[BIOINFO 2025]

privateST: A Privacy-Preserving Framework for Spatial Transcriptomics Prediction from Histopathology Images Using Homomorphic Encryption

Hakin Kim[1,†], Buhm Han [1,2,3,*]

[1] *Interdisciplinary Program for Bioengineering, Seoul National University, Seoul, Republic of Korea*
[2] *Convergence Research Center for Dementia, Seoul National University Medical Research Center, Seoul, Republic of Korea*
[3] *Department of Biomedical Sciences, BK21 Plus Biomedical Science Project, Seoul National University College of Medicine, Seoul, Republic of Korea*
**Corresponding author: buhm.han@snu.ac.kr*

With the increasing availability of spatial transcriptomics (ST) data, numerous clinical studies now integrate both ST data and histopathology images. Recently, several deep learning models have been developed to predict ST data directly from histopathology images, offering insights into spatial gene expression without costly experimental procedures. However, privacy concerns restrict the use of patient data outside clinical institutions. To address this, we introduce privateST, the first privacy-preserving deep learning framework that predicts spatial transcriptomics data from encrypted histopathology images. By incorporating the CKKS homomorphic encryption scheme into a convolutional neural network (CNN) architecture, privateST performs inference directly on encrypted data, ensuring comprehensive data confidentiality. This approach substantiates the feasibility of secure spatial transcriptomics prediction, facilitating privacy-conscious collaborative research in precision medicine.