【19】中華民國　　【12】專利公報　（B）

【11】證書號數：I895098
【45】公告日： 中華民國 114 (2025) 年 08 月 21 日
【51】Int. Cl.：　*H04L9/08　(2006.01)*　*H04L9/28　(2006.01)*
發明　全 5 頁

【54】名　稱：資料處理裝置、資料安全傳輸系統與資料安全傳輸方法

【21】申請案號：113134284　【22】申請日： 中華民國 113 (2024) 年 09 月 10 日

【72】發 明 人： 王榮華 (TW) WANG, JUNG-HUA；陳振耀 (TW) ；賴易鍾 (TW)
【71】申 請 人： 國立臺灣海洋大學　NATIONAL TAIWAN OCEAN UNIVERSITY
基隆市中正區北寧路 2 號
【74】代 理 人： 劉箐茹

【56】參考文獻：
TW　I733106B　CN　118484832A
US　2024/0256850A1

審查人員：黃偉倫

【57】申請專利範圍

1. 一種資料處理裝置，用於根據一第一加密資料(ED)，產生一第一加密處理資料(FD)，以及提供用於對第一加密處理資料(FD)解密的一第一金鑰資料(K)，而不對該第一加密資料(ED)進行解密，且該資料處理裝置(11)包含：
一加密資料處理模組(111)，用於獲取經訓練後的一加密資料處理模型的複數個相關參數(P)，以使用經訓練後的該加密資料處理模型根據該第一加密資料(ED)產生該第一加密處理資料(FD)，以及提供該第一金鑰資料(K)，其中該第一加密處理資料(FD)關聯於該第一加密資料(ED)之一第一未加密資料經一特定處理後的一第一未加密處理資料，該加密資料處理模型為一類神經網路，以及該複數個相關參數(P)為經訓練後之該類神經網路的複數個權重參數；
其中該加密資料處理模型以複數個第二加密資料(ED')與對應於該複數個第二加密資料(ED')之複數個第二加密處理資料(FD')進行訓練，其中該第一加密資料(ED)與該第二加密資料(ED')使用一第一加密規格，以及該第一加密處理資料(FD)與該第二加密處理資料(FD')使用相同或不同於該第一加密規格的一第二加密規格。
2. 如請求項 1 所述之資料處理裝置，更包含：
一加密資料處理模型訓練模組(112)，信號連接該加密資料處理模組(111)，接收複數個第二加密資料(ED')及對應於該複數個第二加密資料(ED')之該複數個第二加密處理資料(FD')，並根據該複數個第二加密資料(ED')與該複數個第二加密處理資料(FD')訓練該加密資料處理模型。
3. 如請求項 1 所述之資料處理裝置，其中該加密資料處理模組(111)根據一識別資料產生關聯於該第一加密處理資料(FD)所使用之一加密金鑰所對應之該第一金鑰資料(K)。
4. 如請求項 3 所述之資料處理裝置，其中該加密金鑰為一加密私鑰，該第一金鑰資料(K)為對應該加密私鑰的一公鑰或該公鑰經過重排攪亂(permutated)的資料，且該識別資料為該加密資料處理模組(111)的一晶片流水序列號或該資料處理裝置(11)的一物理不可仿製函數(Physical Unclonable Function，PUF)資料。

5. 如請求項 2 所述之資料處理裝置，其中該加密資料處理模型訓練模組(112)更接收一特定資訊(I)，並根據該複數個第二加密資料(ED')、該複數個第二加密處理資料(FD')與該特定資訊(I)訓練該加密資料處理模型，以及該加密資料處理模組(111)更接收該特定資訊(I)，並使用經訓練後的該加密資料處理模型根據該第一加密資料(ED)與該特定資訊(I)產生該第一加密處理資料(FD)，以及提供該第一金鑰資料(K)。

6. 一種資料處理裝置，用於根據一第一加密資料(ED)，產生包括一第一加密處理資料(FD)與用於對該第一加密處理資料(FD)解密的一第一金鑰資料(K)之一第一加密組合資料(CD)，而不對該第一加密資料(ED)進行解密，且該資料處理裝置包含：
一加密資料處理模組(111)，用於獲取經訓練後的一加密資料處理模型的複數個相關參數(P)，以使用經訓練後的該加密資料處理模型根據該第一加密資料(ED)產生該第一加密組合資料(CD)，其中該第一加密處理資料(FD)關聯於該第一加密資料(ED)之一第一未加密資料經一特定處理後的一第一未加密處理資料，該加密資料處理模型為一類神經網路，以及該複數個相關參數(P)為經訓練後之該類神經網路的複數個權重參數；
其中該加密資料處理模型以複數個第二加密資料(ED')與複數個第二加密組合資料(CD')進行訓練，該複數個第二加密組合資料(CD')的每一者包括對應該第二加密資料(ED')的一第二加密處理資料(FD')以及該第二加密處理資料(FD')的一第二金鑰資料(K')，該第一加密資料(ED)與該第二加密資料(ED')使用一第一加密規格，以及該第一加密處理資料(FD)與該第二加密處理資料(FD')使用相同或不同於該第一加密規格的一第二加密規格。

7. 一種資料安全傳輸系統，包含：
一資料傳送端(2)；以及
一資料接收端(1)，通訊連接該資料傳送端(2)，包括一如請求項 1 至 5 其中一項所述之資料處理裝置(11)，其中該資料接收端(1)接收該資料傳送端(2)所傳送的該第一加密資料(ED)，並透過該資料處理裝置(11)根據該第一加密資料(ED)產生該第一加密處理資料(FD)。

8. 如請求項 7 所述的一種資料安全傳輸系統，其中該資料傳送端(2)用於獲取該第一未加密資料，該第一未加密資料包括複數個未加密感測資料。

9. 如請求項 8 所述的一種資料安全傳輸系統，其中該資料傳送端(2)更包括一加密裝置(21)，該加密裝置(21)用於將該第一未加密資料加密為該第一加密資料(ED)。

10. 如請求項 7 所述的一種資料安全傳輸系統，更包括：
一資料庫(3)，通訊連接該資料接收端(1)，用於儲存該複數個第二加密資料(ED')與對應於該複數個第二加密資料(ED')之該複數個第二加密處理資料(FD')。

11. 如請求項 7 所述的一種資料安全傳輸系統，其中該資料傳送端(2)為一人造衛星，以及該資料接收端(1)為一岸上資料中心。

12. 如請求項 9 所述之資料安全傳輸系統，其中該加密裝置(21)使用一對稱式加密方式與一非對稱式加密的其中之一或其組合對該第一未加密資料進行加密。

13. 一種資料安全傳輸方法，執行於一資料安全傳輸系統，包含：
透過該資料安全傳輸系統的一資料傳送端(2)，獲取一第一未加密資料，將該第一未加密資料加密為一第一加密資料(ED)，以及將該第一加密資料(ED)傳送給該資料安全傳輸系統的一資料接收端(1)；以及
透過該資料安全傳輸系統的該資料接收端(1)，獲取經訓練後的一加密資料處理模型的複數個相關參數(P)，並使用經訓練後的該加密資料處理模型根據該第一加密資料(ED)產生一第一加密處理資料(FD)，以及提供一第一金鑰資料(K)，其中該第一加密處理資料(FD)關聯於該第一加密資料(ED)之一第一未加密資料經一特定處理後的一第一未加密處理資

料，該加密資料處理模型為一類神經網路，該複數個相關參數(P)為經訓練後之該類神經網路的複數個權重參數；

其中該加密資料處理模型以複數個第二加密資料(ED')與對應於該複數個第二加密資料(ED')之複數個第二加密處理資料(FD')進行訓練，該第一加密資料(ED)與該第二加密資料(ED')使用一第一加密規格，以及該第一加密處理資料(FD)與該第二加密處理資料(FD')使用相同或不同於該第一加密規格的一第二加密規格。

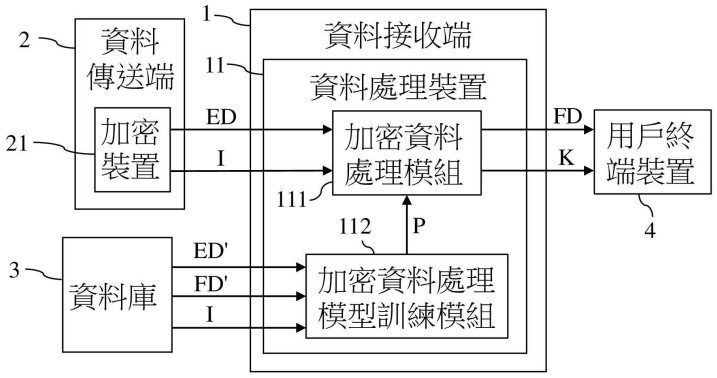
14. 如請求項 13 所述之資料安全傳輸方法，更包括：

透過該資料安全傳輸系統的該資料接收端(1)，接收該複數個第二加密資料(ED')及對應於該複數個第二加密資料(ED')之該複數個第二加密處理資料(FD')，並根據該複數個第二加密資料(ED')與該複數個第二加密處理資料(FD')訓練該加密資料處理模型。

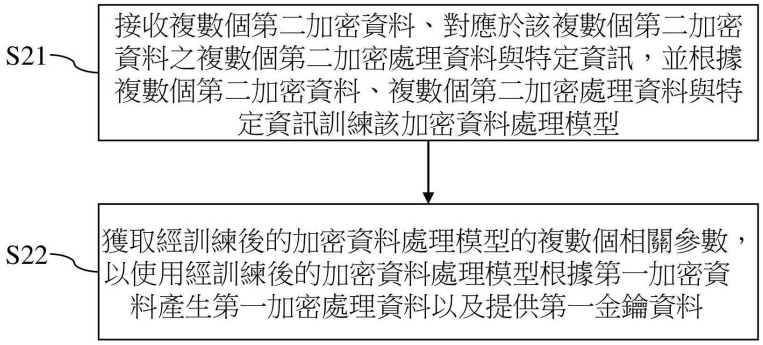
15. 如請求項 13 所述之資料安全傳輸方法，其中該特定處理為一預測處理、一量化處理、一模糊化處理及/或一摘要處理。

圖式簡單說明

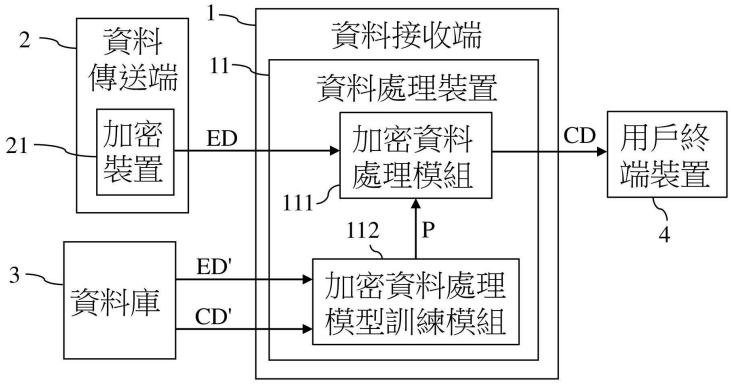
本發明之多個附圖僅是用於使本發明所屬技術領域的通常知識者易於了解本發明，其尺寸與配置關係僅為示意，且非用於限制本發明，其中各附圖簡要說明如下：圖 1 是本發明實施例的資料安全傳輸系統的系統方塊圖；圖 2 是本發明實施例的資料安全傳輸方法的流程圖；圖 3 是本發明另一實施例的資料安全傳輸系統的系統方塊圖；以及圖 4 是本發明實施例的資料安全傳輸系統的應用示意圖。



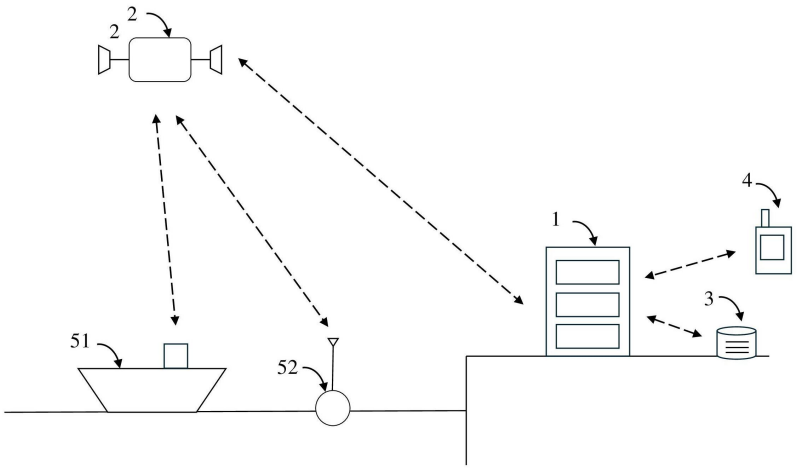

【圖1】


S21
接收複數個第二加密資料、對應於該複數個第二加密資料之複數個第二加密處理資料與特定資訊，並根據複數個第二加密資料、複數個第二加密處理資料與特定資訊訓練該加密資料處理模型
S22
獲取經訓練後的加密資料處理模型的複數個相關參數，以使用經訓練後的加密資料處理模型根據第一加密資料產生第一加密處理資料以及提供第一金鑰資料

【圖2】


1
資料接收端
2
資料傳送端
11
資料處理裝置
21
加密裝置
ED
加密資料處理模組
CD
用戶終端裝置
4
111
112
P
3
資料庫
ED'
CD'
加密資料處理模型訓練模組

【圖3】




【圖4】