【19】中華民國　　【12】專利公報　（B）

【11】證書號數：I462009
【45】公告日： 中華民國 103 (2014) 年 11 月 21 日
【51】Int. Cl.：　*G06F7/58　(2006.01)*

發明　　全 3 頁

【54】名　稱：亂數產生方法
METHOD FOR RANDOM NUMBER GENERATION

【21】申請案號：100143325　　【22】申請日： 中華民國 100 (2011) 年 11 月 25 日
【11】公開編號：201322119　　【43】公開日期： 中華民國 102 (2013) 年 06 月 01 日

【72】發 明 人： 陳以德 (TW) CHEN, I TE；蔡哲民 (TW) TSAI, JER MIN；曾正男 (TW) TZENG, JENG NAN；何文獻 (TW) HO, WEN HSIEN
【71】申 請 人： 高雄醫學大學　KAOHSIUNG MEDICAL UNIVERSITY
高雄市三民區十全一路 100 號
【74】代 理 人： 黃耀霆

【56】參考文獻：
TW　I240200　　TW　I270004
US　2010/0106756A1

審查人員：林明宗

[57]申請專利範圍

1. 一種亂數產生方法，係包含：一樣本選取步驟，係將一取樣裝置所擷取之訊號源，傳送至一轉碼器以輸出一序列，再透過一運算器從該序列中，隨機選取符合運算長度且連續之序列，作為一運算種子；一運算值設定步驟，係利用該運算器所包含之一設定演算法，將該運算種子轉換為數運算值中之一第一運算值，其中該數個運算值中除了該第一運算值之外皆設為 0；一亂度判斷步驟，係藉由該運算器，判斷數運算值中之該第一運算值與一第二運算值間之數值差異是否大於一亂度門檻值；一運算值處理步驟，係於該亂度判斷步驟判斷為否時，利用該運算器判斷該第一運算值進入該運算值處理步驟之一重設次數是否大於一重設限制值，若是，則執行該樣本選取步驟，若否，則利用該運算器所包含之一重設演算法重設該第一運算值，再執行該亂度判斷步驟；一亂數產生步驟，係於該亂度判斷步驟判斷為是時，利用該運算器所包含之一亂數演算法，將該數運算值轉換為一亂數值；一亂數處理步驟，係利用該運算器計算該亂數值之位元總數，當該位元總數不為該運算種子之運算長度之位元個數的倍數時，執行該運算值設定步驟；當該位元總數 為該運算種子之運算長度之位元個數的倍數時，係將最後產生且符合運算長度之位元個數的數亂數值設定為該運算種子，再執行該運算值設定步驟。
2. 如申請專利範圍第 1 項所述之亂數產生方法，其中該數運算值包含該第一運算值、該第二運算值及一第三運算值，且該第一運算值、第二運算值及第三運算值之初始值皆設為 0。
3. 如申請專利範圍第 2 項所述之亂數產生方法，其中該運算值設定步驟之設定演算法為：$C_i = 10 + (RND_{byte} * i + (CP_i << 2) + R)\%25$ 其中，該 C_i 為第一運算值；該 CP_i 為第二運算值；該 RND_{byte} 為該運算種子；i 為選取序列之個數；R 為該演算法執行之總次數；<<2 代表向左移位 2 位元；%25 代表將前述數值除以 25 並取餘數之值。
4. 如申請專利範圍第 2 項所述之亂數產生方法，其中該亂度判斷步驟中，該第一和第二運算值間之數值差異的計算方式為：$(C_i - CP_i)^2$

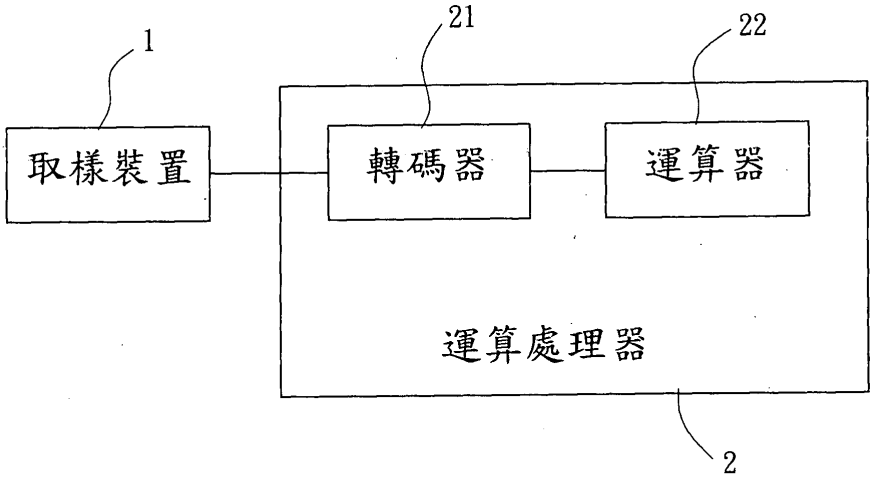
5. 如申請專利範圍第 2 項所述之亂數產生方法，其中該運算值重設與計次步驟之重設演算法為：$C_i = 10 + (CP_i + (C_i \wedge W) + R)\%25$ 其中，該 W 代表該重設次數，^代表指數運算子。
6. 如申請專利範圍第 2 項所述之亂數產生方法，其中該亂數產生步驟之亂數演算法為：$bit[i] = 1\&(C_1 \oplus C_2 \oplus ... \oplus C_n \oplus CP_1 \oplus CP_2 \oplus ... \oplus CP_n \oplus CPP_1 \oplus CPP_2 \oplus ... \oplus CPP_n)$ 其中，該&代表 AND 運算子，該⊕代表 XOR 運算子，$bit[i]$ 代表產生之該亂數值。
7. 如申請專利範圍第 2 項所述之亂數產生方法，其中該亂數處理步驟係包含：步驟(a)：係利用該運算器，判斷該亂數值之位元總數是否為該運算種子之運算長度之位元個數的倍數；步驟(b)：係於該步驟(a)判斷為否時，利用該運算器將該第二運算值之序列指定為該第一運算值之序列，並執行該運算值設定步驟；步驟(c)：係於該步驟(a)判斷為是時，利用該運算器將該第三運算值之序列指定為該第一運算值之序列；步驟(d)：係於該步驟(a)判斷為是時，利用該運算器將最後產生且符合該運算種子之位元總數的數亂數值設定為該運算種子。
8. 如申請專利範圍第 1 項所述之亂數產生方法，其中該亂度門檻值設為該訊號源前 1K byte 的資料之變異數的一半。
9. 如申請專利範圍第 1 項所述之亂數產生方法，其中該重設限制值設為 100。

圖式簡單說明

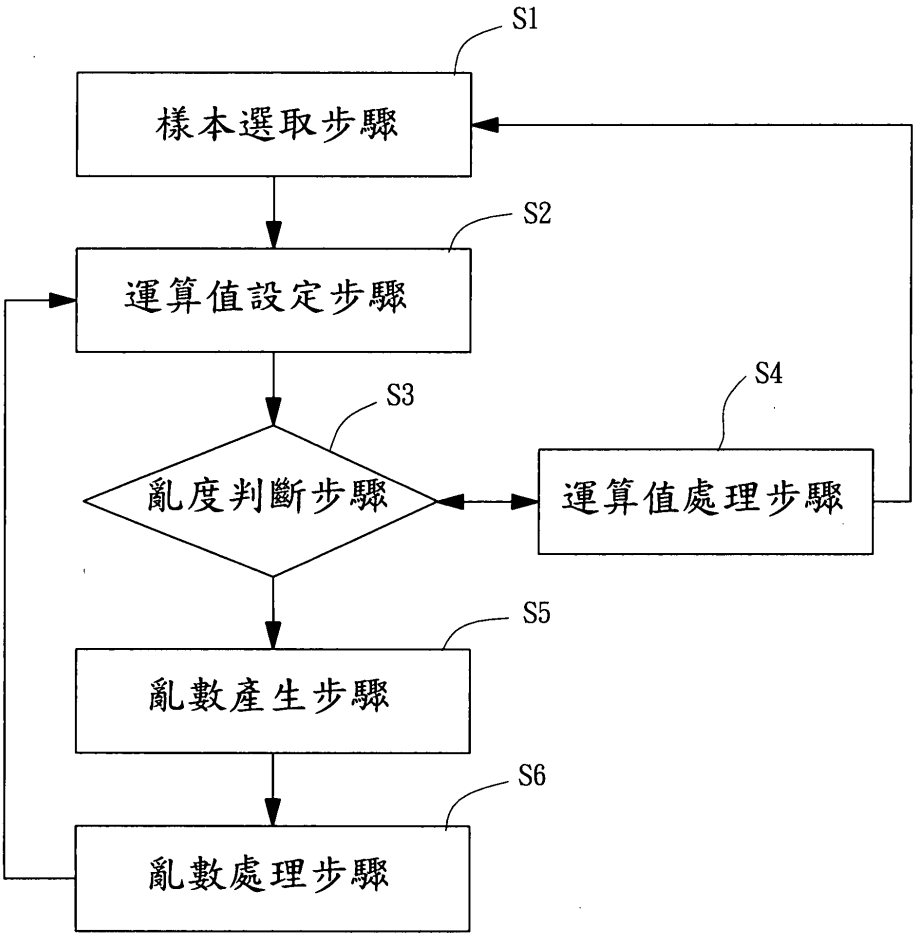
第 1 圖：本發明亂數產生方法之架構圖。

第 2 圖：本發明亂數產生方法之步驟流程圖。

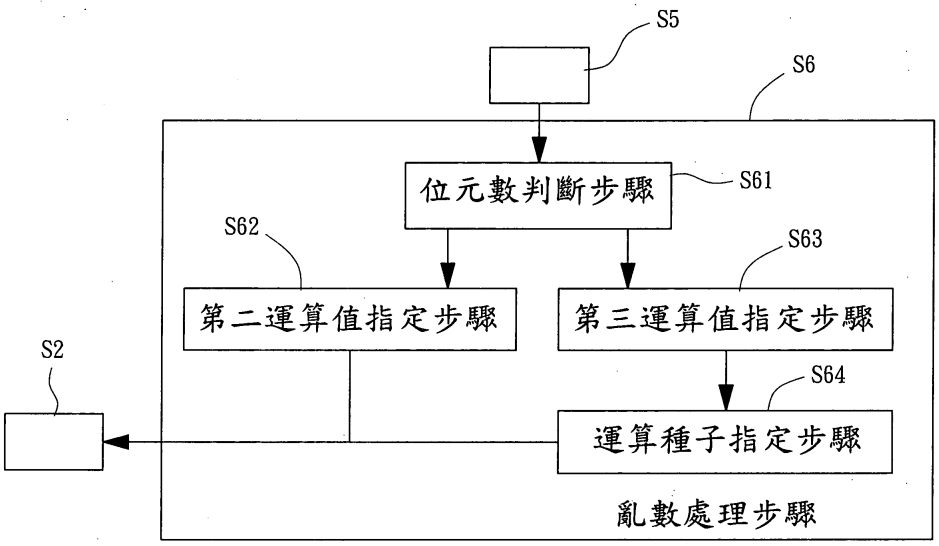
第 3 圖：本發明亂數產生方法之亂數處理步驟流程圖。



第 1 圖


S1
樣本選取步驟
S2
運算值設定步驟
S3
亂度判斷步驟
S4
運算值處理步驟
S5
亂數產生步驟
S6
亂數處理步驟

第 2 圖


S5
S6
位元數判斷步驟
S61
S62
S63
第二運算值指定步驟
第三運算值指定步驟
S2
S64
運算種子指定步驟
亂數處理步驟

第 3 圖