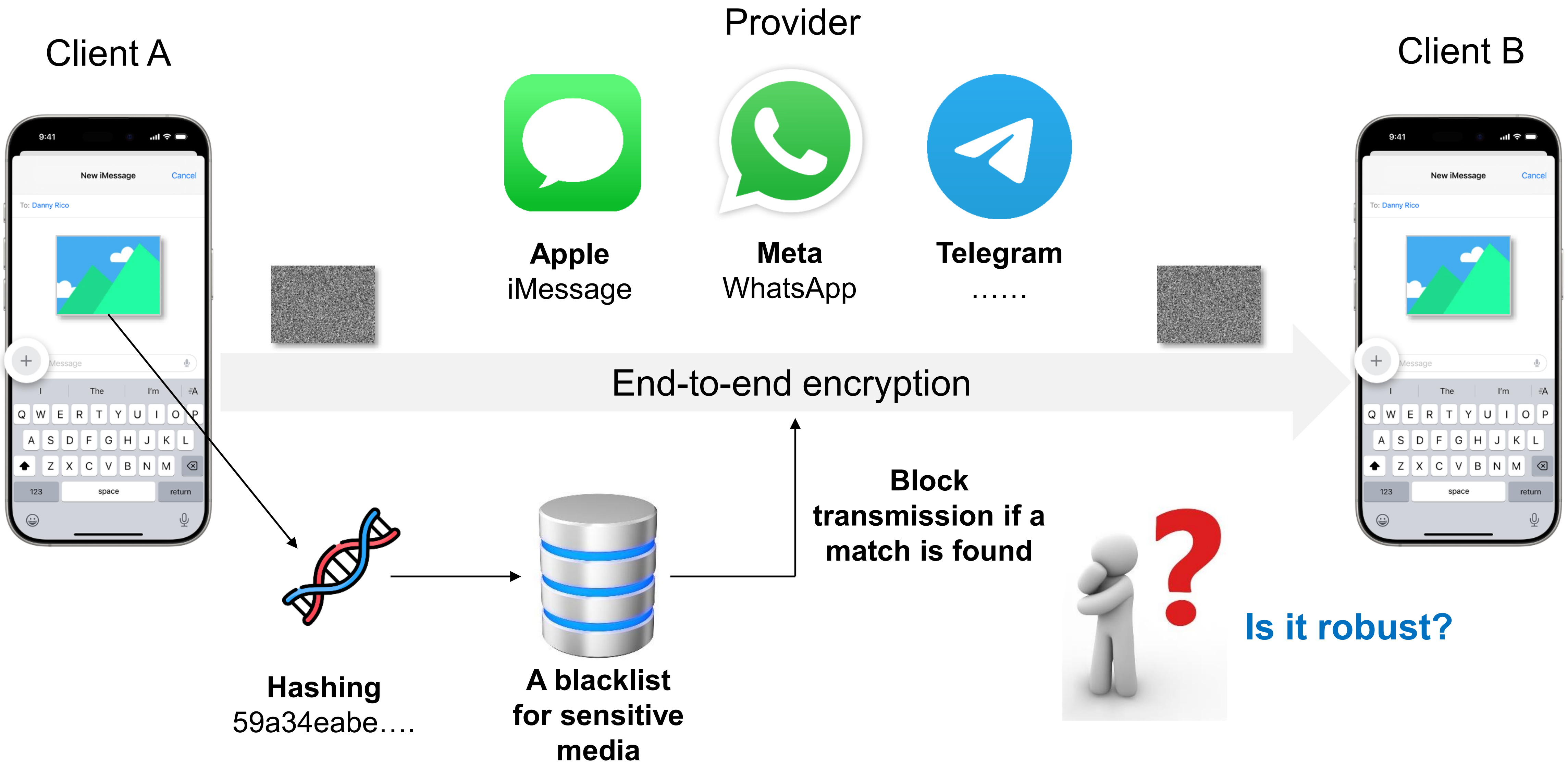
`Atkscopes`: Multiresolution Adversarial Perturbation as a Unified Attack on Perceptual Hashing and Beyond

The 34th USENIX Security Symposium, Seattle, 2025

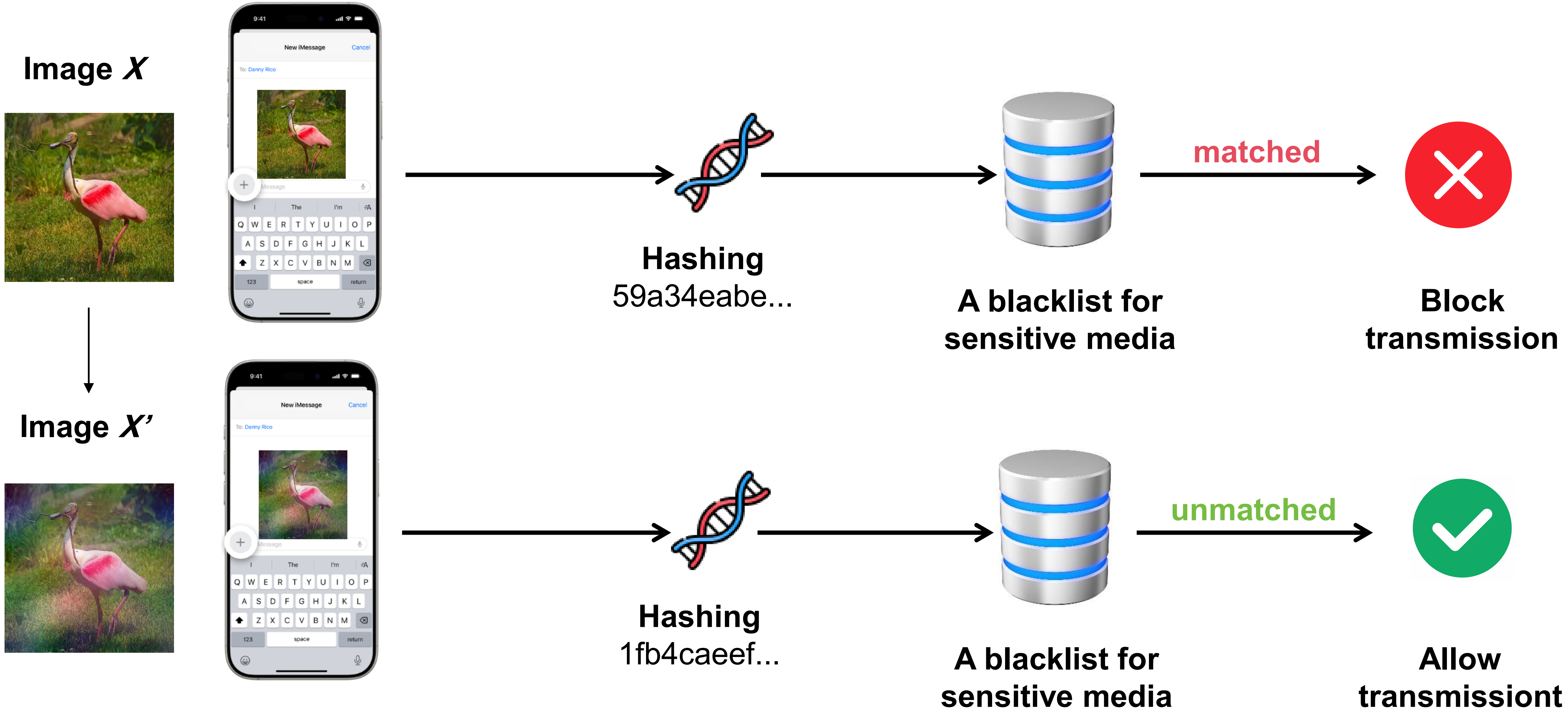
Yushu Zhang[1], Yuanyuan Sun[1], Shuren Qi[1]*, Zhongyun Hua[2], Wenying Wen[3], and Yuming Fang[3]

[1] Nanjing University of Aeronautics and Astronautics
[2]Harbin Institute of Technology, Shenzhen
[3]Jiangxi University of Finance and Economics
*Corresponding author: Shuren Qi, https://shurenqi.github.io/

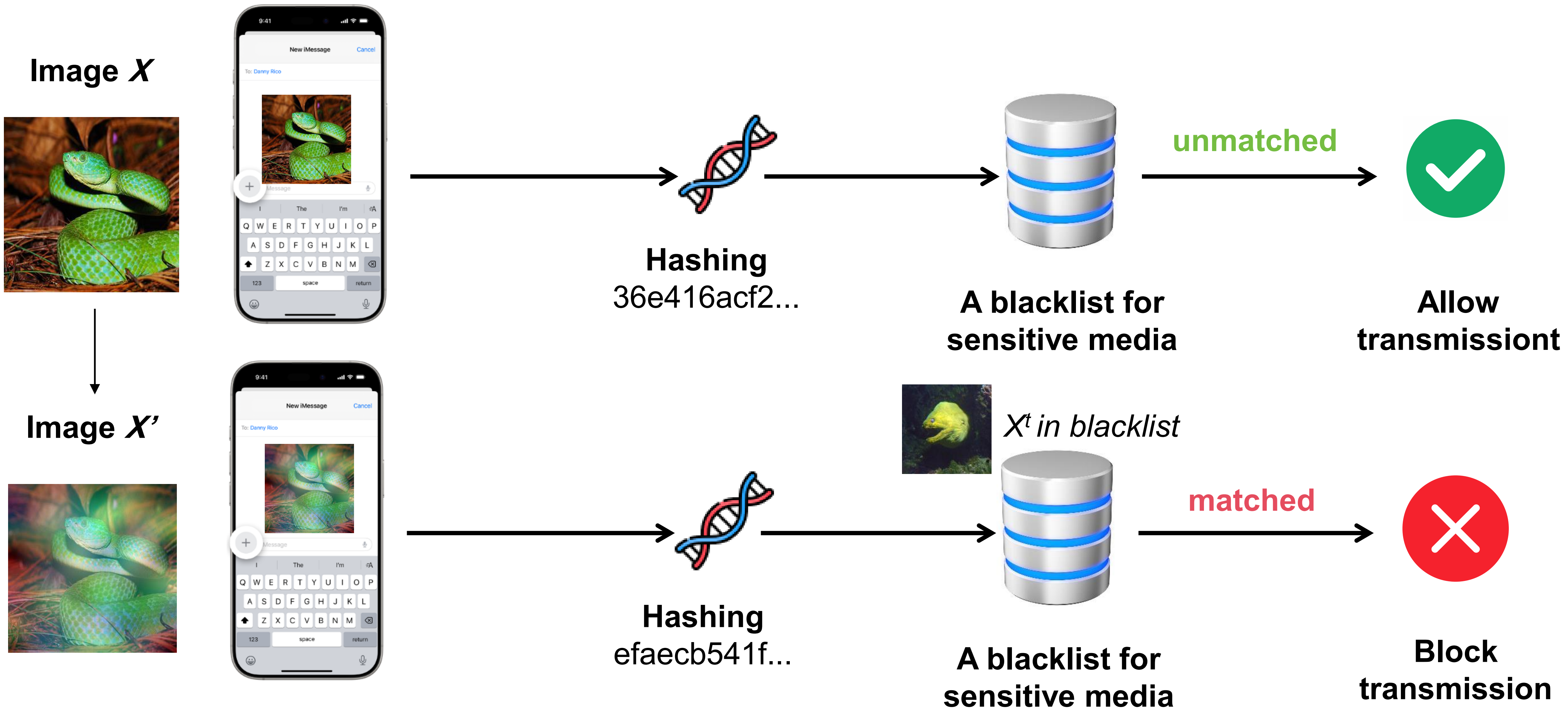
Privacy v.s. Regulation



Case 1: Escaping Regulation Attack



Case 2: Triggering Regulation Attack



`Atkscopes`: Multiresolution Adversarial Perturbation

Definition 1. ***(Multiresolution perturbation).*** *The addition of multiresolution perturbation is defined as follows:*

$$X'_{(x,y)\in D_{uvw}} = \mathcal{F}^{-1}\left(\mathcal{F}(X)+\delta\right), \tag{3}$$

with notations of

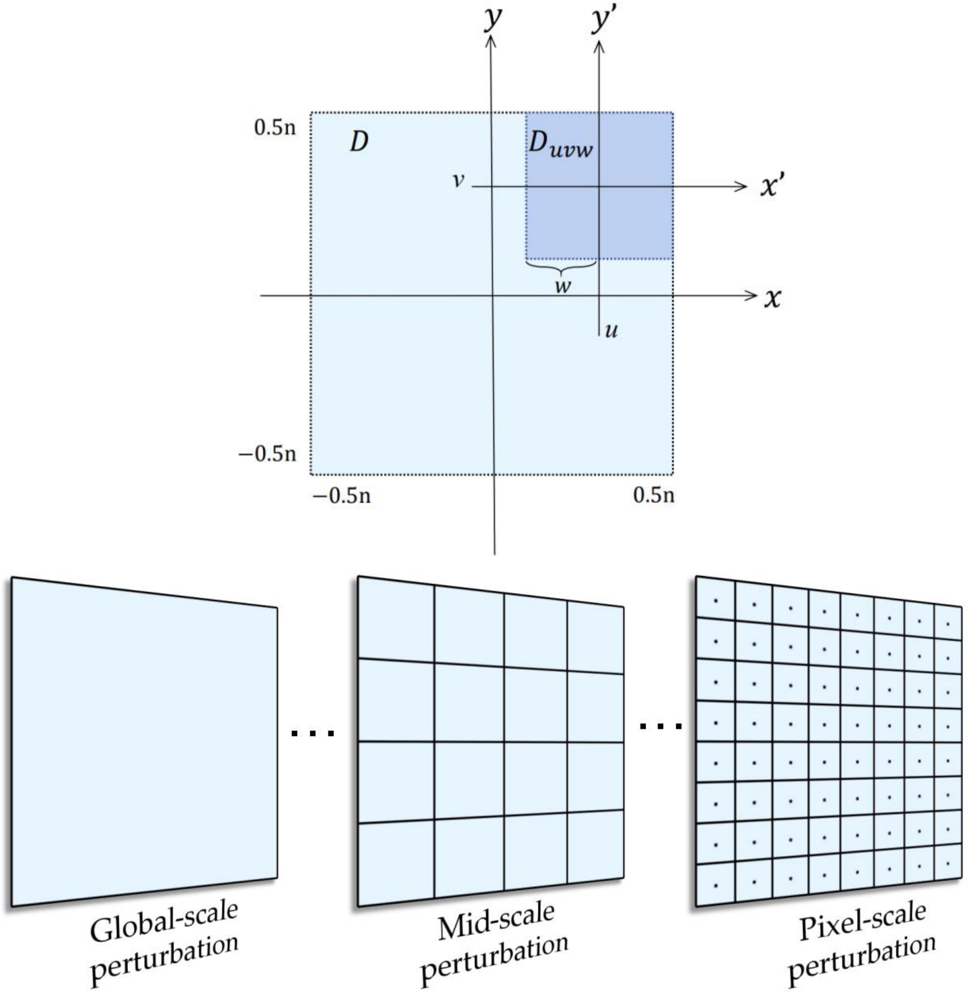
$$\mathcal{F}(X) = \langle X, V_{nm}^{uvw}\rangle = \iint_D (V_{nm}^{uvw}(x,y))^* X(x,y)dxdy, \tag{4}$$

and

$$\mathcal{F}^{-1}(\mathcal{F}(X)) = \sum_{n,m} V_{nm}^{uvw}(x,y)\mathcal{F}(X), \tag{5}$$

where $\mathcal{F}$ denotes the local orthogonal transformation [39], with image $X(x,y)$ on domain $(x,y)\in D$. The local orthogonal basis function V_{nm}^{uvw} is defined on the domain D_{uvw} with the order parameters $(n,m)\in\mathbb{Z}^2$, converting D to D_{uvw} by the translation offset (u,v) and the scaling factor w, as illustrated in Figure 2. Note that the local orthogonal basis function V_{nm}^{uvw} can be defined from any global orthogonal basis function V_{nm}, e.g., a family of harmonic functions, with following form:

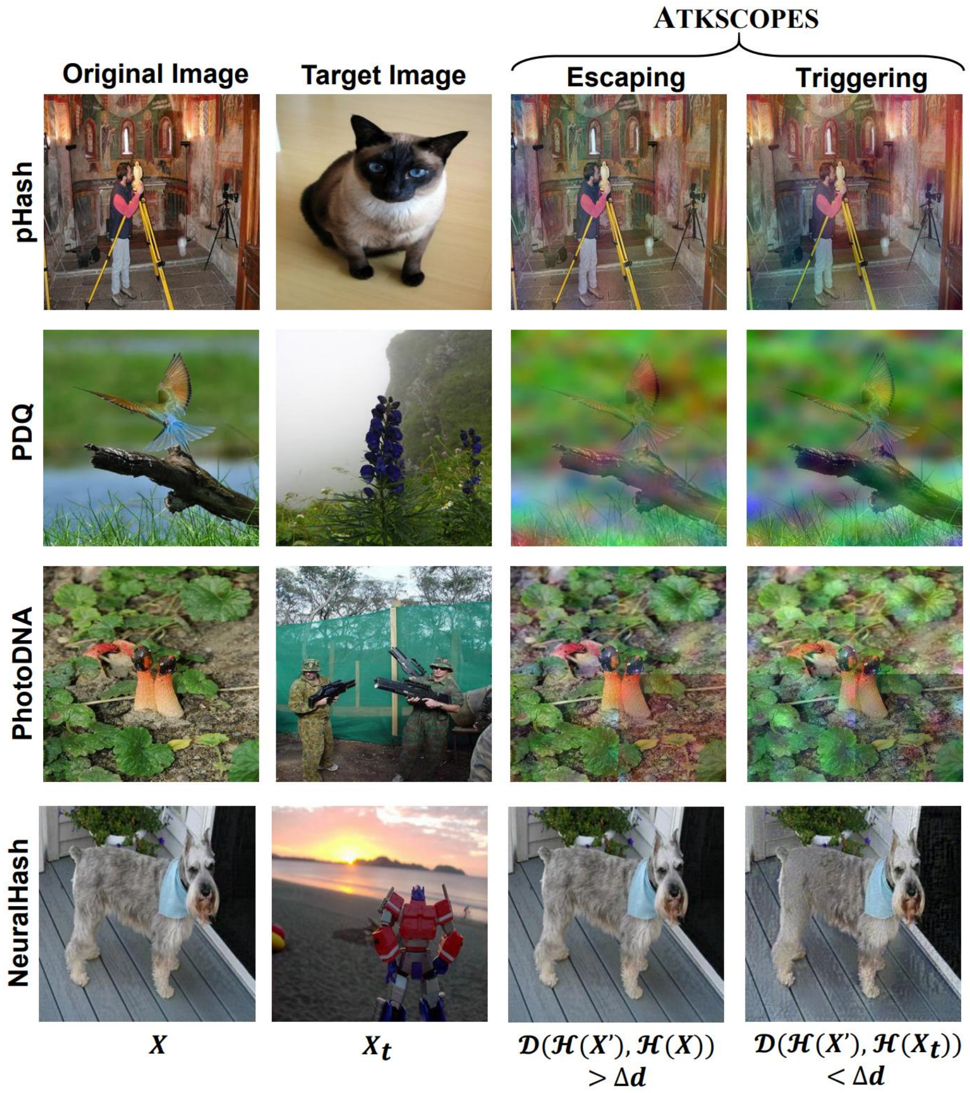
$$V_{nm}^{uvw}(x,y) = V_{nm}(x',y') = V_{nm}\left(\frac{x-u}{w},\frac{y-v}{w}\right). \tag{6}$$

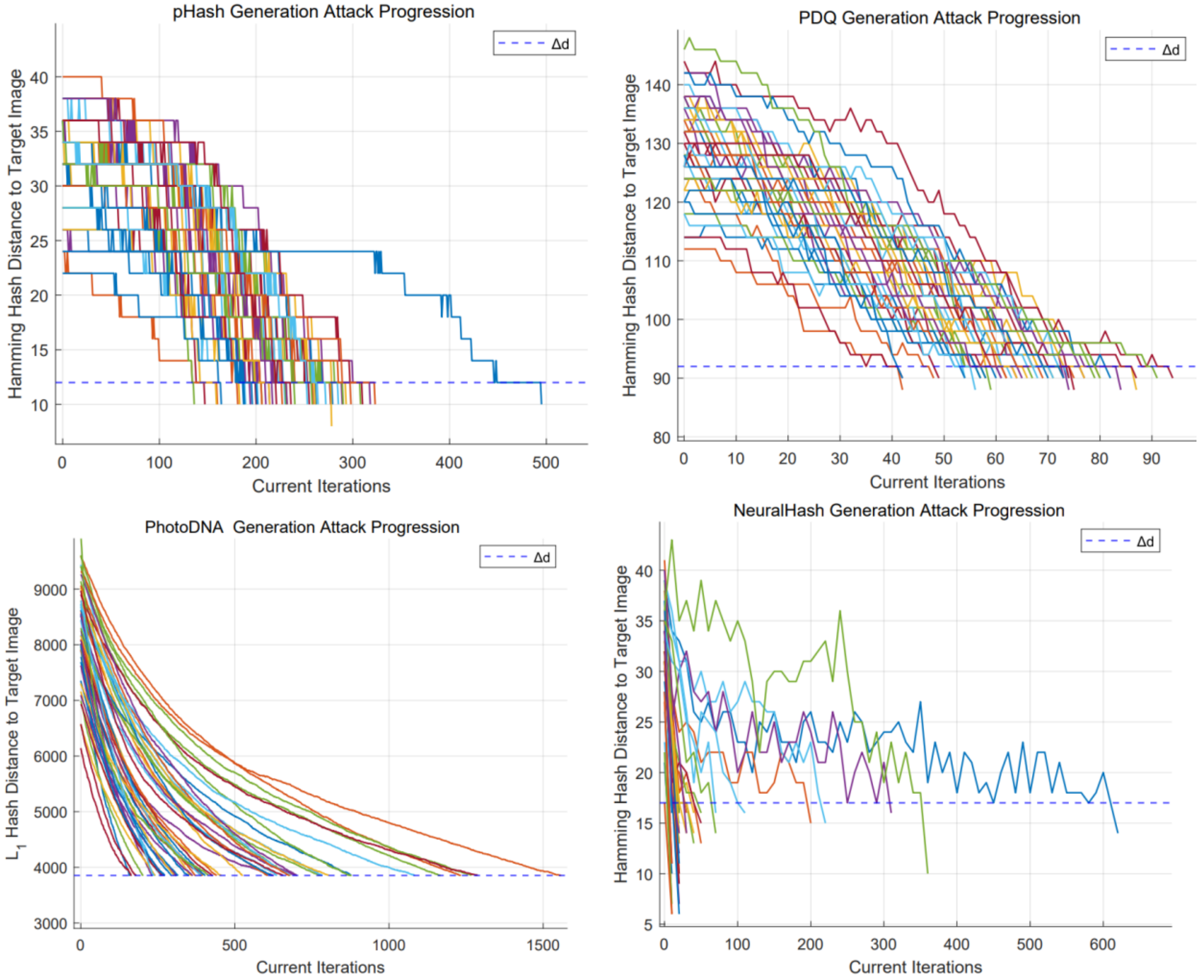


Uniform, Fast, and Successful Attacks

Meta

Microsoft





Q & A