I808905

(19)中華民國智慧財產局

(12)發明說明書公告本 **(11)證書號數：TW I808905 B**

(45)公告日： 中華民國 112 (2023) 年 07 月 11 日

(21)申請案號：111137746 (22)申請日： 中華民國 111 (2022) 年 10 月 04 日

(51)Int. Cl.： ***G06F21/72 (2013.01)*** ***H04L9/32 (2006.01)***

(71)申請人：財團法人資訊工業策進會 (中華民國) INSTITUTE FOR INFORMATION INDUSTRY (TW)

臺北市大安區和平東路二段 106 號 11 樓

(72)發明人：廖建維 LIAO, JIAN WEI (TW) ；李承恩 LEE, CHENG EN (TW) ；林霆宇 LIN, TING YU (TW)

(74)代理人：閻啓泰；林景郁

(56)參考文獻：

TW	201729576A	CN	111832025A
CN	112883385A	US	2010/0246808A1

審查人員：劉建宏

申請專利範圍項數：18 項 圖式數：18 共 40 頁

(54)名稱

加密訊號辨識裝置與方法

(57)摘要

本發明提供加密訊號辨識方法，藉由處理器執行以下步驟：接收旁通道訊號；過濾旁通道訊號的雜訊，以產生濾波後的旁通道訊號；利用濾波器轉換濾波後的旁通道訊號，以產生相量訊號；利用標準差窗口計算相量訊號的週期性以定位加密區段；從加密區段中擷取至少一加密特徵；以及利用特徵辨識模型識別至少一加密特徵，以產生加密訊號識別結果，其中加密訊號識別結果包含加密區段的位置以及旁通道訊號對應的加密訊號類型；本發明可自動且較有效率的定位加密區段，並且有效率的分析加密訊號類型。

The present invention provides an encryption determining method; the method is executed by a processor, and the method includes the following steps: receiving a trace; filtering noise from the trace and generating a filtered trace; converting the filtered trace by using a filter to generate a phasor signal; calculating a periodicity of the phasor signal by using a standard of deviation window for locating an encryption segment; extracting at least one encryption characteristic element from the encryption segment; and identifying the at least one encryption characteristic element by using a characteristic element determining model, and generating an encryption signal identification result, wherein the encryption signal identification result includes a location of the encryption segment and an encryption signal type corresponding to the trace. The present invention is able to automatically and efficiently locate the encryption segment, and to efficiently analyze the encryption signal type.

指定代表圖：

符號簡單說明：

S1~S6:步驟

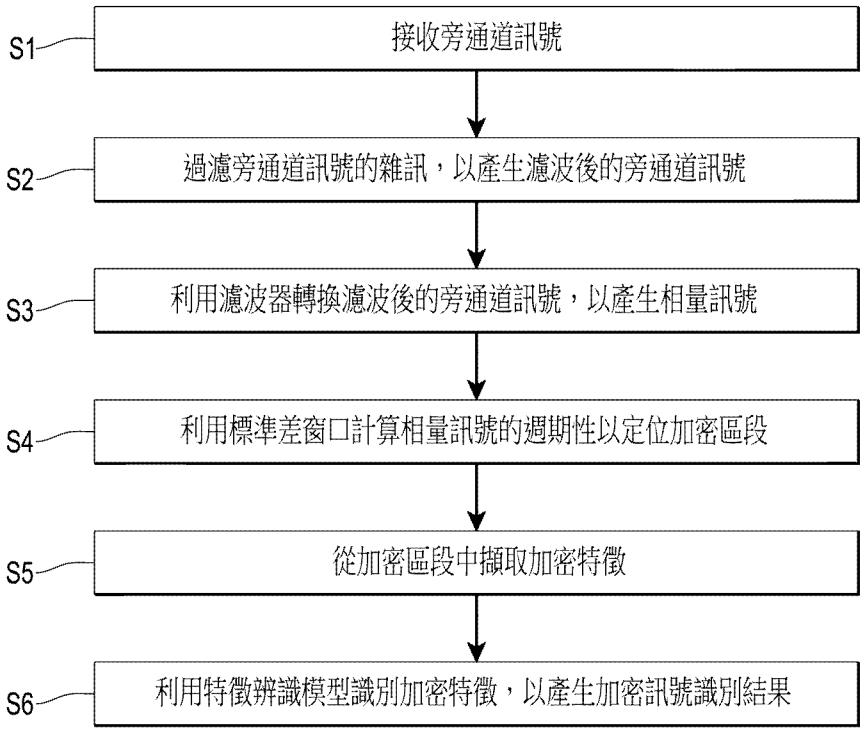

圖3

公告本

I808905

【發明摘要】

【中文發明名稱】加密訊號辨識裝置與方法

【英文發明名稱】Encryption Determining Device and Method thereof

【中文】

本發明提供加密訊號辨識方法，藉由處理器執行以下步驟：接收旁通道訊號；過濾旁通道訊號的雜訊，以產生濾波後的旁通道訊號；利用濾波器轉換濾波後的旁通道訊號，以產生相量訊號；利用標準差窗口計算相量訊號的週期性以定位加密區段；從加密區段中擷取至少一加密特徵；以及利用特徵辨識模型識別至少一加密特徵，以產生加密訊號識別結果，其中加密訊號識別結果包含加密區段的位置以及旁通道訊號對應的加密訊號類型；本發明可自動且較有效率的定位加密區段，並且有效率的分析加密訊號類型。

【英文】

The present invention provides an encryption determining method; the method is executed by a processor, and the method includes the following steps: receiving a trace; filtering noise from the trace and generating a filtered trace; converting the filtered trace by using a filter to generate a phasor signal; calculating a periodicity of the phasor signal by using a standard of deviation window for locating an encryption segment; extracting at least one encryption characteristic element from the encryption segment; and identifying the at least one encryption characteristic element by using a characteristic element determining model, and generating an encryption signal identification result, wherein the encryption signal identification result includes a location of the encryption segment and an encryption signal type corresponding to the trace. The present invention is able to automatically and efficiently locate the encryption segment, and to efficiently analyze the encryption signal type.

【指定代表圖】圖3

【代表圖之符號簡單說明】

S1~S6:步驟

【發明說明書】

【中文發明名稱】加密訊號辨識裝置與方法

【英文發明名稱】Encryption Determining Device and Method thereof

【技術領域】

【0001】 一種加密訊號辨識裝置與方法，尤指一種基於旁通道資訊之加密訊號辨識裝置與方法。

【先前技術】

【0002】 隨著安全意識的提高，越來越多的硬體電路在設計上具有加密運算的能力，而當這些硬體電路使用現今的加密演算法做保護時，目前已難以從正面破解此軟硬體結合的加密防護。

【0003】 在此趨勢之下，近年來針對已封裝晶片(post-silicon)，旁通道攻擊(Side Channel Attack；SCA)成為了國際上受到關注的知名攻擊手法。SCA係藉由蒐集硬體裝置進行密碼運算時不經意洩漏之物理訊號，以統計、訊號處理等技術分析而得到相關的秘密訊息，例如加解密所使用之金鑰或是加密前之明文。這些密碼運算時不經意洩漏之物理訊號，例如電磁波強度、電流、功耗、運算聲音變化、運算儀器的信號燈所發出之光訊號變化等，皆可透過不同類型的SCA採集儀器擷取獲得，由SCA採集儀器擷取到的訊號即稱為旁通道資訊(Trace)。

【0004】 目前來說，旁通道資訊的採集和量測儀器已於國外發展多時，因此旁通道資訊的採集作業較無困難。困難點在於旁通道資訊的解析，例如從旁通道資訊中破解出加密金鑰的現行作法，主要是藉由統計分析法對旁通道資訊進行分析，進而得到所使用的加密金鑰，但過程中需要龐大的運算時間。由於旁通道資訊中可能充滿了大量的訊號雜訊或是其它運算過程產生的訊號，因此需要有經驗的專業人員協助人力辨識旁通道資訊，以從旁通道資訊當中找出資訊的加密區段。

【發明內容】

【0005】 本發明提供一種加密訊號辨識裝置與方法，能夠偵測旁通道訊號，並且有效率的定位旁通道訊號中加密區段之位置，和分析加密區段之加密種類。

【0006】 加密訊號辨識裝置包括旁通道感測器、儲存器和處理器。處理器電性連接至旁通道感測器與儲存器。旁通道感測器用以偵測旁通道訊號，儲存器用以儲存特徵辨識模型，而處理器用以執行以下步驟：從旁通道感測器接收旁通道訊號；過濾旁通道訊號的雜訊，以產生濾波後的旁通道訊號；利用濾波器轉換濾波後的旁通道訊號，以產生相量訊號；利用標準差窗口計算相量訊號的週期性以定位加密區段；從加密區段中擷取至少一加密特徵；以及利用特徵辨識模型識別至少一加密特徵，以產生加密訊號識別結果，其中加密訊號識別結果包含加密區段的位置以及旁通道訊號對應的加密訊號類型。

【0007】 本發明之加密訊號辨識方法係由處理器執行，且包括以下步驟：接收旁通道訊號；過濾旁通道訊號的雜訊，以產生濾波後的旁通道訊號；利用濾波器轉換濾波後的旁通道訊號，以產生相量訊號；利用標準差窗口計算相量訊號的週期性以定位加密區段；從加密區段中擷取至少一加密特徵；以及利用一特徵辨識模型識別至少一加密特徵，以產生加密訊號識別結果，其中加密訊號識別結果包含加密區段的位置以及旁通道訊號對應的加密訊號類型。

【0008】 當旁通道感測器自電路接收旁通道訊號後，旁通道感測器即將接收之旁通道訊號傳送給處理器，由處理器執行加密訊號辨識方法。藉由處理器過濾旁通道訊號的雜訊，轉換濾波後的旁通道訊號而產生相量訊號，並利用標準差窗口計算相量訊號的週期性以定位加密區段。相較於先前技術，本發明無需人為協助定位加密區段，而可自動化的根據接收到的旁通道訊號產生定位加密區段之結果。進一步，本發明能針對受到定位之加密區段擷取至少一加密特徵，以利

通過儲存器內存有的特徵辨識模型識別至少一加密特徵以產生加密訊號識別結果，如此解析旁通道訊號所對應的加密訊號類型。

【0009】 整體而言，本發明除了無需人為協助運作外，也因可以較有效率的定位加密區段，一併減少了整體分析加密訊號類型所需的時間，藉此提高識別加密訊號類型的效率。

【圖式簡單說明】

【0010】 圖1為本發明加密訊號辨識裝置的系統方塊圖。

【0011】 圖2為本發明加密訊號辨識裝置的系統示意圖。

【0012】 圖3為本發明加密訊號辨識方法的流程圖。

【0013】 圖4A為本發明旁通道訊號的訊號圖。

【0014】 圖4B為本發明濾波後的旁通道訊號的訊號圖。

【0015】 圖5為本發明相量訊號的訊號圖。

【0016】 圖6為本發明加密訊號辨識方法的另一流程圖。

【0017】 圖7為本發明標準差線的示意圖。

【0018】 圖8為本發明標準差線之差值的示意圖。

【0019】 圖9為本發明加密訊號辨識方法的另一流程圖。

【0020】 圖10為本發明劃分待定區段的示意圖。

【0021】 圖11為本發明於第一待定區段投影形成特徵區段的示意圖。

【0022】 圖12為本發明於第二待定區段投影形成特徵區段的示意圖。

【0023】 圖13為本發明加密訊號辨識方法的另一流程圖。

【0024】 圖14為本發明加密訊號辨識方法的另一流程圖。

【0025】 圖15為本發明於加密區段偵測輪數的示意圖。

【0026】 圖16為本發明於另一加密區段偵測輪數的示意圖。

【0027】 圖17為本發明對應加密區段之濾波後的旁通道訊號的訊號圖。

【0028】 圖18為本發明另一對應加密區段之濾波後的旁通道訊號的訊號圖。

【實施方式】

【0029】 本發明提供加密訊號辨識裝置與加密訊號辨識方法。

【0030】 請參閱圖1所示，本發明之加密訊號辨識裝置包括旁通道感測器10、儲存器20、處理器30，且加密訊號辨識裝置係用於感測並辨識電路100的旁通道資訊。處理器30分別電性連接旁通道感測器10和儲存器20。電路100係受到電子裝置200之控制而運作，例如對訊號進行加密。

【0031】 請一併參閱圖2所示，舉例來說，儲存器20和處理器30可為電子裝置200中之記憶體和處理器或是獨立於電子裝置200外之設備。而電子裝置200還包括螢幕201、鍵盤202和滑鼠203。本發明的使用者可透過電子裝置200的螢幕201、鍵盤202和滑鼠203操作電子裝置200。電路100包括通訊埠101，且通訊埠101係電性連接電子裝置200中的處理器30以作為電路100和處理器30間的通訊埠口。在此例子中，處理器30發送具有明文的原始訊號Sor至電路100的通訊埠101，而電路100透過通訊埠101從處理器30接收原始訊號Sor後，即對原始訊號Sor之明文執行加密運算。

【0032】 旁通道感測器10包括和電子裝置200電性連接的示波器11和偵測器12，且偵測器12電性連接示波器11。旁通道感測器10的偵測器12係用以偵測電路100在執行加密運算時產生的旁通道訊號(Trace)，其中偵測器12自電路100蒐集旁通道訊號，且偵測器12將旁通道訊號送至示波器11。示波器11可顯示旁通道訊號的波形，以利使用者透過操作示波器11追蹤旁通道訊號的波形變化，確保旁通道感測器10所蒐集之旁通道訊號波形明確清楚。

【0033】 在本實施例中，偵測器12為電壓導線，且此電壓導線用以電性連接電路100的旁通道訊號產生點，以利蒐集電路100執行加密運算時產生的電壓

訊號，作為旁通道訊號。例如，旁通道訊號產生點可為電路100的通訊埠101，亦或是其他能夠收集到旁通道訊號的節點。在其他實施例中，偵測器12為電流導線，且此電流導線用以蒐集電路100執行加密運算時之電流訊號；或是偵測器12為紅外線溫度感測器，以紅外線近距測量電路100執行加密運算時的溫度訊號；亦或是偵測器12為電磁波感測器，以近距測量電路100執行加密運算時逸散出的電磁波訊號等。換句話說，本發明並不限制蒐集旁通道訊號之物理訊號種類，例如旁通道訊號可為電壓訊號、電流訊號、溫度訊號或電磁波訊號等。

【0034】 另外，儲存器20存有特徵辨識模型、工作頻率、預設設定檔和權重數據。特徵辨識模型為受過訓練之人工智能模型。當本發明之處理器30希望進一步再訓練特徵辨識模型時，處理器30即使用本發明產生之結果和權重數據訓練特徵辨識模型。權重數據為使用者透過電子裝置200所輸入對本發明產生結果之評分，換言之，權重數據用於訓練特徵辨識模型更正確的產生分析結果。工作頻率為電路100正常運作時的頻率，而預設設定檔包含了本發明執行計算和分析時所使用之參數。

【0035】 請參閱圖3所示，本發明之旁通道感測器10自電路100偵蒐旁通道訊號後，即將旁通道訊號傳送至處理器30。本發明之處理器30執行下述之步驟S1~S6。步驟S1：從旁通道感測器10接收旁通道訊號。步驟S2：過濾旁通道訊號的雜訊，以產生濾波後的旁通道訊號。步驟S3：利用濾波器轉換濾波後的旁通道訊號，以產生相量訊號。步驟S4：利用標準差窗口計算相量訊號的週期性以定位加密區段。步驟S5：從加密區段中擷取至少一加密特徵。步驟S6：利用特徵辨識模型識別至少一加密特徵，以產生加密訊號識別結果，其中加密訊號識別結果包含加密區段的位置以及旁通道訊號對應的加密訊號類型。以下將針對本發明之處理器30執行步驟S1至步驟S6之內容依序做出對應說明。

【0036】 在步驟S1中，處理器30接收從旁通道感測器10偵測到旁通道訊號，如前文所述，所蒐集之旁通道訊號的種類可為電壓訊號、電流訊號、溫度訊號或電磁波訊號等。

【0037】 在步驟S2中，處理器30過濾旁通道訊號的雜訊，以產生濾波後的旁通道訊號。具體而言，處理器30係頻譜過濾(spectral filtering)旁通道訊號大於或小於工作頻率之雜訊以產生濾波後的旁通道訊號。換言之，濾波後的旁通道訊號的頻率即為工作頻率。

【0038】 請參閱圖4A和4B所示，圖4A示意了濾波前之旁通道訊號的波形圖，而圖4B示意了濾波後的旁通道訊號的波形圖。圖4A和4B的縱軸(Y軸)單位為十倍的毫伏特(millivolt；mV)，而橫軸(X軸)單位為毫秒(millisecond；ms)。圖4A中濾波前之旁通道訊號具有較大的振幅，和例如55 ms至75 ms間具有較多不規律的訊號浮動，而圖4B中濾波後之濾波後的旁通道訊號具有較小的振幅，和例如55 ms至75 ms間較具有規律的訊號浮動。如此，濾波後的旁通道訊號之波形較明確，因此較適合本發明用以定位加密區段和分析加密訊號類型。

【0039】 請參閱圖5所示，在步驟S3中，處理器30利用數位濾波器轉換濾波後的旁通道訊號以產生相量訊號，而處理器30所產生之相量訊號如圖5所示，其縱軸為相量訊號的相量值(phasor)，橫軸為對應濾波後的旁通道訊號的測量時間的樣本數。舉例來說，圖4B中濾波後的旁通道訊號的測量時間為80 ms，圖5中的樣本數為320,000筆樣本，即處理器30在產生相量訊號時，將濾波後的旁通道訊號的每一毫秒對應取320,000/80=4,000筆的樣本做處理以呈現圖5所示之相量訊號。

【0040】 在本實施例中，數位濾波器係希爾伯特轉換濾波器(Hilbert transform filter)。即處理器30在利用希爾伯特轉換濾波器產生相量訊號時，係以希爾伯特轉換(Hilbert transform)將濾波後的旁通道訊號轉換為相量訊號。

【0041】 請參閱圖6至8所示，在步驟S4中，處理器30利用標準差窗口計算相量訊號的週期性以定位加密區段。具體來說，當處理器30執行步驟S4時，處理器30係執行步驟S4所包括的下述子步驟S41~S44。步驟S41：利用標準差窗口計算相量訊號的標準差(standard of deviation；σ)以產生標準差線L1，其中標準差窗口係擷取部份的相量訊號進行標準差計算。步驟S42：利用差值窗口擷取部份的標準差線L1。步驟S43：計算部份的標準差線L1對應的最大值與最小值，並計算最大值與最小值之間的差值。步驟S44：根據差值定位加密區段。

【0042】 在步驟S41中，處理器30利用標準差窗口計算相量訊號的標準差以產生標準差線L1，而圖7為處理器30執行步驟S41後所產生的標準差線L1之示意圖。標準差窗口的大小及其在橫軸移動之間距也可視需求而設定。在執行本發明前，可透過操作電子裝置200以設定預設設定檔之內容，調整關於標準差窗口的設定。當處理器30執行步驟S4時，處理器30根據儲存器20中的預設設定檔調整標準差窗口的大小和其於橫軸移動之間距，以利調整每次標準差窗口內所包含之樣本數量，調整根據標準差窗口內所包含樣本之相量訊號所計算的標準差，調整標準差線L1的產生。

【0043】 在步驟S42和步驟S43中，處理器30利用差值窗口擷取部份的標準差線L1，且處理器30計算部份的標準差線L1對應的最大值與最小值，並計算最大值與最小值之間的差值，而圖8為處理器30執行步驟S43後所產生標準差線L1最大值與最小值之間的差值之示意圖。差值窗口的大小和差值窗口於橫軸移動之間距也同樣可視需求而設定，定義於儲存器20中的預設設定檔中。

【0044】 請參閱圖8至10所示，在步驟S44中，處理器30根據差值定位加密區段。具體來說當處理器30執行步驟S44時，處理器30係進一步執行步驟S44所包括的下述子步驟S441~S447。步驟S441：根據差值的變化量將標準差線L1劃分為複數個待定區段。步驟S442：計算每一待定區段內所包含之標準差線L1的平

均值，並設定平均值為比較閾值。步驟S443：在每一待定區段中，將標準差線L1與比較閾值相比較，將大於比較閾值的標準差線L1標記為複數個子區段。步驟S444：將子區段對X軸垂直投影以形成複數個特徵區段。步驟S445：判斷特徵區段的長度是否近似。步驟S446：當判斷特徵區段的長度近似時，即判斷待定區段的其中之一為加密區段。步驟S447：當判斷特徵區段的長度未近似時，即判斷待定區段非加密區段。

【0045】 在步驟S441中，處理器30根據差值的變化量將標準差線L1劃分為多個待定區段，具體來說，處理器30係找出第一樣本S_1和最後樣本S_A之間差值最高的分隔樣本S_B。如圖10所示，分隔樣本S_B出現的位置即對應了標準差線L1中正確劃分待定區段的樣本位置。處理器30找出分隔樣本S_B後即根據分隔樣本S_B劃分待定區段，劃分分隔樣本S_B左側的標準差線L1部分為第一待定區段R1，並且劃分分隔樣本S_B右側的標準差線L1部分為第二待定區段R2。

【0046】 請參閱圖11和12所示，在步驟S442中，處理器30計算每一待定區段內所包含之標準差線L1的平均值，並設定平均值為比較閾值，具體來說，處理器30係分別計算第一待定區段R1內所包含之標準差線L1的第一平均值A_1，和計算第二待定區段R2內所包含之標準差線L1的第二平均值A_2。在步驟S443和S444中，處理器30在每一待定區段中，將標準差線L1與比較閾值相比較，將大於比較閾值的標準差線L1標記為多個子區段，並且判斷從子區段垂直投影形成的特徵區段的長度是否近似。具體來說，處理器30係分別於第一待定區段R1中將大於第一平均值A_1的標準差線L1部分標記為第一待定區段R1中的複數第一子區段，於第二待定區段R2中將大於第二平均值A_2的標準差線L1部分標記為第二待定區段R2中的複數第二子區段。並且，處理器30分別將第一待定區段R1中的第一子區段和第二待定區段R2中的第二子區段對X軸垂直投影以形成特徵區段Sg1~Sg9。

【0047】 詳細來說，在圖11所示的第一待定區段R1中，第一子區段對X軸垂直投影形成了共9個特徵區段Sg1~Sg9，而在圖12示的第二待定區段R2中，第二子區段對X軸垂直投影形成了共8個特徵區段Sg1~Sg8。X軸即標準差線L1分別被劃分於第一待定區段R1和第二待定區段R2的樣本數。換言之，第一待定區段R1中所對應的9個特徵區段Sg1~Sg9對應了9個區段的樣本數，而第二待定區段R2中所對應的8個特徵區段Sg1~Sg8對應了8個區段的樣本數。

【0048】 請參閱圖13所示，在步驟S445中，處理器30判斷特徵區段的長度是否近似。具體來說，處理器30執行步驟S445時，處理器30係進一步執行步驟S445所包括的下述子步驟S4451~S4453。步驟S4451：比較特徵區段之間的長度差異量是否小於或等於差異閾值。步驟S4452：當特徵區段之間的長度差異量小於或等於差異閾值時，即判斷特徵區段的長度近似，而進一步執行步驟S446。步驟S4453：當特徵區段之間的長度差異量大於差異閾值時，即判斷特徵區段的長度非近似，而進一步執行步驟S447。

【0049】 就圖11和12的例子而言，第一待定區段R1中所對應的9個特徵區段Sg1~Sg9彼此之間的長度差異量微小，即第一待定區段R1中所對應的9個特徵區段Sg1~Sg9對應了長度近似的樣本數量，如此，在意義上即第一待定區段R1中所對應的9個特徵區段Sg1~Sg9具有週期性，因此特徵區段Sg1~Sg9的至少其中之一者為加密區段。反觀，第二待定區段R2中所對應的8個特徵區段Sg1~Sg8彼此之間的長度差異量較大，即第二待定區段R2中所對應的8個特徵區段Sg1~Sg8對應了長度不近似的樣本數量，如此，在意義上即第二待定區段R2中所對應的8個特徵區段Sg1~Sg8非具有週期性，因此特徵區段Sg1~Sg8非加密區段。差異閾值的制定可視需求而設定，定義於儲存器20中的預設設定檔中。

【0050】 根據現有對旁通道訊號的認知，旁通道訊號中受到加密之區段應具有週期性，而濾波後的旁通道訊號、相量訊號、標準差線L1中受到加密之區段

都應保有週期性。當處理器30執行步驟S445後，處理器30所判斷之加密區段具有週期性，而處理器30所判斷非加密區段的區段因對應之長度不夠一致而不具有週期性。這裡所指的長度，如前述，雖指樣本數量的長度，但也意指旁通道訊號的測量時間長度，這兩者的對應關係已前述，為處理器30取樣本時取樣次數對上一毫秒單位時間之比例關係。詳細來說，旁通道訊號的測量時間長度和樣本數量的長度成正比關係，且關係如下：

樣本數量 = (測量時間長度) * (取樣本頻率)

【0051】 其中，取樣本頻率即為處理器30過濾旁通道訊號而產生濾波後的旁通道訊號時之取樣本頻率，例如每一毫秒對應取4,000筆旁通道訊號的樣本做處理而產生濾波後的旁通道訊號。

【0052】 請參閱圖14至16所示，在步驟S5中，處理器30從加密區段中擷取至少一加密特徵。具體來說，處理器30執行步驟S5時，處理器30係進一步執行步驟S5所包括的下述子步驟S51~S54。步驟S51：識別在加密區段中的標準差線L1的波峰數目或是波谷數目作為輪數。步驟S52：計算加密區段的時間長度。步驟S53：擷取對應加密區段的濾波後的旁通道訊號作為旁通道訊號加密區段。步驟S54：計算旁通道訊號加密區段的平均振幅。如此，從加密區段中擷取之至少一加密特徵包含輪數、時間長度和平均振幅。

【0053】 在步驟S6中，處理器30利用特徵辨識模型識別至少一加密特徵，以產生加密訊號識別結果。具體來說，當處理器30執行步驟S6時，處理器30係利用特徵辨識模型識別輪數、時間長度或平均振幅至少一者以產生加密訊號識別結果。這是因為，舉例來說，就目前現有的對稱密鑰演算法(Symmetric-key algorithm)而言，較知名的資料加密標準(Data Encryption Standard；DES)加密法和進階加密標準(Advanced Encryption Standard；AES)加密法在執行加密時分別對應了不同的運作週期數、不同的運作時間、和不同的運作能耗功率。不同加密

法之不同的運作週期數，對應了本案加密區段中的輪數數量。不同加密法之運作時間，對應了本案加密區段的樣本數量，也對應了本案加密區段所對應濾波後的旁通道訊號部分之時間長短。不同加密法之運作能耗功率，對應了本案加密區段所對應濾波後的旁通道訊號部分之振幅幅度變化。

【0054】 如圖15所示，在此例子中，處理器30計算第一週期G1的重複次數為9次，即處理器30偵測加密區段的波形大致重複之次數，代表加密區段的輪數為9輪。

【0055】 如圖16所示，在此例子中，處理器30同樣能大致訂定第二週期G2，並且計算第二週期G2的重複次數為16輪之輪數。並且，根據特徵辨識模型，處理器30判斷9輪之輪數為對應AES加密法，而16輪之輪數為對應DES加密法，因此處理器30判斷圖15例子中之加密區段為使用AES加密法，而圖16例子中之加密區段為使用DES加密法。

【0056】 請參閱圖17至18所示，定位加密區段後，本發明之處理器30也可根據特徵辨識模型識別時間長度或是平均振幅以產生加密訊號識別結果。具體來說，處理器30可根據加密區段所對應之標準差線L1得出對應之相量訊號，再根據對應之相量訊號得出對應之濾波後的旁通道訊號的部分。

【0057】 如圖17所示，在此例子中，已定位之加密區段所對應之濾波後的旁通道訊號的部分具有兩個特徵分別是一第一時間長度特徵T_1和一第一電壓振幅特徵V_{A1}。根據特徵辨識模型，處理器30判斷具有第一時間長度特徵T_1的加密區段為使用AES加密法。另外，第一電壓振幅特徵V_{A1}為此例子中濾波後的旁通道訊號之電壓波動的幅度，處理器30計算此例子中濾波後的旁通道訊號之電壓的絕對值的平均值為第一電壓振幅特徵V_{A1}，且認定第一電壓振幅特徵V_{A1}即為平均振幅。根據特徵辨識模型，處理器30判斷具有第一電壓振幅特徵V_{A1}的加密區段為使用AES加密法。

【0058】 在另一實施例中，已定位之加密區段所對應之濾波後的旁通道訊號的部分另具有第一功率特徵。處理器30計算圖17例子中濾波後的旁通道訊號之電壓的平方的平均值為第一功率特徵，且認定第一功率特徵即為平均振幅。並且，根據特徵辨識模型，處理器30判斷具有第一功率特徵的加密區段為使用AES加密法。換言之，在此實施例中平均振幅為對應AES加密法運作之能耗功率，而能耗功率和電壓之平方成正比，因此可以線性的判斷圖17例子中濾波後的旁通道訊號係使用何種加密法。

【0059】 如圖18所示，在此例子中，已定位之加密區段所對應之濾波後的旁通道訊號的部分具有兩個特徵分別是一第二時間長度特徵T_2和一第二電壓振幅特徵V_{A2}。根據特徵辨識模型，處理器30判斷具有第二時間長度特徵T_2的加密區段為使用DES加密法。另外，第二電壓振幅特徵V_{A2}為此例子中濾波後的旁通道訊號之電壓波動的幅度，處理器30計算此例子中濾波後的旁通道訊號之電壓的絕對值的平均值為第二電壓振幅特徵V_{A2}，且認定第二電壓振幅特徵V_{A2}即為平均振幅。根據特徵辨識模型，處理器30判斷具有第二電壓振幅特徵V_{A2}的加密區段為使用DES加密法。

【0060】 在另一實施例中，已定位之加密區段所對應之濾波後的旁通道訊號的部分另具有第二功率特徵。處理器30計算圖18例子中濾波後的旁通道訊號之電壓的平方的平均值為第二功率特徵，且認定第二功率特徵即為平均振幅。並且，根據特徵辨識模型，處理器30判斷具有第二功率特徵的加密區段為使用DES加密法。換言之，在此實施例中平均振幅為對應DES加密法運作之能耗功率，而能耗功率和電壓之平方成正比，因此可以線性的判斷圖18例子中濾波後的旁通道訊號係使用何種加密法。因為DES加密法所對應的能耗功率應大於AES加密法所對應的能耗功率，DES加密法所對應的電壓振幅應大於AES加密法所對應的電壓振幅，DES加密法所對應的加密時間長度應大於AES加密法所對應的加密時間

長度，本發明之處理器30也可一併使用上述之判斷，即根據特徵辨識模型綜合多種之判斷，認定圖17所示之濾波後的旁通道訊號為使用AES加密法，而圖18所示之濾波後的旁通道訊號為使用DES加密法。並且，濾波後的旁通道訊號所使用的加密法即為受到處理器30濾波前旁通道訊號所對應使用的加密訊號類型。

【0061】 本發明之處理器30還可進一步執行：利用至少一加密特徵以及至少一加密特徵對應的加密訊號識別結果作為訓練資料，以產生特徵辨識模型。具體來說，本發明利用至少一加密特徵以及至少一加密特徵對應的加密訊號識別結果配合儲存器20存有的權重數據以機器學習之方式訓練特徵辨識模型，以利特徵辨識模型在後續判斷時更精確地產生加密訊號識別結果。如此，加密區段的位置以及旁通道訊號所對應的加密訊號類型能更有效率的分別受到定位和分析。

【0062】 本發明無需如先前技術般，蒐集多個旁通道訊號，在時間軸上執行運算花費較大、能耗較大、且運算較費時的對齊步驟，以對齊多個旁通道訊號同步時間，以再分析對齊之多個旁通道訊號以產生分析加密法之結果。本發明僅需接收單筆旁通道訊號，即可針對單筆之旁通道訊號進行訊號處理以產生加密訊號識別結果。如此，本發明利用訓練後的特徵辨識模型可以自動定位加密區段的位置和分析加密訊號類型，藉此提高識別加密訊號類型的效率，降低分析加密訊號類型所需花費的時間及人力成本。

【符號說明】

【0063】

10:旁通道感測器

11:示波器

12:偵測器

20:儲存器

30:處理器

100:電路

101:通訊埠

200:電子裝置

201:螢幕

202:鍵盤

203:滑鼠

G1:第一週期

G2:第二週期

R1:第一待定區段

R2:第二待定區段

Sor:原始訊號

S_1:第一樣本

S_A:最後樣本

S_B:分隔樣本

Sg1~Sg9:特徵區段

S1~S6:步驟

S41~S44:步驟

S51~S54:步驟

S441~S447:步驟

S4451~S4453:步驟

T_1:第一時間長度特徵

T_2:第二時間長度特徵

V_{A1}:第一電壓振幅特徵

V_{A2}:第二電壓振幅特徵

【發明申請專利範圍】

【請求項 1】一種加密訊號辨識裝置，包括：

一旁通道感測器，用以偵測一旁通道訊號；

一儲存器，用以儲存一特徵辨識模型；以及

一處理器，電性連接至該旁通道感測器與該儲存器，該處理器用以執行下列步驟：

從該旁通道感測器接收該旁通道訊號；

過濾該旁通道訊號的雜訊，以產生一濾波後的旁通道訊號；

利用一濾波器轉換該濾波後的旁通道訊號，以產生一相量訊號；

利用一標準差窗口計算該相量訊號的週期性以定位一加密區段；

從該加密區段中擷取至少一加密特徵；以及

利用該特徵辨識模型識別該至少一加密特徵，以產生一加密訊號識別結果，其中該加密訊號識別結果包含該加密區段的位置以及該旁通道訊號對應的一加密訊號類型。

【請求項2】如請求項1所述之加密訊號辨識裝置，其中該處理器更用以執行以下運作：

利用該至少一加密特徵以及該至少一加密特徵對應的該加密訊號識別結果作為訓練資料，以產生該特徵辨識模型。

【請求項3】如請求項1所述之加密訊號辨識裝置，其中該處理器利用該標準差窗口計算該相量訊號的週期性以定位該加密區段時，該處理器更執行以下運作：

利用該標準差窗口計算該相量訊號的標準差以產生一標準差線，其中該標準差窗口係擷取部份的該相量訊號進行標準差計算；

利用一差值窗口擷取部份的該標準差線；

計算部份的該標準差線對應的一最大值與一最小值，並計算該最大值與該最小值之間的一差值；以及

根據該差值定位該加密區段。

【請求項4】如請求項3所述之加密訊號辨識裝置，其中當該處理器根據該差值定位該加密區段時，該處理器更執行以下運作：

根據該差值的變化量將該標準差線劃分為複數個待定區段；

在每一該些待定區段中，將該標準差線與一比較閾值相比較，將大於該比較閾值的該標準差線標記為複數個子區段；

將該些子區段對一X軸垂直投影以形成複數個特徵區段；

判斷該些特徵區段的長度是否近似，當該些特徵區段的長度近似時，即判斷該些待定區段的其中之一為該加密區段。

【請求項5】如請求項4所述之加密訊號辨識裝置，其中，該處理器係計算每一該些待定區段內所包含之該標準差線的一平均值，並設定各該平均值為每一該些待定區段內的該比較閾值。

【請求項6】如請求項4所述之加密訊號辨識裝置，其中，當該處理器判斷該些特徵區段的長度是否近似時，該處理器更執行以下運作：

比較該些特徵區段之間的長度差異量是否小於或等於一差異閾值；

當該些特徵區段之間的長度差異量小於或等於該差異閾值時，即判斷該些特徵區段的長度近似。

【請求項7】如請求項3所述之加密訊號辨識裝置，其中，當該處理器從該加密區段中擷取該至少一加密特徵時，該處理器更執行以下運作：

識別在該加密區段中的該標準差線的一波峰數目或是一波谷數目作為一輪數；其中，該至少一加密特徵包含該輪數。

【請求項8】如請求項1所述之加密訊號辨識裝置，其中，當該處理器從該加密區段中擷取該至少一加密特徵時，該處理器更執行以下運作：

計算該加密區段的一時間長度；其中，該至少一加密特徵包含該時間長度。

【請求項9】如請求項1所述之加密訊號辨識裝置，其中，當該處理器從該加密區段中擷取該至少一加密特徵時，該處理器更執行以下運作：

擷取對應該加密區段的該濾波後的旁通道訊號作為一旁通道訊號加密區段；以及

計算該旁通道訊號加密區段的一平均振幅；其中，該至少一加密特徵包含該平均振幅。

【請求項10】一種加密訊號辨識方法，由一處理器執行，且包括以下步驟：

接收一旁通道訊號；

過濾該旁通道訊號的雜訊，以產生一濾波後的旁通道訊號；

利用一濾波器轉換該濾波後的旁通道訊號，以產生一相量訊號；

利用一標準差窗口計算該相量訊號的週期性以定位一加密區段；

從該加密區段中擷取至少一加密特徵；以及

利用一特徵辨識模型識別該至少一加密特徵，以產生一加密訊號識別結果，其中該加密訊號識別結果包含該加密區段的位置以及該旁通道訊號對應的一加密訊號類型。

【請求項11】如請求項10所述之加密訊號辨識方法，進一步包括以下步驟：

利用該至少一加密特徵以及該至少一加密特徵對應的該加密訊號識別結果作為訓練資料，以再訓練該特徵辨識模型。

【請求項12】如請求項10所述之加密訊號辨識方法，其中利用該標準差窗口計算該相量訊號的週期性以定位該加密區段之步驟，進一步包括以下子步驟：

利用該標準差窗口計算該相量訊號的標準差以產生一標準差線，其中該標準差窗口係擷取部份的該相量訊號進行標準差計算；

利用一差值窗口擷取部份的該標準差線；

計算部份的該標準差線對應的一最大值與一最小值，並計算該最大值與該最小值之間的一差值；以及

根據該差值定位該加密區段。

【請求項13】如請求項12所述之加密訊號辨識方法，其中根據該差值定位該加密區段之步驟，係包括以下子步驟：

根據該差值的變化量將該標準差線劃分為複數個待定區段；

在每一該些待定區段中，將該標準差線與一比較閾值相比較，將大於該比較閾值的該標準差線標記為複數個子區段；

將該些子區段對一X軸垂直投影以形成複數個特徵區段；

判斷該些特徵區段的長度是否近似，當該些特徵區段的長度近似時，即判斷該些待定區段的其中之一為該加密區段。

【請求項14】如請求項13所述之加密訊號辨識方法，其中：

該比較閾值為每一該些待定區段內所包含之該標準差線的一平均值。

【請求項15】如請求項13所述之加密訊號辨識方法，其中判斷該些特徵區段的長度是否近似之步驟，係包括以下子步驟：

比較該些特徵區段之間的長度差異量是否小於或等於一差異閾值；

當該些特徵區段之間的長度差異量小於或等於該差異閾值時，即判斷該些特徵區段的長度近似。

【請求項16】如請求項12所述之加密訊號辨識方法，其中從該加密區段中擷取該至少一加密特徵之步驟，進一步包括以下子步驟：

識別在該加密區段中的該標準差線的一波峰數目或是一波谷數目作為一輪數；

其中，該至少一加密特徵包含該輪數。

【請求項17】如請求項10所述之加密訊號辨識方法，其中從該加密區段中擷取該至少一加密特徵之步驟，進一步包括以下子步驟：

計算該加密區段的一時間長度；

其中，該至少一加密特徵包含該時間長度。

【請求項18】如請求項10所述之加密訊號辨識方法，其中從該加密區段中擷取該至少一加密特徵之步驟，進一步包括以下子步驟：

擷取對應該加密區段的該濾波後的旁通道訊號作為一旁通道訊號加密區段；以及

計算該旁通道訊號加密區段的一平均振幅；

其中，該至少一加密特徵包含該平均振幅。

【發明圖式】

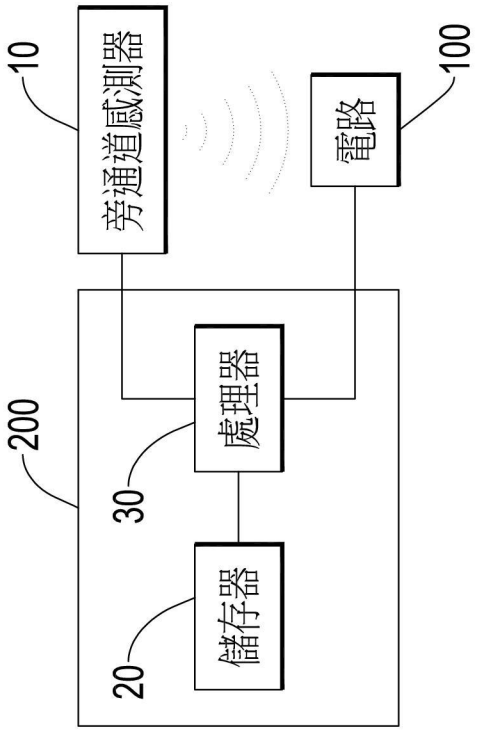

圖1

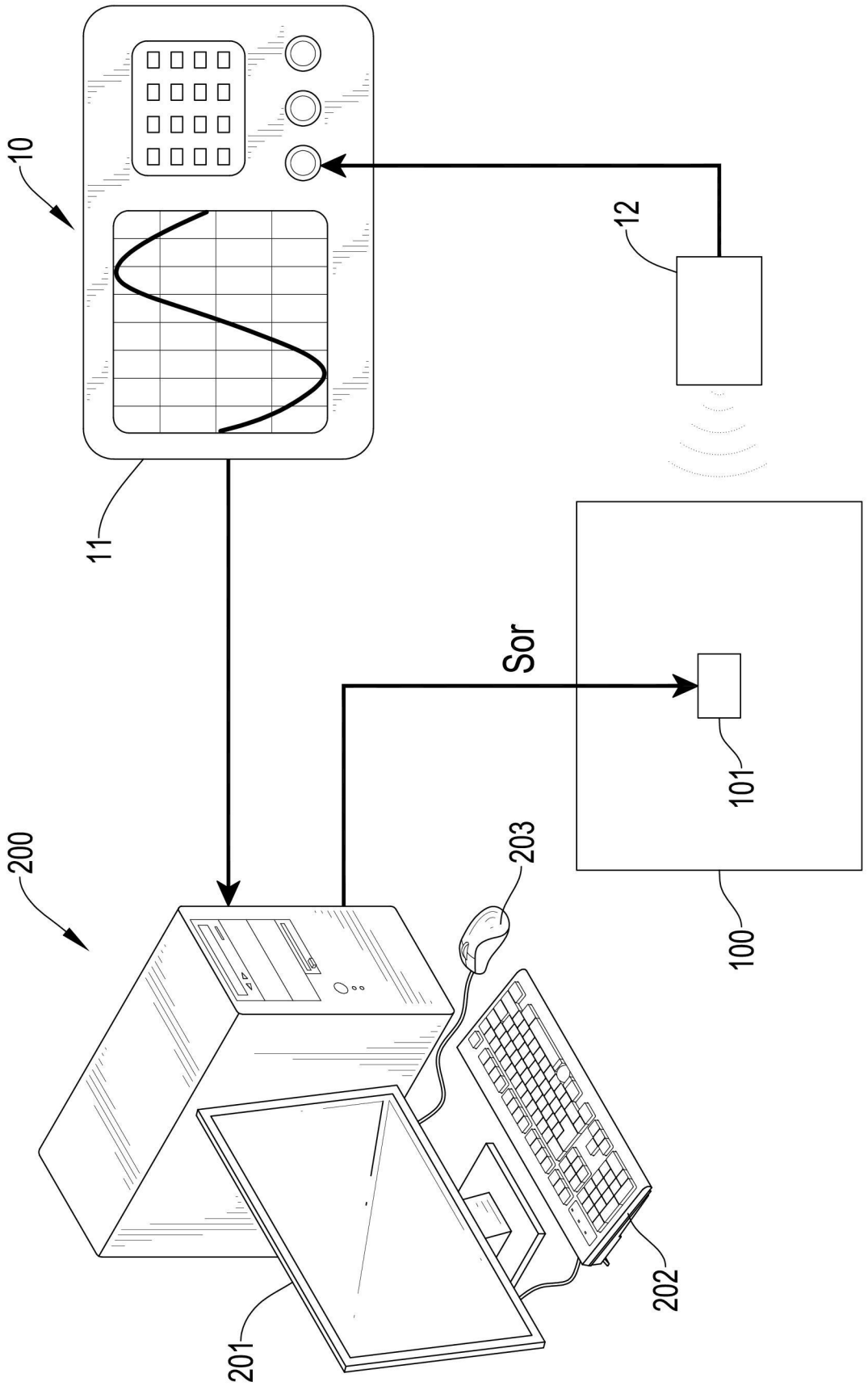

圖2

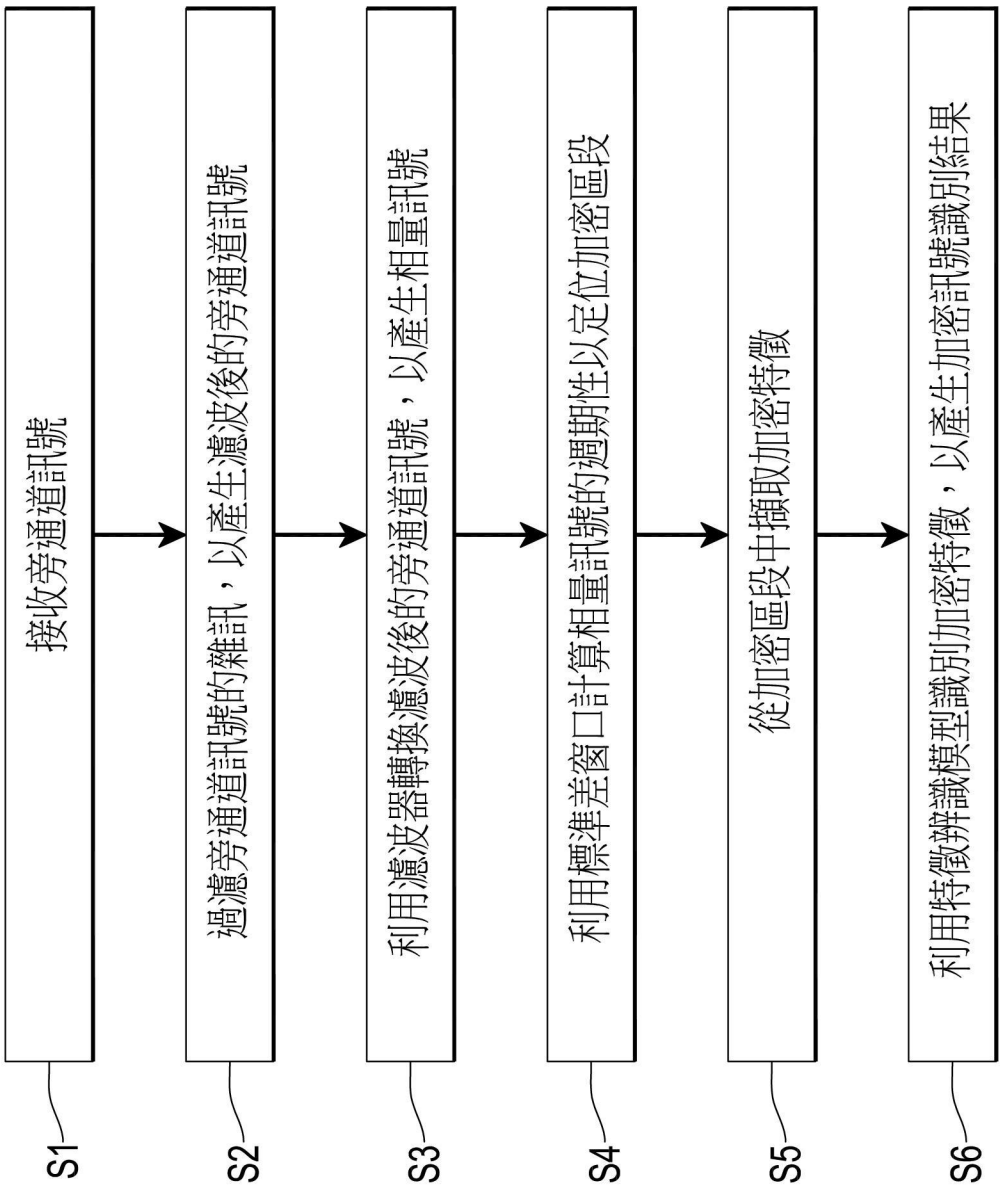
接收旁通道訊號
過濾旁通道訊號的雜訊，以產生濾波後的旁通道訊號
利用濾波器轉換濾波後的旁通道訊號，以產生相量訊號
利用標準差窗口計算相量訊號的週期性以定位加密區段
從加密區段中擷取加密特徵
利用特徵辨識模型識別加密特徵，以產生加密訊號識別結果
S1
S2
S3
S4
S5
S6

圖3

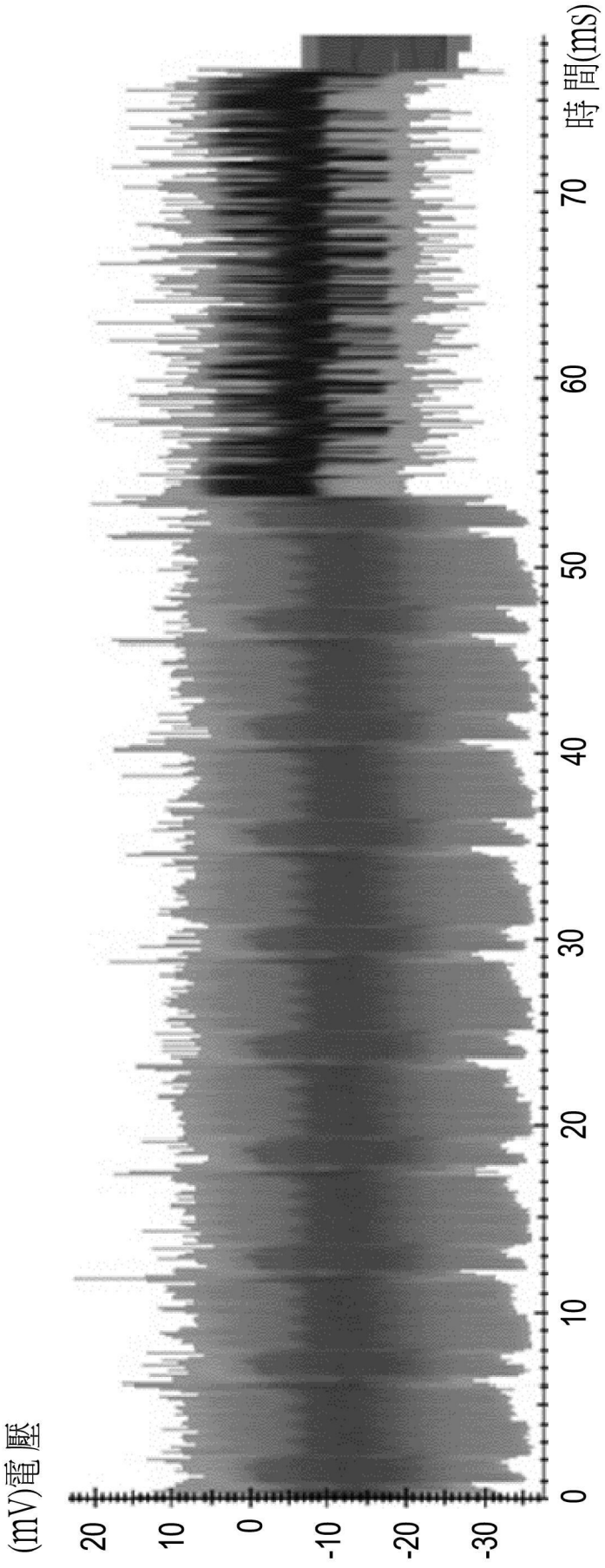

圖4A

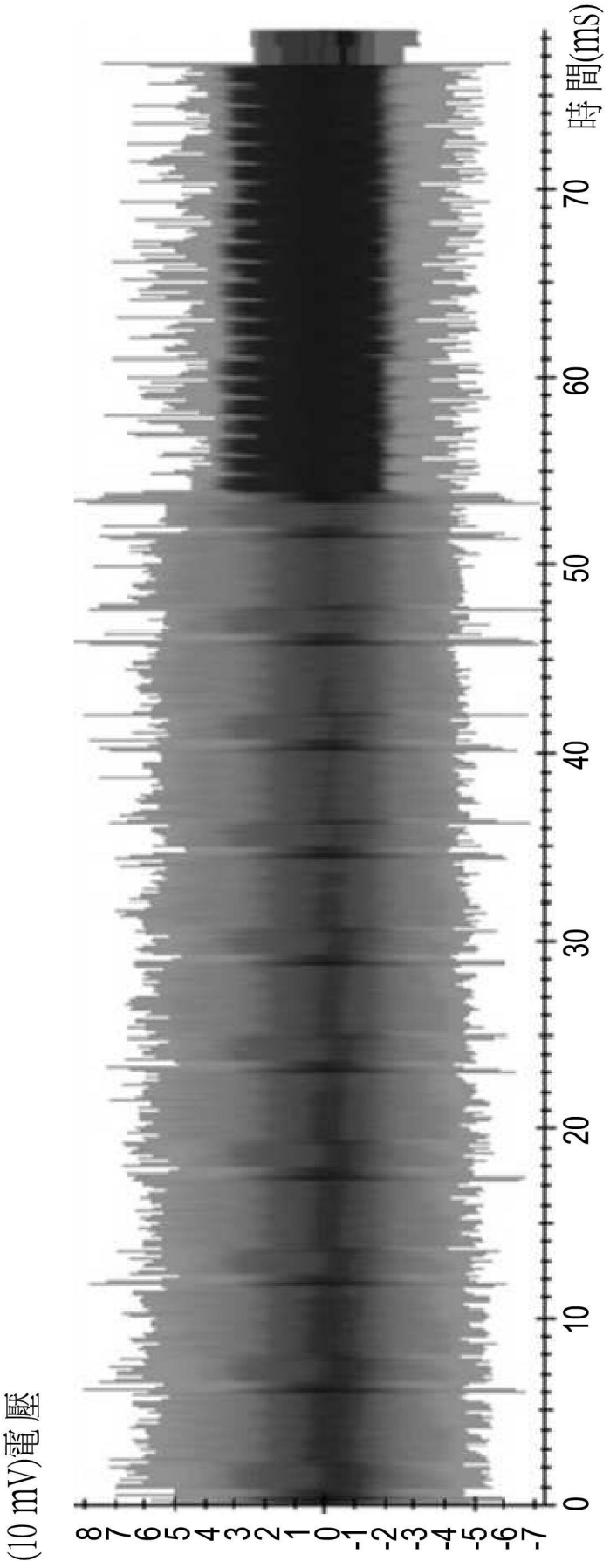

圖4B

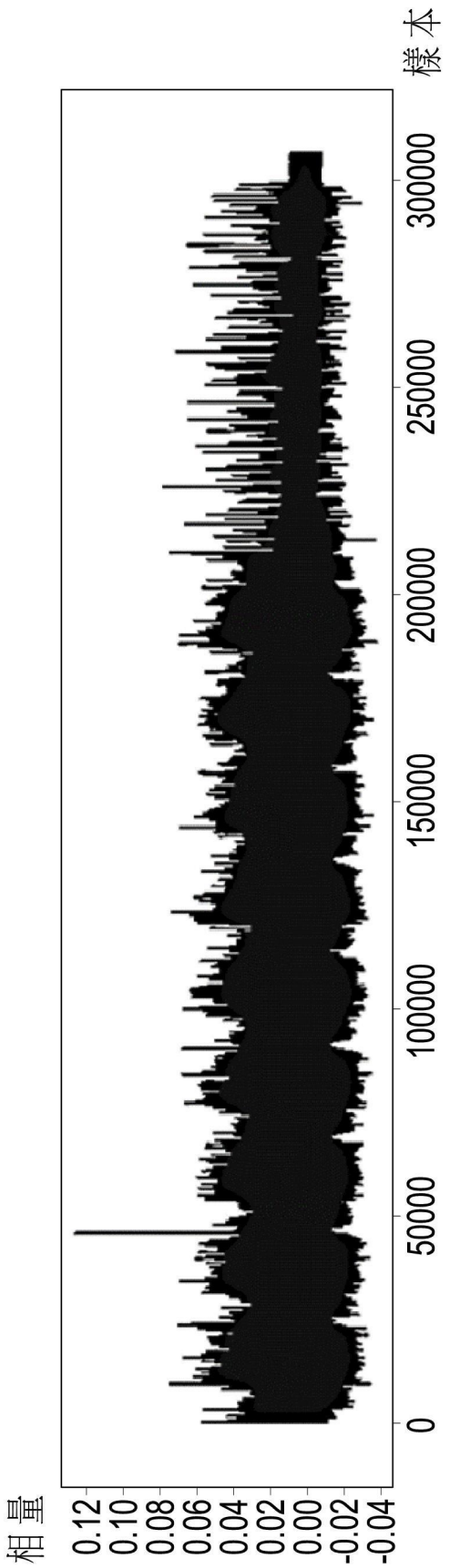
相量
0.12
0.10
0.08
0.06
0.04
0.02
0.00
-0.02
-0.04
0
50000
100000
150000
200000
250000
300000
樣本

圖5

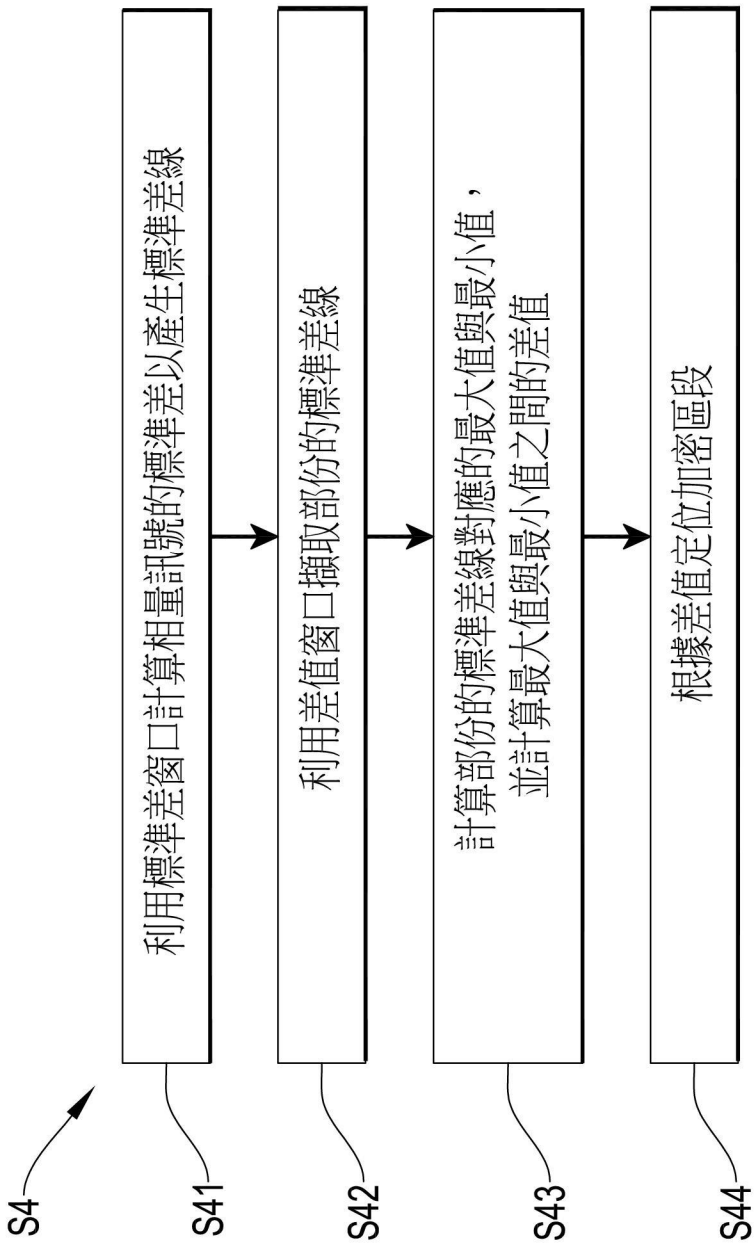
S4
S41
利用標準差窗口計算相量訊號的標準差以產生標準差線
S42
利用差值窗口擷取部份的標準差線
S43
計算部份的標準差線對應的最大值與最小值，
並計算最大值與最小值之間的差值
S44
根據差值定位加密區段

圖6

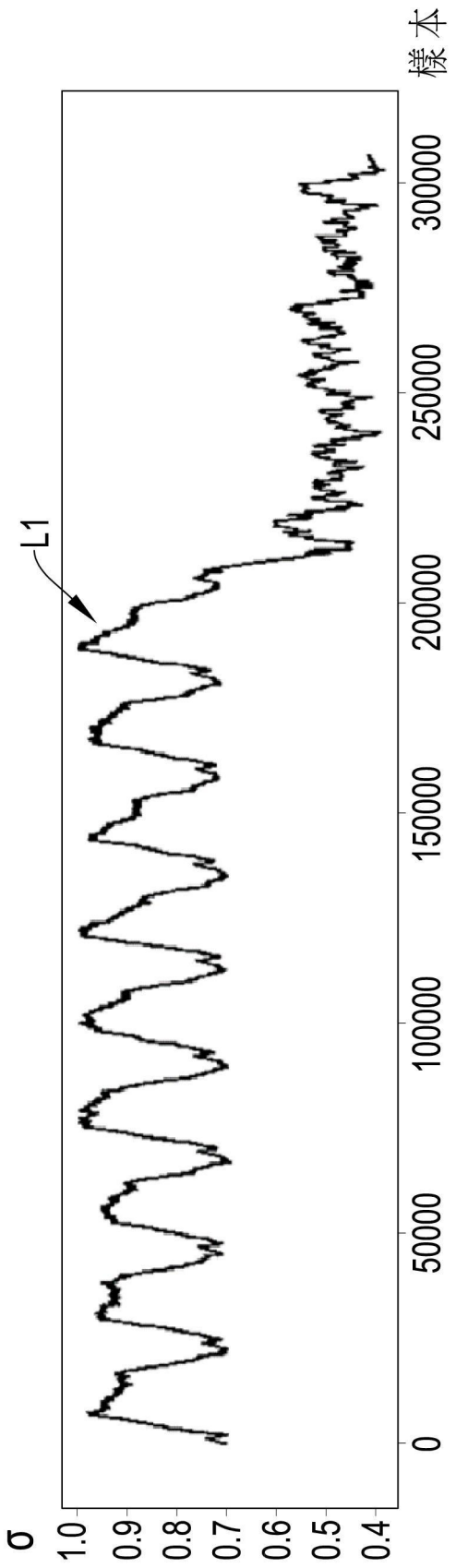
σ
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0
50000
100000
150000
200000
250000
300000
樣本
L1

圖7

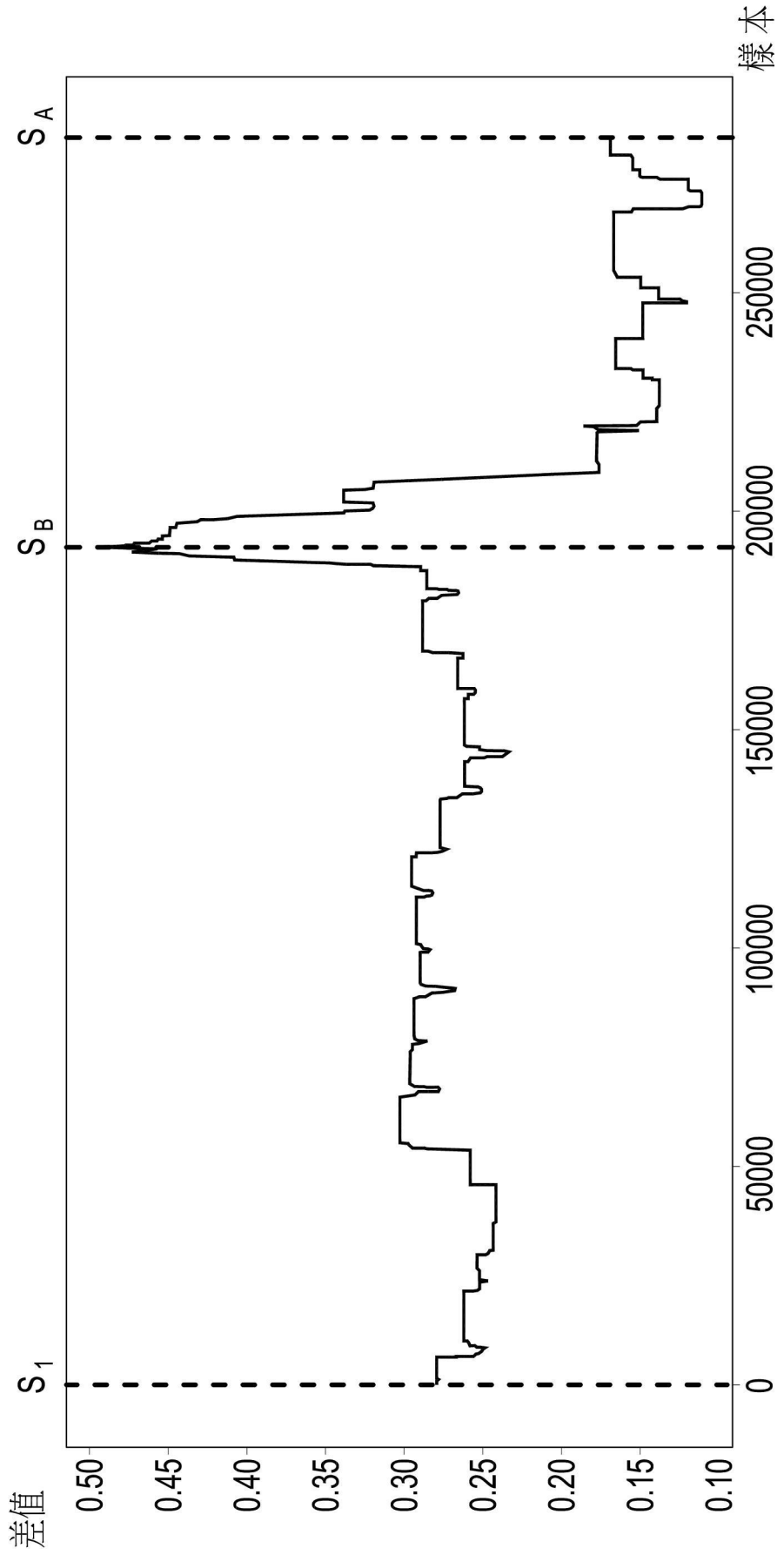
差值
0.50
0.45
0.40
0.35
0.30
0.25
0.20
0.15
0.10
S_1
S_B
S_A
0
50000
100000
150000
200000
250000
樣本

圖8

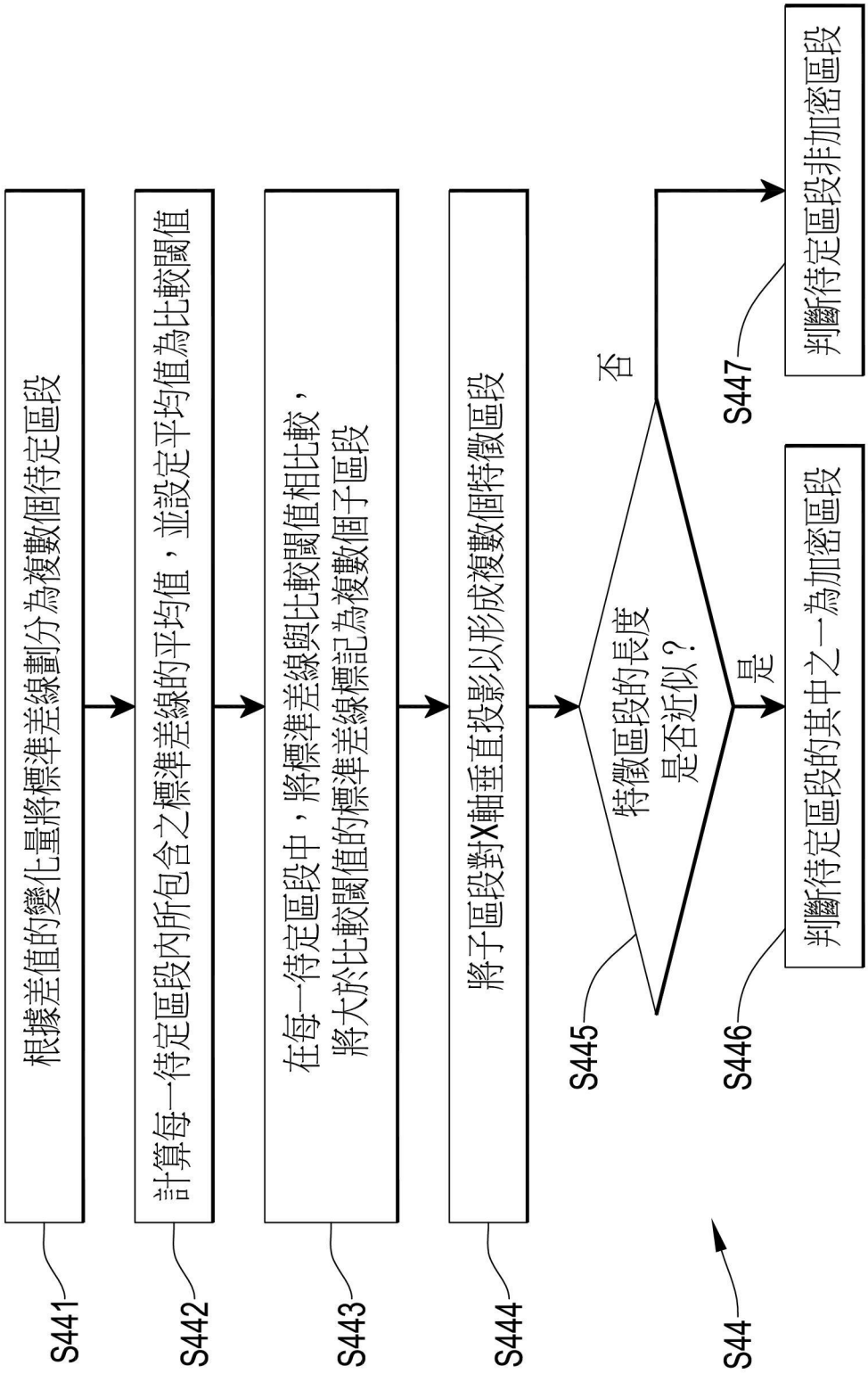
根據差值的變化量將標準差線劃分為複數個待定區段
S441
計算每一待定區段內所包含之標準差線的平均值，並設定平均值為比較閾值
S442
在每一待定區段中，將標準差線與比較閾值相比較，
將大於比較閾值的標準差線標記為複數個子區段
S443
將子區段對X軸垂直投影以形成複數個特徵區段
S444
特徵區段的長度
是否近似？
S445
否
是
S446
S447
判斷待定區段非加密區段
判斷待定區段的其中之一為加密區段
S44

圖9

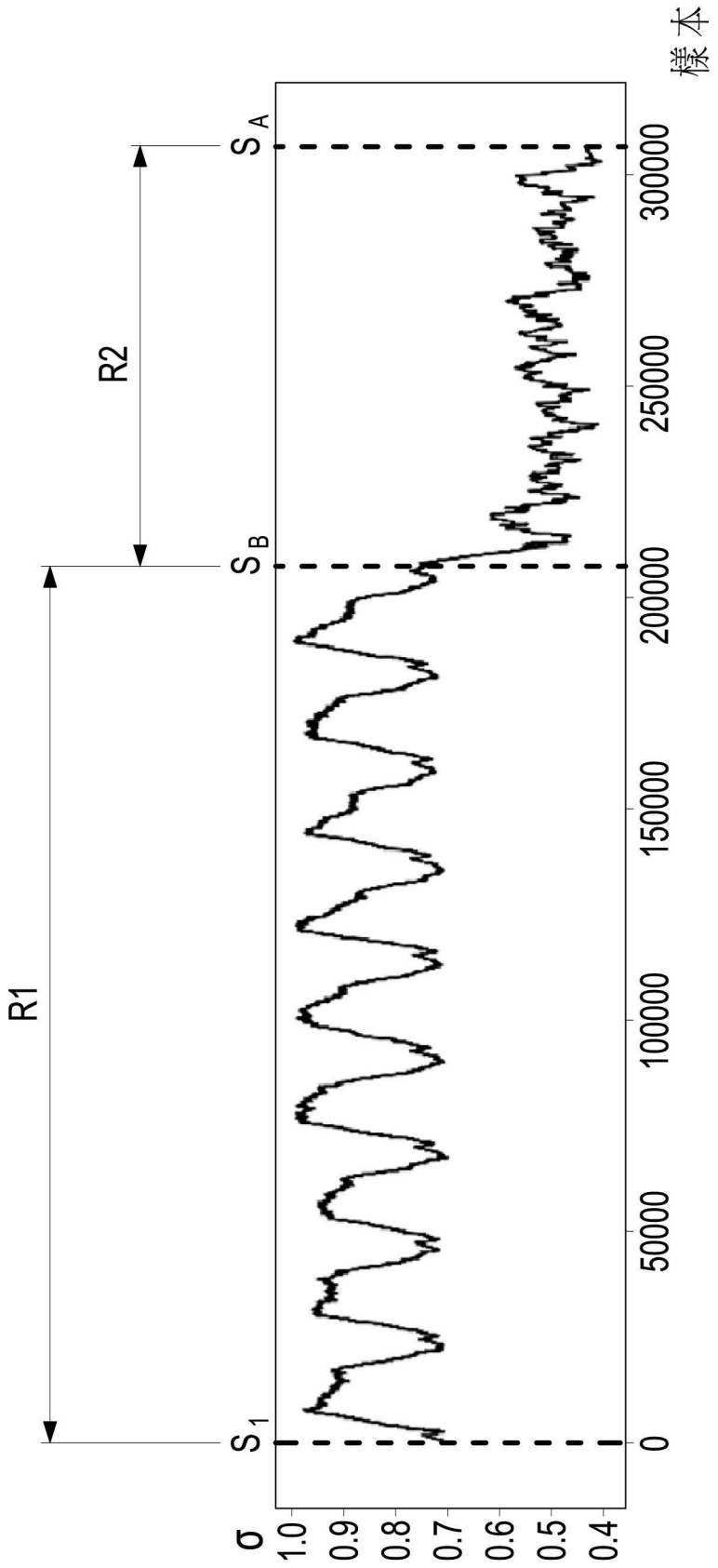
σ
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0
50000
100000
150000
200000
250000
300000
樣本
S1
SB
SA
R1
R2

圖10

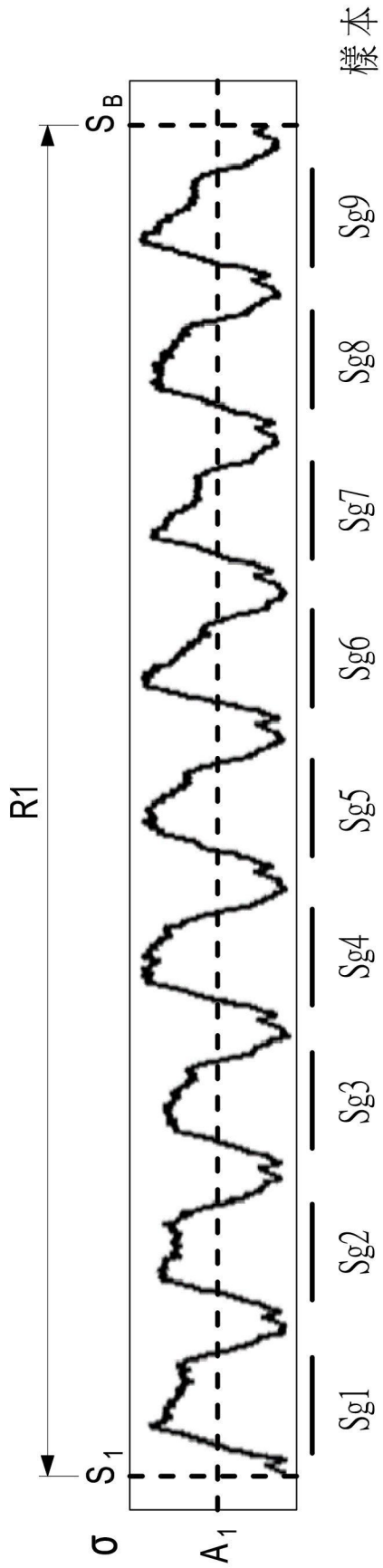

圖11

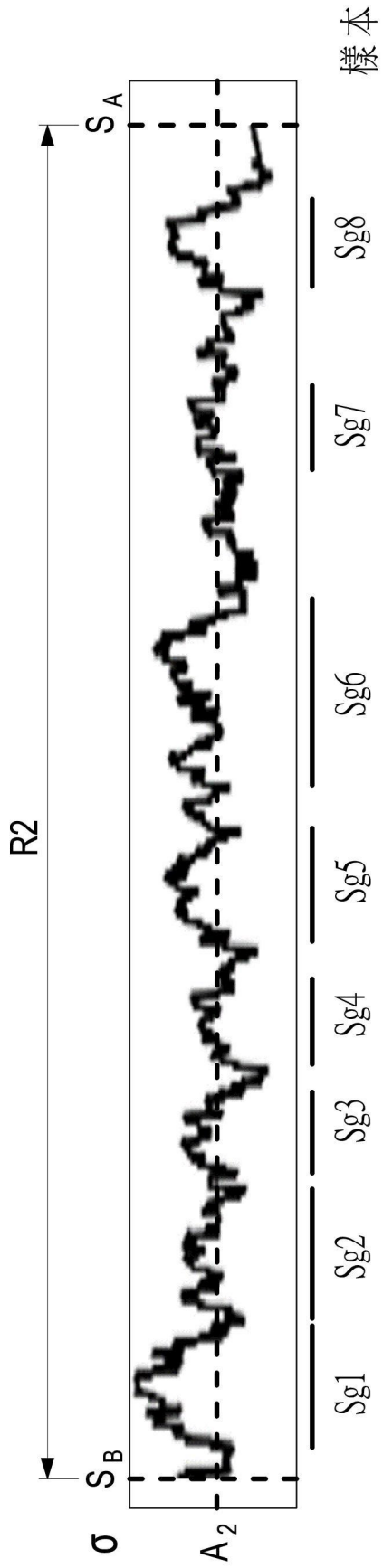

圖12

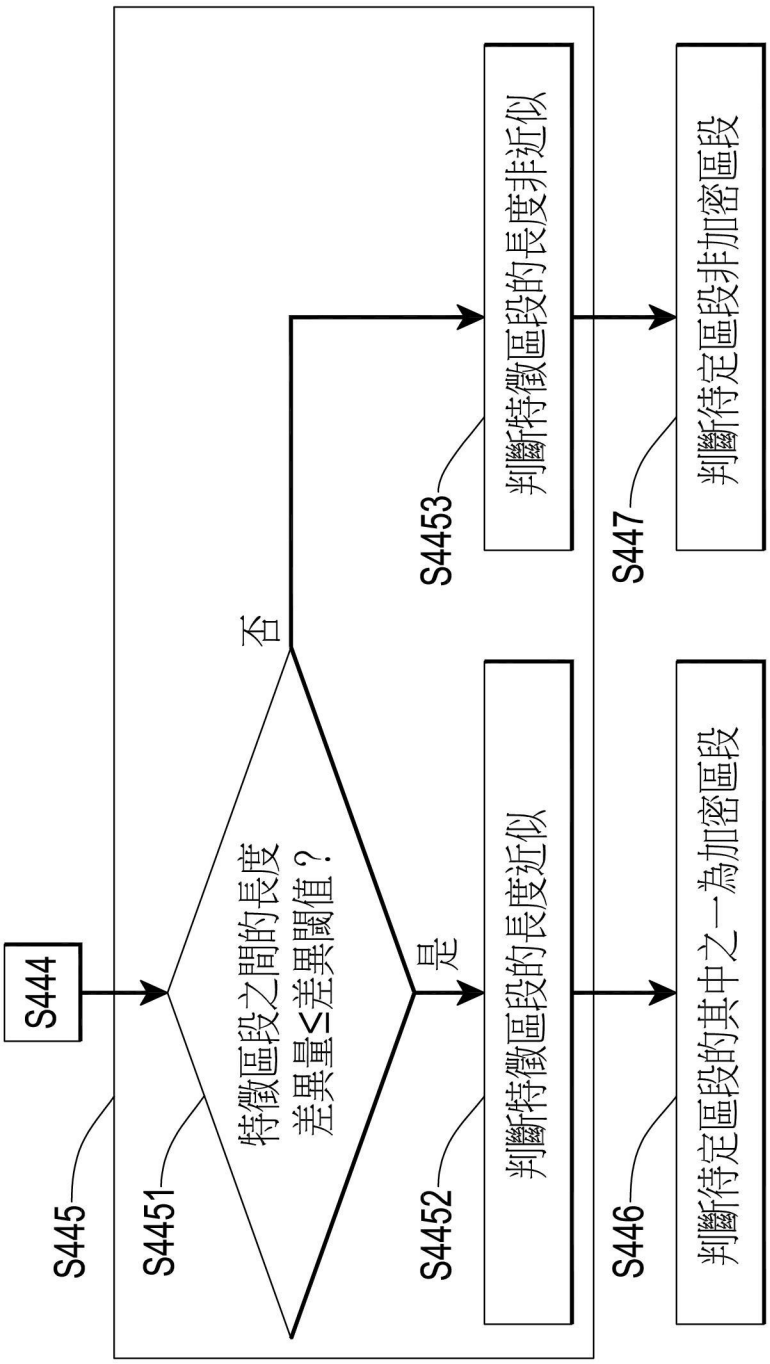
S444
S445
S4451
特徵區段之間的長度
差異量≤差異閾值？
否
是
S4452
判斷特徵區段的長度近似
S446
判斷待定區段的其中之一為加密區段
S4453
判斷特徵區段的長度非近似
S447
判斷待定區段非加密區段

圖13

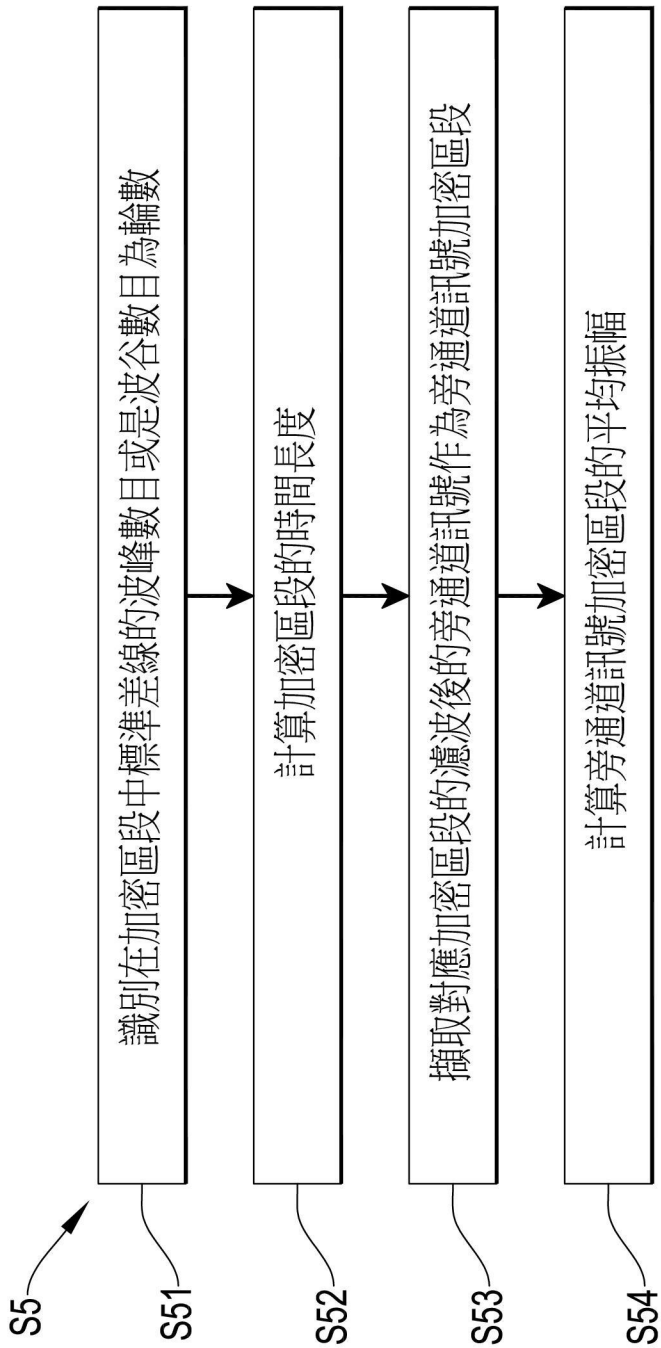
S5
S51
識別在加密區段中標準差線的波峰數目或是波谷數目為輪數
S52
計算加密區段的時間長度
S53
擷取對應加密區段的濾波後的旁通道訊號作為旁通道訊號加密區段
S54
計算旁通道訊號加密區段的平均振幅

圖14

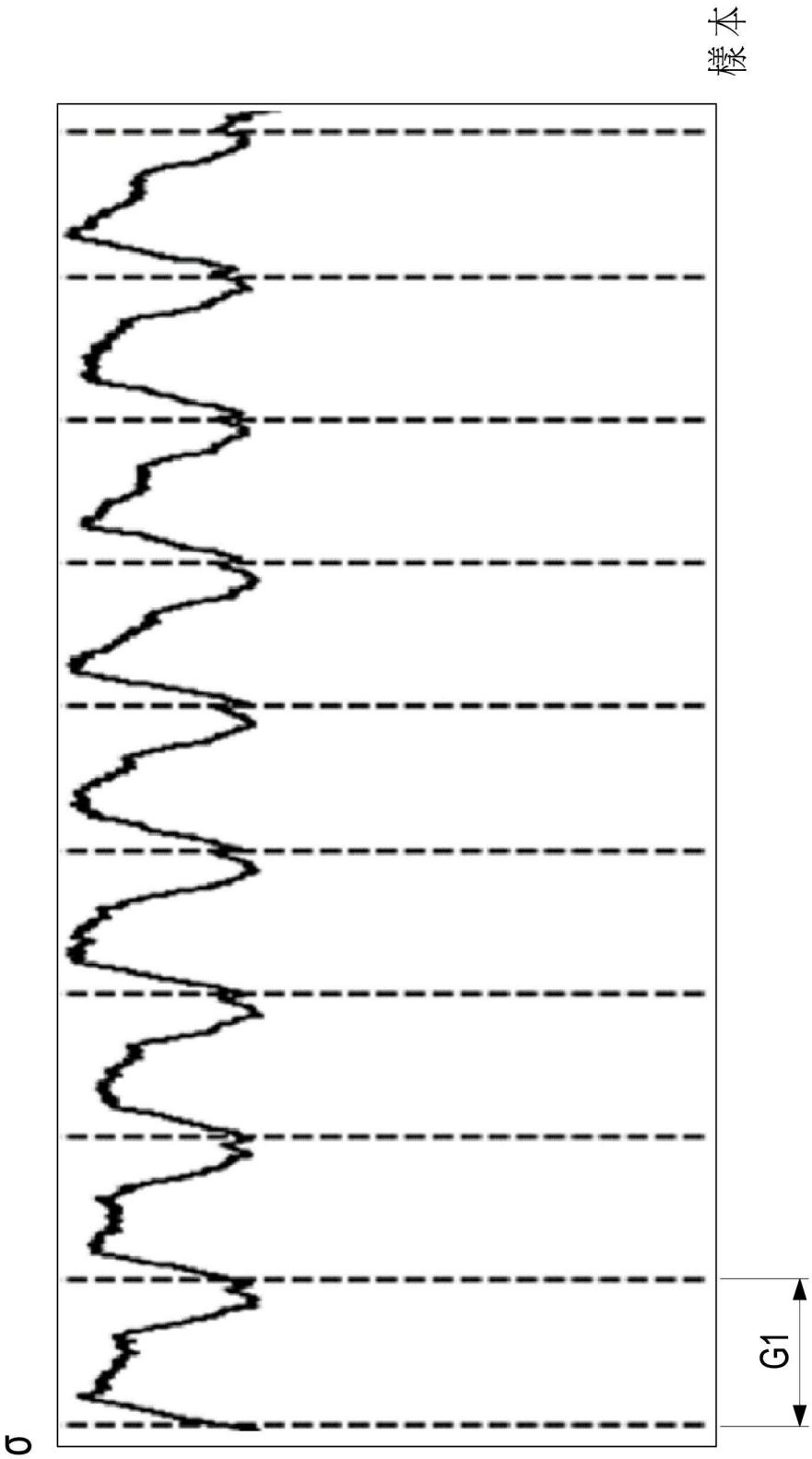

圖15

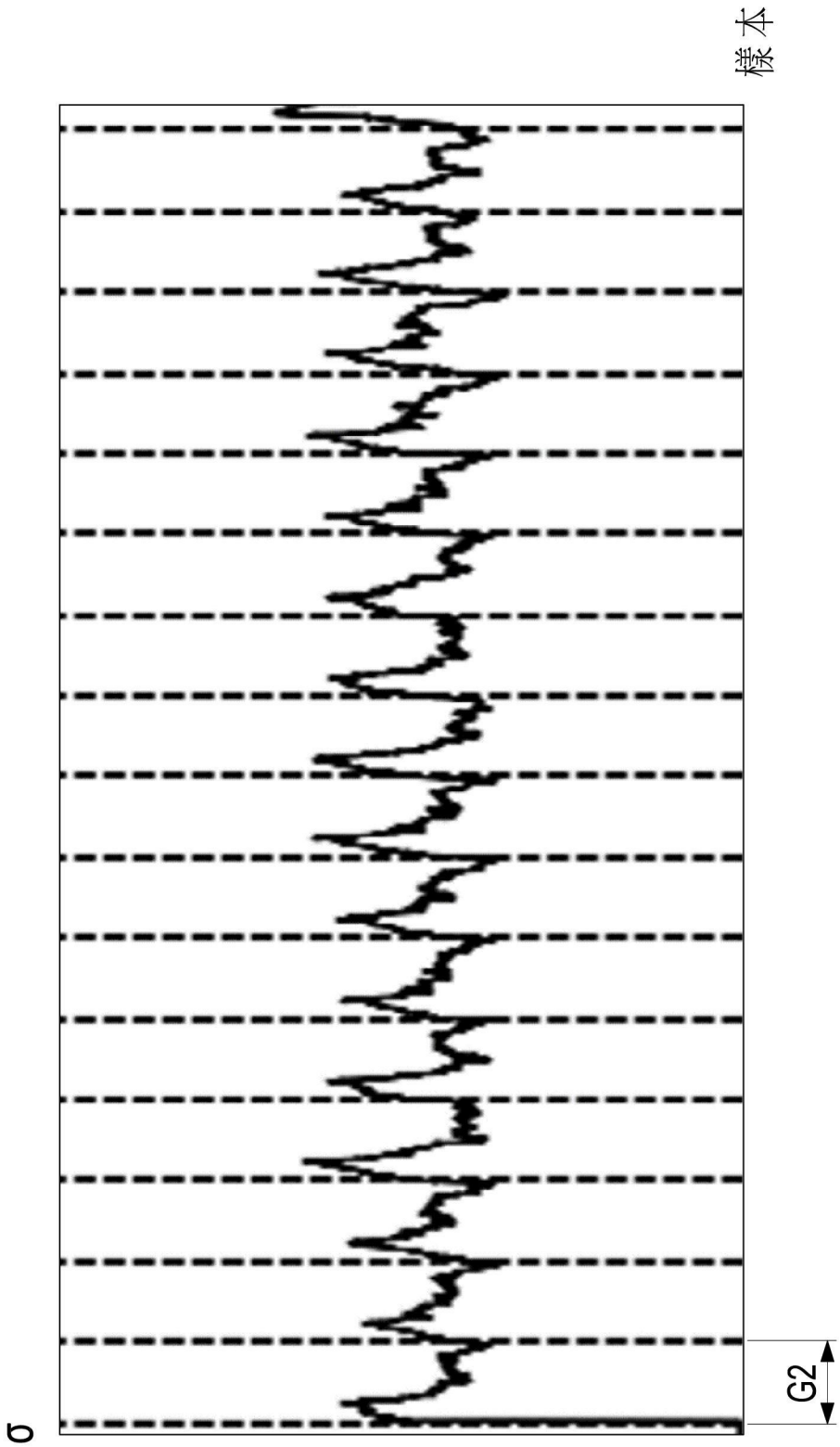

圖16

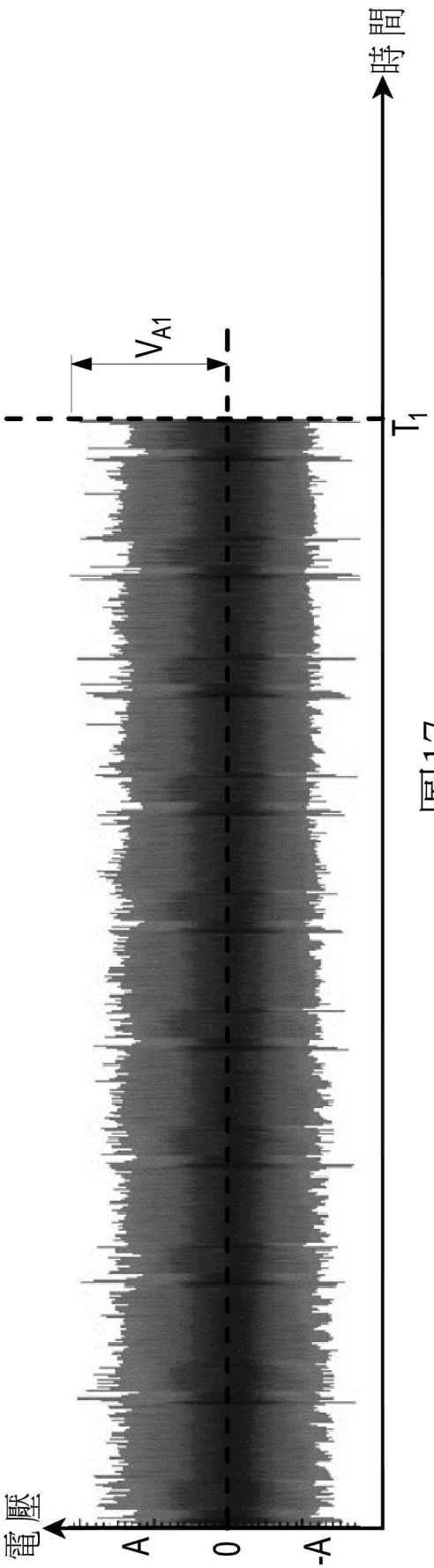

圖17

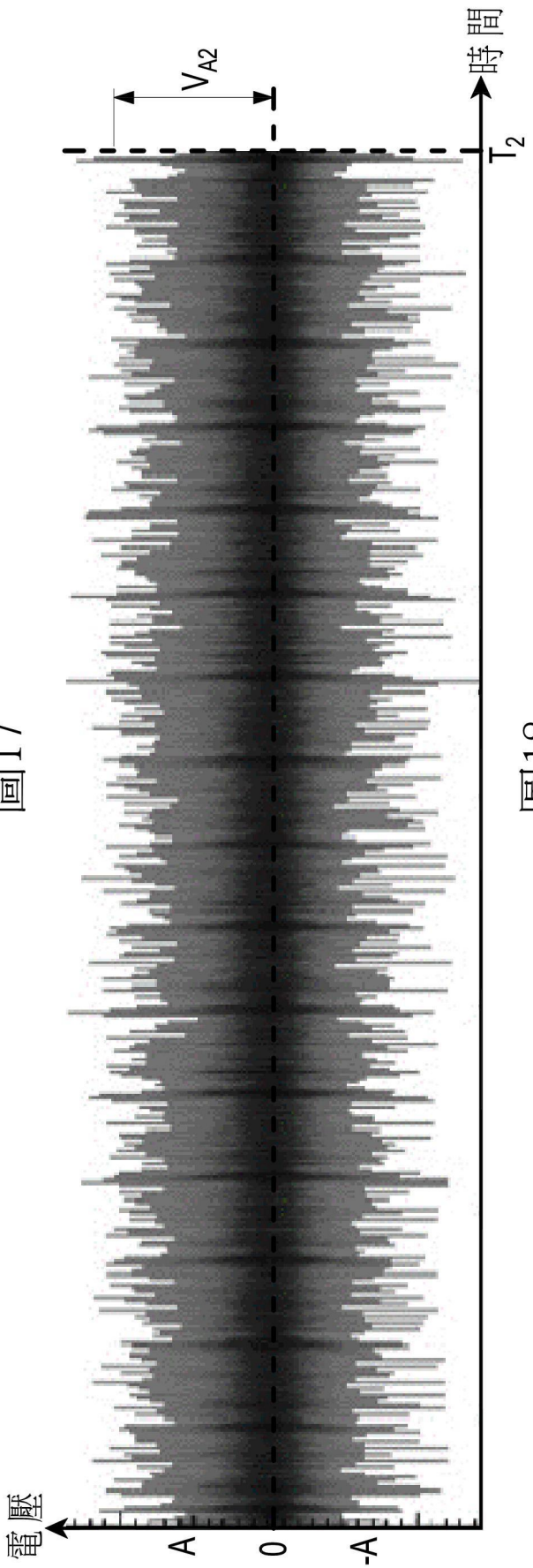

圖18