

A APPENDIX

A.1 ABLATION STUDY

In this section, we present an ablation study to evaluate the contribution of different components in our proposed adversarial attack framework. The study is divided into two parts: (1) analyzing the impact of spatial and spectral attention mechanisms, and (2) evaluating the contributions of the local pixel dependency attack and the Multiscale attack. The results of the ablation experiments are summarized in Table 3.

A.1.1 SENSITIVITY ANALYSIS OF SCALE FACTORS AND WINDOW SIZE

To investigate the impact of key hyperparameters in our adversarial attack framework, we conducted ablation experiments on (1) the set of scale factors S used in the Multiscale Information Attack and (2) the window size N employed in the Local Pixel Dependency Attack. These parameters control the granularity of Multiscale perturbations and the extent of local spatial averaging, respectively.

(a) Effect of Scale Factors S : We evaluated the framework using four different scale sets:

Spatial Attention	Spectral Attention	Local Pixel	Multiscale	Norma Tissue(\uparrow)	Tumor Tissue(\downarrow)	Hyper vascularized(\uparrow)	Background(\uparrow)
✓	×	✓	✓	85.94	30.67	84.24	89.76
×	✓	✓	✓	79.04	26.49	75.97	83.43
✓	✓	✓	×	95.31	15.48	91.74	94.98
✓	✓	×	✓	98.49	12.76	95.06	96.24
✓	✓	✓	✓	94.89	8.46	89.25	94.51

Table 3: Performance Comparison with Different Attention Mechanisms and Methods.

$$S_1 = \{1\}, \quad S_2 = \{1, 2\}, \quad S_3 = \{1, 2, 4\}, \quad S_4 = \{1, 2, 4, 8\}$$

As shown in Table 4, introducing more scales improves the effectiveness of the attack. However, excessive scaling may over-smooth the perturbation and slightly reduce attack sharpness. Therefore, $S = \{1, 2, 4\}$ is selected as the optimal configuration.

Table 4: Effect of Scale Factors S on Attack Effectiveness (Tumor Class Accuracy \downarrow)

Scale Factors S	Tumor Acc. (%) \downarrow
$\{1\}$	50.87
$\{1, 2\}$	27.43
$\{1, 2, 4\}$	9.27
$\{1, 2, 4, 8\}$	16.36

(b) Effect of Window Size N :

To assess the sensitivity to local spatial context, we varied the window size N in the Local Pixel Dependency Attack as:

$$N = 3 \times 3, 5 \times 5, 7 \times 7, 11 \times 11$$

As shown in Table 5, moderate window sizes such as 5×5 offer the best trade-off between spatial coherence and attack precision. Larger windows may dilute local structures, weakening the perturbation’s targeting power.

Table 5: Effect of Window Size N on Attack Effectiveness (Tumor Class Accuracy \downarrow)

Window Size N	Tumor Acc. (%) \downarrow
3×3	28.74
5×5	12.55
7×7	19.49
11×11	26.68

A.1.2 ABLATION STUDY ON ATTENTION MECHANISMS AND ATTACK COMPONENTS

We systematically evaluate the contributions of spatial and spectral attention mechanisms and core attack components through ablation studies in Table 3. When removing both spatial and spectral attention, tumor classification accuracy rises to 30.67%, indicating degraded feature detection capability. Isolating spectral attention removal further degrades performance (26.49% tumor accuracy), underscoring its critical role in leveraging spectral dependencies. Incorporating both mechanisms significantly enhances attack effectiveness, reducing tumor accuracy to 12.76%.

For core attack components, the Multiscale attack alone achieves 15.48% tumor accuracy by disrupting multiresolution features, while the local pixel attack reaches 12.76% by exploiting spatial dependencies. Their synergistic combination maximizes impact, reducing tumor accuracy to 8.46%, a 44.5% improvement over individual components. These findings quantitatively validate the complementary roles of attention mechanisms and attack strategies in exploiting MHSI vulnerabilities.

A.1.3 OVERALL EVALUATION

Combining spatial/spectral attention and local - pixel/Multiscale attack strategies yields the most potent adversarial attack. This setup hits the lowest tumor classification accuracy (8.46%) while strongly degrading accuracy across other classes, highlighting the need to integrate these components to fully exploit model vulnerabilities.

Our ablation study shows each framework component boosts effectiveness, with maximal impact when used together. These insights stress the superiority of our integrated approach in exposing MHSI classifier vulnerabilities, underscoring the need for robust, tailored defenses.