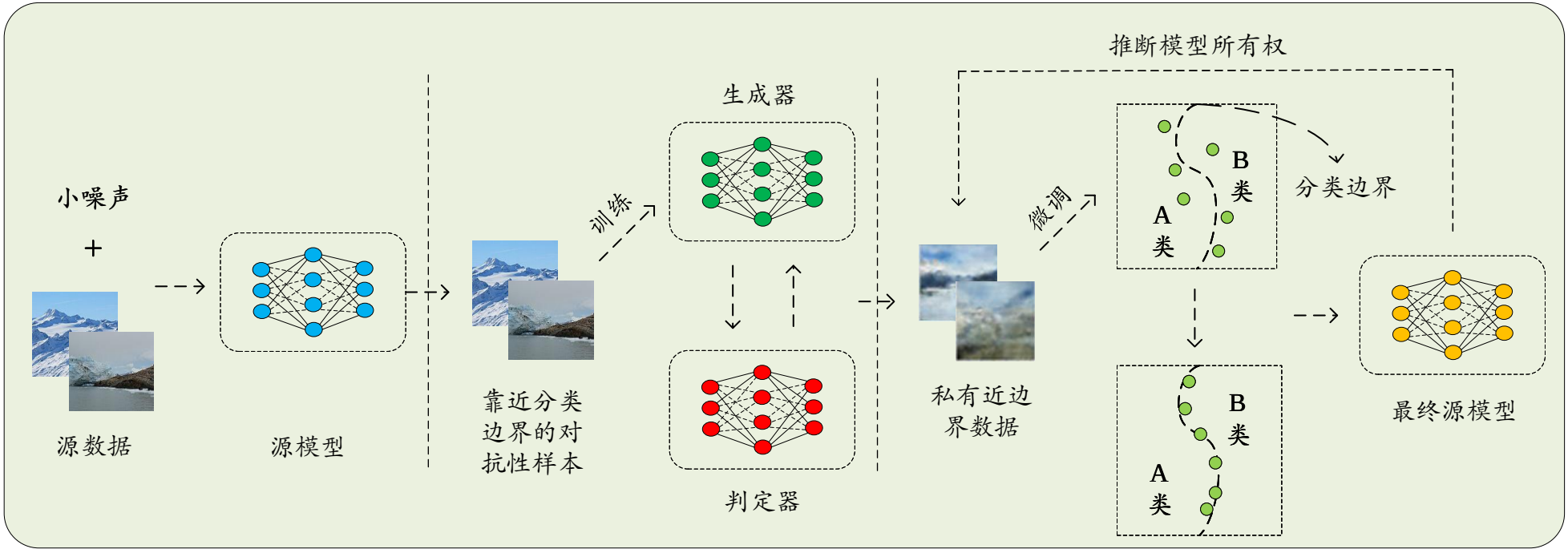
推断模型所有权
小噪声
+
源数据
源模型
训练
靠近分类
边界的对
抗性样本
生成器
判定器
微调
私有近边
界数据
B
类
A
类
分类边界
B
类
A
类
最终源模型