公告本

I234706

申請日期： 91.7.26.	案號： 91116693
類別： G06F11/22, G01C1/00	

（以上各欄由本局填註）

發明專利說明書

一、發明名稱	中 文	韌體鑑權系統及方法
	英 文	SYSTEM AND METHOD FOR FIRMWARE AUTHENTICATION
二、發明人	姓 名（中文）	1. 王宏榮
	姓 名（英文）	1. Wang, Hung-Zung
	國 籍	1. 中華民國 ROC
	住、居所	1. 台北縣土城市自由街2號 (2, Tzu Yu Street, Tu-Cheng City, Taipei Hsien, Taiwan, ROC)
三、申請人	姓 名（名稱）（中文）	1. 鴻海精密工業股份有限公司
	姓 名（名稱）（英文）	1. HON HAI PRECISION INDUSTRY CO., LTD.
	國 籍	1. 中華民國 ROC
	住、居所（事務所）	1. 台北縣土城市自由街2號 (2, Tzu Yu Street, Tu-Cheng City, Taipei Hsien, Taiwan, ROC)
	代表人姓 名（中文）	1. 郭台銘
	代表人姓 名（英文）	1. Gou, Tai-Ming

本案已向

國(地區)申請專利	申請日期	案號	主張優先權
無			

有關微生物已寄存於　　寄存日期　　寄存號碼

無

五、發明說明（1）

【發明領域】

本發明係有關一種韌體鑑權系統及方法，尤指一種使用於資訊產品之韌體鑑權系統及方法。

【發明背景】

按，隨著資訊產業之快速發展，市場上出現多種資訊產品。而在各種資訊產品上，一般均設有一貯存器以貯存韌體，該韌體與資訊產品上的電路相配合，從而實現該資訊產品之功能。惟，該資訊產品的電路設計一經公開使用，即很容易被他人複製；而隨著半導體技術的發展，他人亦很容易藉燒錄器對貯存在貯存器中的韌體進行複製。從而，他人可不經授權即製造相同的資訊產品，使得該資訊產品的設計利益受損。

【發明目的】

本發明之目的在於提供一種防止他人未經授權而對韌體非法使用之韌體鑑權系統及方法。

【發明特徵】

本發明之韌體鑑權系統及方法，該韌體鑑權系統包括一貯存有韌體之貯存器、一可程式化微處理器及一微處理器，其中微處理器係用於耦合貯存器與可程式化微處理器。韌體中包括第一密碼算法，可程式化微處理器中設有小容量的只讀貯存器以貯存第二密碼算法。該韌體鑑權方法係藉由校驗第一、第二密碼算法所產生的二數字簽章是否匹配而進行，而所述第一、第二密碼算法係採用相同輸入值進行運算以產生所述二數字簽章。

五、發明說明（2）

【較佳實施例】

請參閱第一圖所示，其係一利用本發明之韌體鑑權系統的實施例。該韌體鑑權系統包括一貯存有韌體10之貯存器1、一可程式化微處理器2及一微處理器3，該微處理器3連接在貯存器1與可程式化微處理器2之間。韌體10包括隨機數產生單元11、計數單元12、數據合成單元13、第一密碼算法14、校驗單元15及功能單元16，功能單元16係用於實現資訊產品的功能。可程式化微處理器2中設有小容量的只讀貯存器20以貯存第二密碼算法24。

請參閱第二圖所示，本發明之韌體鑑權方法在微處理器3中的的執行步驟如下：

步驟110：隨機數產生單元11隨機產生隨機數；

步驟111：計數單元12對累加數n（累加數n初始值為0）進行計數，並判斷累加數n是否大於一特定值N（N值一般為5），若是，則系統終止，若否，則執行下一步驟112；

步驟112：數據合成單元13藉由上述隨機數為輸入執行運算，產生十六位元的鑰匙；

步驟113：十六位元的鑰匙被傳送給可程式化微處理器2；

步驟114：貯存器1中的第一密碼算法14藉由十六位元的鑰匙為輸入執行運算，產生數字簽章A，同時，可程式化微處理器2中的第二密碼算法24藉由十六位元的鑰匙為輸入執行運算，產生數字簽章B；

五、發明說明（3）

步驟115：微處理器3從可程式化微處理器2中接收數字簽章B；

步驟116：校驗單元15對數字簽章A與數字簽章B進行校驗是否匹配，若是，則鑑權流程結束，開始執行功能單元16，若否，則回到步驟111重新開始執行鑑權流程。

在實施中，第一密碼算法14與第二密碼算法24可以相同，此時，校驗單元15採用一比較器比對數字簽章A與數字簽章B是否相同即可完成校驗工作。

第一密碼算法14與第二密碼算法24亦可不相同，此時，校驗單元15係為一互補比較器，該互補比較器校檢第一、第二密碼算法14、24所產生的數字簽章A、B是否互補，即可完成校驗工作。

另，計數單元12可以省略以減少鑑權流程所需步驟，惟此可能會導致鑑權流程進入死循環。數據合成單元13亦可省略，二密碼算法14、24可採用隨機數產生單元11所產生的隨機數為輸入。

因可程式化微處理器2中只讀貯存器20所貯存的第二密碼算法他人無法進行非法複製，如是，即便他人可以將資訊產品上的電路設計及貯存器1中的韌體10非法複製，惟其因無相應的可程式化微處理器2而無法製造相同的產品。

相較於習知技術，本發明藉由貯存器1中的第一密碼算法14及可程式化微處理器2中的第二密碼算法24進行鑑權，可防止他人未經授權而非法使用韌體10。

五、發明說明（4）

綜上所述，本發明確已符合發明專利之要件，爰依法提出申請。惟，以上所述僅為本發明之較佳實施例，自不能以此限定本發明之權利範圍。舉凡熟悉此項技藝之人士爰依本發明之精神所作之等效修飾或變化者，皆應涵蓋在以下申請專利範圍內。

圖式簡單說明

第一圖係本發明鑑權系統之硬體方塊圖。

第二圖係本發明鑑權方法之流程圖。

【元件符號說明】

貯存器	1	韌體	10
隨機數產生單元	11	計數單元	12
數據合成單元	13	第一密碼算法	14
校驗單元	15	功能單元	16
可程式化微處理器	2	只讀貯存器	20
第二密碼算法	24	微處理器	3

四、中文發明摘要　（發明之名稱：韌體鑑權系統及方法）

一種韌體鑑權系統及方法，該韌體鑑權系統包括一貯存有韌體之貯存器、一可程式化微處理器及一微處理器，其中微處理器係用於耦合貯存器與可程式化微處理器。韌體中包括第一密碼算法，可程式化微處理器中設有小容量的只讀貯存器以貯存第二密碼算法。該韌體鑑權方法係藉由校驗第一、第二密碼算法所產生的二數字簽章是否匹配而進行，而所述第一、第二密碼算法係採用相同輸入值進行運算以產生所述二數字簽章。

英文發明摘要　（發明之名稱：SYSTEM AND METHOD FOR FIRMWARE AUTHENTICATION）

A system and method for firmware authentication, the system includes a memory embedded with a firmware therein, a programmable microprocessor, and a microprocessor coupling the memory with the programmable microprocessor. The firmware includes a first cryptographic algorithm. The programmable microprocessor has a ROM that stores a second cryptographic algorithm. The first and second cryptographic algorithms respectively generate a first and a second digital signatures

四、中文發明摘要　（發明之名稱：韌體鑑權系統及方法）

英文發明摘要　（發明之名稱：SYSTEM AND METHOD FOR FIRMWARE AUTHENTICATION）

in response to a same input. The method is accomplished by checking whether the first and second digital signatures match to each other.

六、申請專利範圍

1. 一種韌體鑑權系統，係用於防止他人非法使用貯存在貯存器中的韌體，包括：

隨機數產生單元、第一密碼算法、校驗單元，係設於韌體中；

可程式化微處理器，其中設有只讀貯存器以貯存第二密碼算法；及

微處理器，係耦合該貯存器與該可程式化微處理器；其中

第一、第二密碼算法藉由隨機數產生單元所產生的同一隨機數為輸入而產生二數字簽章，校驗單元校驗該二數字簽章是否匹配，若是，則韌體鑑權流程結束。

2. 如申請專利範圍第1項所述之韌體鑑權系統，其中貯存器中的第一密碼算法與可程式化微處理器中的第二密碼算法相同。

3. 如申請專利範圍第2項所述之韌體鑑權系統，其中校驗單元係一比較器。

4. 如申請專利範圍第1項所述之韌體鑑權系統，其中貯存器中的第一密碼算法與可程式化微處理器中的第二密碼算法不相同。

5. 如申請專利範圍第4項所述之韌體鑑權系統，其中校驗單元係為一互補比較器。

6. 如申請專利範圍第1項所述之韌體鑑權系統，其中韌體之隨機數產生單元與第一密碼算法之間還包括一數據合成單元，該數據合成單元藉由隨機數產生單元所產

六、申請專利範圍

生的隨機數為輸入而產生一數位式的鑰匙，該鑰匙同時傳送給二密碼算法。

7. 如申請專利範圍第6項所述之韌體鑑權系統，其中數位式的鑰匙具有十六位元。

8. 如申請專利範圍第6項所述之韌體鑑權系統，其中韌體之隨機數產生單元與數據合成單元之間進一步還包括一計數單元，計數單元對累加數n進行計數，並判斷累加數n是否大於一特定值N，若是，則韌體鑑權流程中止，若否，則執行數據合成單元。

9. 一種韌體鑑權方法，係可用於防止他人非法使用貯存在貯存器中的韌體，包括下述步驟：

在韌體中提供隨機數產生單元、第一密碼算法及校驗單元；

提供一可程式化微處理器，該可程式化微處理器中設有一只讀貯存器以貯存一第二密碼算法；

提供一微處理器，係耦合於貯存器與可程式化微處理器之間，該微處理器可執行上述韌體；

隨機數產生單元隨機產生隨機數；

第一、第二密碼算法採用該隨機數為輸入而產生二數字簽章；

校驗單元校驗該二數字簽章是否匹配，若是，則鑑權流程結束。

10. 如申請專利範圍第9項所述之韌體鑑權方法，其中所述韌體鑑權方法還包括下述步驟：

六、申請專利範圍

在韌體之隨數產生單元與第一密碼算法之間提供一數據合成單元；

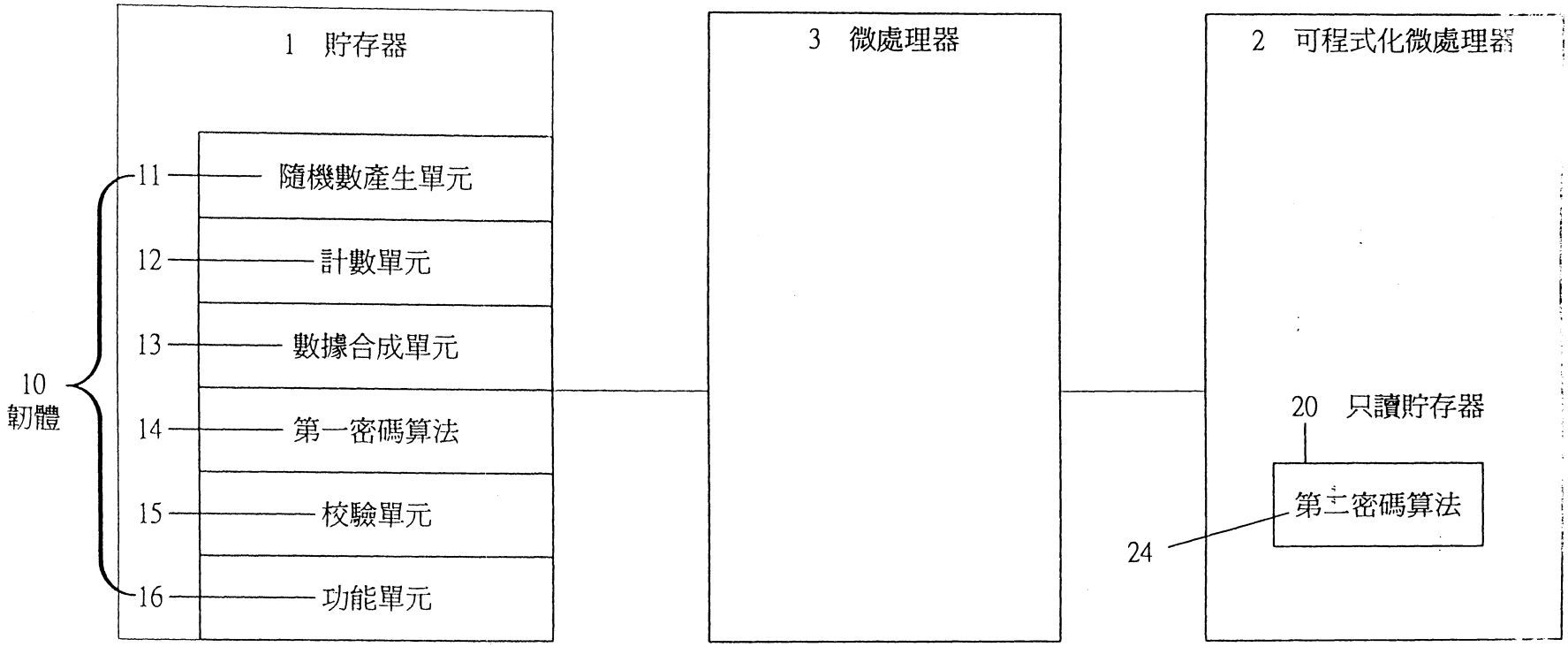
數據合成單元藉由隨機數產生單元所產生的隨機數為輸入產生十六位元的鑰匙；

將該十六位元的鑰匙同時傳送給二密碼算法。

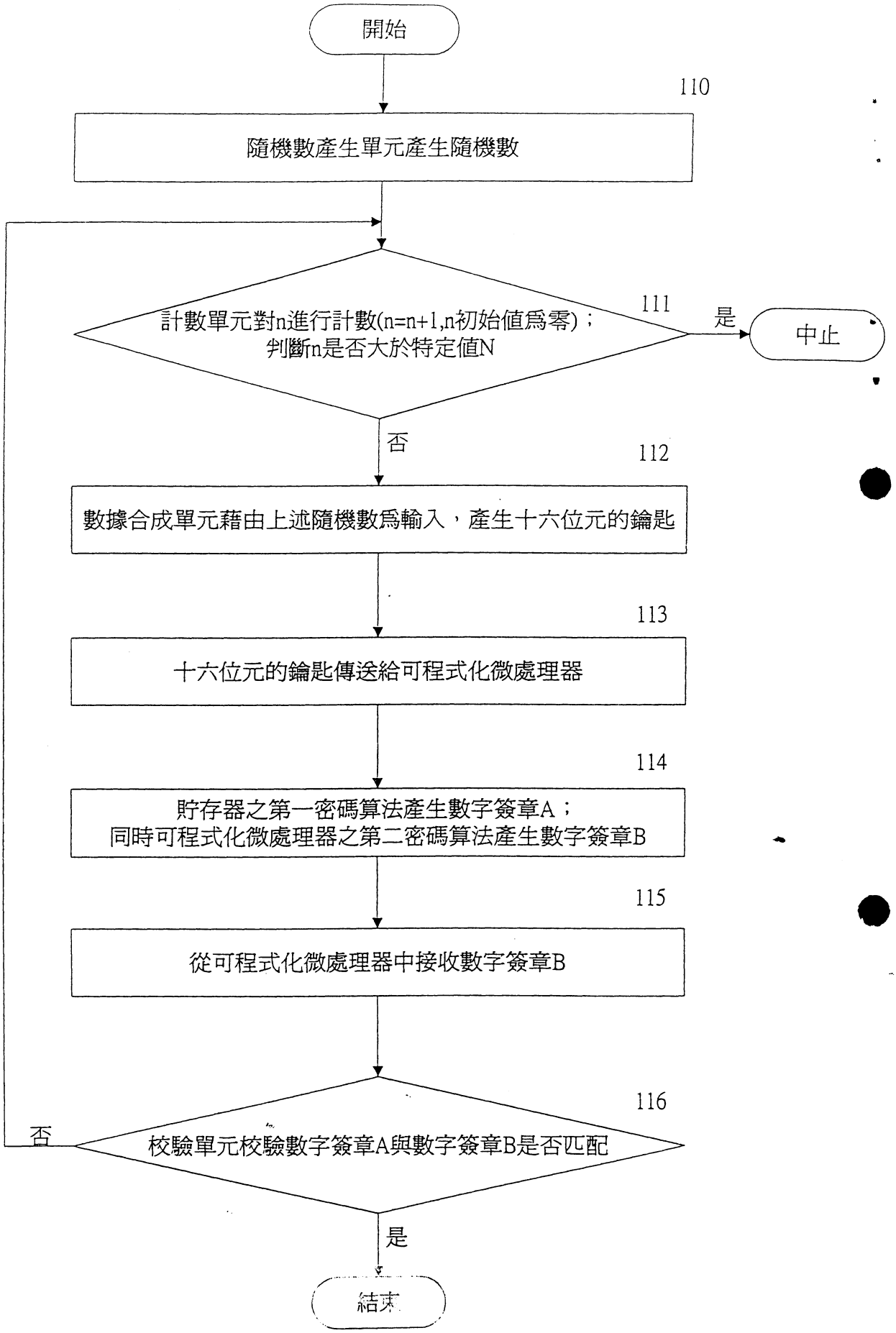
11. 如申請專利範圍第10項所述之韌體鑑權方法，其中所述韌體鑑權方法還包括下述步驟：

在韌體之隨數產生單元與數據合成單元之間進一步提供一計數單元；

計數單元對累加數n進行計數，並判斷累加數n是否大於一特定值N，若是，則韌體鑑權流程中止，若否，則執行數據合成單元。


1 貯存器
11
隨機數產生單元
12
計數單元
13
數據合成單元
10
韌體
14
第一密碼算法
15
校驗單元
16
功能單元
3 微處理器
2 可程式化微處理器
20 只讀貯存器
第二密碼算法
24

第一圖


開始
110
隨機數產生單元產生隨機數
111
計數單元對n進行計數(n=n+1,n初始值爲零)；
判斷n是否大於特定值N
是
中止
否
112
數據合成單元藉由上述隨機數爲輸入，產生十六位元的鑰匙
113
十六位元的鑰匙傳送給可程式化微處理器
114
貯存器之第一密碼算法產生數字簽章A；
同時可程式化微處理器之第二密碼算法產生數字簽章B
115
從可程式化微處理器中接收數字簽章B
116
否
校驗單元校驗數字簽章A與數字簽章B是否匹配
是
結束

第二圖