Algorithm 1 Stealthing and Robust Backdoor based on Steganographic Algorithm

Input: start epoch E_s, attack num E_a, end epoch E_e, client set C, selected client set C_m, adversary set C_{adv}, global model G, local model θ, central server C_s, aggregate algrithm $PartFedAvg$, benign datasets $\hat{D}$,poisoned datasets $\hat{D_p}$, benign learning rate η_b, poison learning rate η_p, PartFedAvg gradient removal scale $\mathscr{R}\%$

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
for epoch $<$ E_e and epoch $>$ $E_s + E_a$ **do**
    for number k of client in C_m **do**
        if client $e_i \in C_{adv}$ **then**
            Download G as local model L and train L by poisoned datasets $\hat{D_p}$,
            Compute gradient by $\hat{D_p}$ on batch B_i of size ℓ
            $g_i^p = \frac{1}{n}\sum_{i=1}^{n} \nabla_\theta \mathscr{L}(\theta_{e_i}, \hat{D_p})$
            for $Value(g_i^p[x,y])$ in g_i^p **do**
                if $Value(g_i^p[x,y]) \subseteq top_{5\%}(g_i^p)$ **then**
                    Set $g_i^p[x,y] = 0$
            Update $\theta_{e_{i+1}} = \theta_{e_i} - \eta_p g_i^p$ where $g_i^p \not\subseteq top_{5\%}(g)$
            Upload $\theta_{e_{i+1}}$ 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
            Compute gradient by $\hat{D_b}$ on batch B_i of size ℓ
            $g_i^b = \frac{1}{n}\sum_{i=1}^{n} \nabla_\theta \mathscr{L}(\theta_{e_i}, \hat{D})$
            Update $\theta_{e_{i+1}} = \theta_{e_i} - \eta_b g_i^b$
            Upload $\theta_{e_{i+1}}$ to C_s
        C_s recieve $\sum_1^k \theta_{e_{i+k}}$ and generate update gradient U for G
        for $Value(U[x,y])$ in U **do**
            Set $g_i^p[x,y] = 0$
    Randomly set $\mathscr{R}\%$ of gradient U to zero
    $G_{i+1} = G_i - U_i$
return Final global model G with backdoor