Algorithm 1 A Stealth and Defensive Backdoor based on Steganographic Algorithm in Federated Learning

Input: client set C, selected client set C_m, adversary set C_{adv}, global model G, local model L, central server C_s, aggregate algrithm $PartFedAvg$, benign datasets $\hat{D}$,poisoned datasets $\hat{D}_p$, learning rate η

Output: a global model with high accuracy, stealth and defensive backdoor and high accuracy in main-task

C_s select n clients by random into C_m
C_s build a global model G
C_s send G to each client in C_m
model update $\theta =$
for epoch **do**
    for number of client in C_m **do**
        if client $e_i \in C_{adv}$ **then**
            Download G as local model L and train L by private benign
            Compute gradient by $\hat{D}$
            Update $L_{i+1} = L - g$
            Upload $Li + 1$ to C_s
        else if client $e_i \notin C_{adv}$ **then**
            Download G as local model L and train L by private poisoned dataset
            Upload trained L to C_s
        C_s recieve update , aggregate by specific algrithm $PartFedAvg$ and generate update gradient U for G
        G updated by U
return Final global model G with backdoor