專利申請實務分享

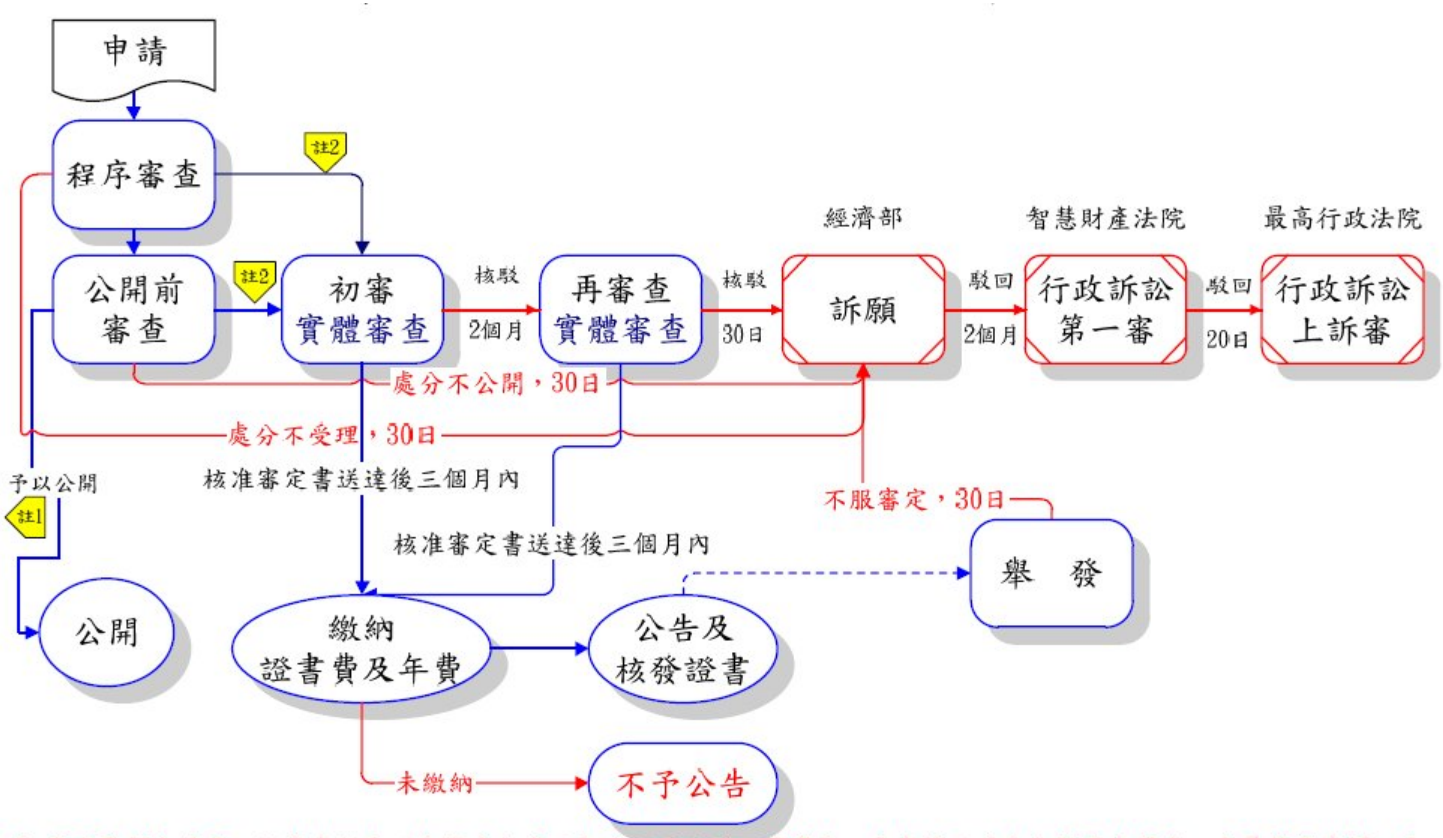
專利要件

- 申請發明/新型專利應具備新穎性、進步性及產業上可利用性(實用性)
- 產業利用性
  - 若申請專利之發明在產業上能被製造或使用，則認為該發明具產業利用性
  - 不考慮經濟價值，僅須具有應用於產業可能性即可
  - 專利三要件中第一項審查要件
- 新穎性
  - 若申請專利範圍(Claim)中所載之發明未構成先前技術(Prior art)的一部分時，則該發明具新穎性；
    - 先前技術涵蓋申請日前所有能為公眾得知之資訊，且不限區域、語言及形式，即所有處於公眾有可能接觸並能獲知該技術之實質內容的狀態之資訊，例如書面、電子、網際網路、口頭、展示或使用等
  - 如果發明於申請前已見於刊物或已公開使用或為公眾所知悉者，該發明即不具新穎性
- 進步性
  - 申請專利之發明雖與先前技術有差異，但該發明之整體係為該發明所屬技術領域中具有通常知識者依申請前之先前技術所能輕易完成時，稱該發明不具進步性。

專利申請注意事項(台灣)

- **中華民國專利申請可分為發明、新型、新式樣**
- **發明專利**
  - 申請專利之「發明」必須是利用自然界中固有的規律所產生之技術思想的創作；即須具有技術性， 例如：(不需使用底片之照相機)
  - 自然法則(例 如：科學原理)本身、單純之發現、違反自然法則者(例如：永動機) 非利用自然法則者(例如：數學方法、推理能力、遊戲規則)、非技術思想者(例如：技能、單純資訊揭露、美術創作)等，都不符合專利對發明的定義。
  - 法律規定：不予發明專利之項目
    - 動、植物及生產動、植物之主要生物學方法
    - 人體或動物疾病之診斷、治療或外科手術方法
    - 妨害公共秩序、善良風俗、或衛生者
  - 申請日起算二十年
- **新型專利**
  - 申請專利之「新型」必須是利用自然界中固有的規律所產生之技術思想，對物品之形狀、構造或裝置之創作， 例如：(照相機之快門裝置)
  - 如果沒有固定形狀就是申請「發明」專利
  - 申請日起算十年
- **新式樣專利**
  - 申請專利之「新式樣」 必須是對物品之形狀、花紋、色彩或其結合，透過視覺訴求之創作，即新式樣專利為保護外觀視覺性創作的設計專利。例如：(流線型照相機匣)
  - 申請日起算十二年

發明專利案審查及行政救濟流程圖



1. 發明專利申請案，經審查認無不合規定程式且無應不予公開之情事者，自申請日（有主張優先權者，自最早優先權之次日）起18個月後公開之。
2. 發明專利申請案，自申請日起3年內，任何人均得申請實體審查，始進入實體審查。

專利號碼的種類

- 發明申請案達18個月，會將專利申請案的內容公開，所以官方會給一個公開號碼
- 所謂『公告號』係指專利申請案已獲准，官方會給一個公告號，而該公告號又稱為專利號、授證號或證書號
- 英文I**代表發明專利**，M**代表新型專利**，D**則代表新式樣專利**

台灣專利首頁資訊

【19】中華民國　　【12】專利公報　（B）

【11】證書號數：I350486

【45】公告日：中華民國 100 (2011) 年 10 月 11 日

【51】Int. Cl.：　*G06K9/00　(2006.01)*　　*G09C1/00　(2006.01)*

發明　　全 4 頁

【54】名　稱：生物辨識方法與裝置以及其生物特徵資料之加密方法

BIOMETRICS METHOD AND APPARATUS AND BIOMETRIC DATA ENCRYPTION METHOD THEREOF

【21】申請案號：096144798　　【22】申請日：中華民國 96 (2007) 年 11 月 26 日

【11】公開編號：200923798　　【43】公開日期：中華民國 98 (2009) 年 06 月 01 日

【72】發 明 人：邱錫彥 (TW) CHIOU, SHIN YAN；陳彥學 (TW) CHEN, YEN SHA

【71】申 請 人：財團法人工業技術研究院　INDUSTRIAL TECHNOLOGY RESEARCH INSTITUTE

新竹縣竹東鎮中興路 4 段 195 號

【74】代 理 人：詹銘文；蕭錫清

【56】參考文獻：

TW	200530943	TW	200707310
US	20070253608A1	US	2007/0174633A1

[57]申請專利範圍

1. 一種生物特徵資料之加密方法，包括：提供一生物特徵資料；依據一門檻值，定義出多個數值範圍，其中該些數值範圍各自具有一量化值；若該生物特徵資料落入該些數值範圍其中之一，則以該數值範圍之量化值做為一量化特徵資料以取代該生物特徵資料；進行一單向函數運算，以將該量化特徵資料轉換為一加密特徵資料；計算該量化特徵資料與該生物特徵資料之差值，以獲得一調整值；以及儲存該調整值與該加密特徵資料。
2. 如申請專利範圍第 1 項所述生物特徵資料之加密方法，更包括設定該門檻值。
3. 如申請專利範圍第 1 項所述生物特徵資料之加密方法，其中該生物特徵資料包括指紋特徵值、虹膜特徵值、掌紋特徵值或瞳孔特徵值。
4. 如申請專利範圍第 1 項所述生物特徵資料之加密方法，其中該單向函數運算包括一雜湊函數運算。
5. 如申請專利範圍第 1 項所述生物特徵資料之加密方法，其中進行該單向函數運算之步驟，包括將該量化特徵資料與一金鑰值一同進行一雜湊函數運算。
6. 如申請專利範圍第 5 項所述生物特徵資料之加密方法，其中該金鑰值包括：一預設值、一亂數、或一實數。
7. 一種生物辨識方法，包括：提供一加密註冊資料與一調整值；擷取一生物特徵資料；依據該調整值調整該生物特徵資料；依據一門檻值，定義出多個數值範圍，其中該些數值範圍各自具有一量化值；若調整後的該生物特徵資料落入該些數值範圍其中之一，則以該數值範圍之量化值做為一量化特徵資料以取代調整後的該生物特徵資料；進行一單向函數運算，以將該量化特徵資料轉換為一加密特徵資料；以及比對該加密註冊資料與該加密特徵資料。
8. 如申請專利範圍第 7 項所述生物辨識方法，更包括設定該門檻值。
9. 如申請專利範圍第 7 項所述生物辨識方法，其中該生物特徵資料包括指紋特徵值、虹膜特徵值、掌紋特徵值或瞳孔特徵值。

獲證專利首頁相關資訊-美國

類別碼

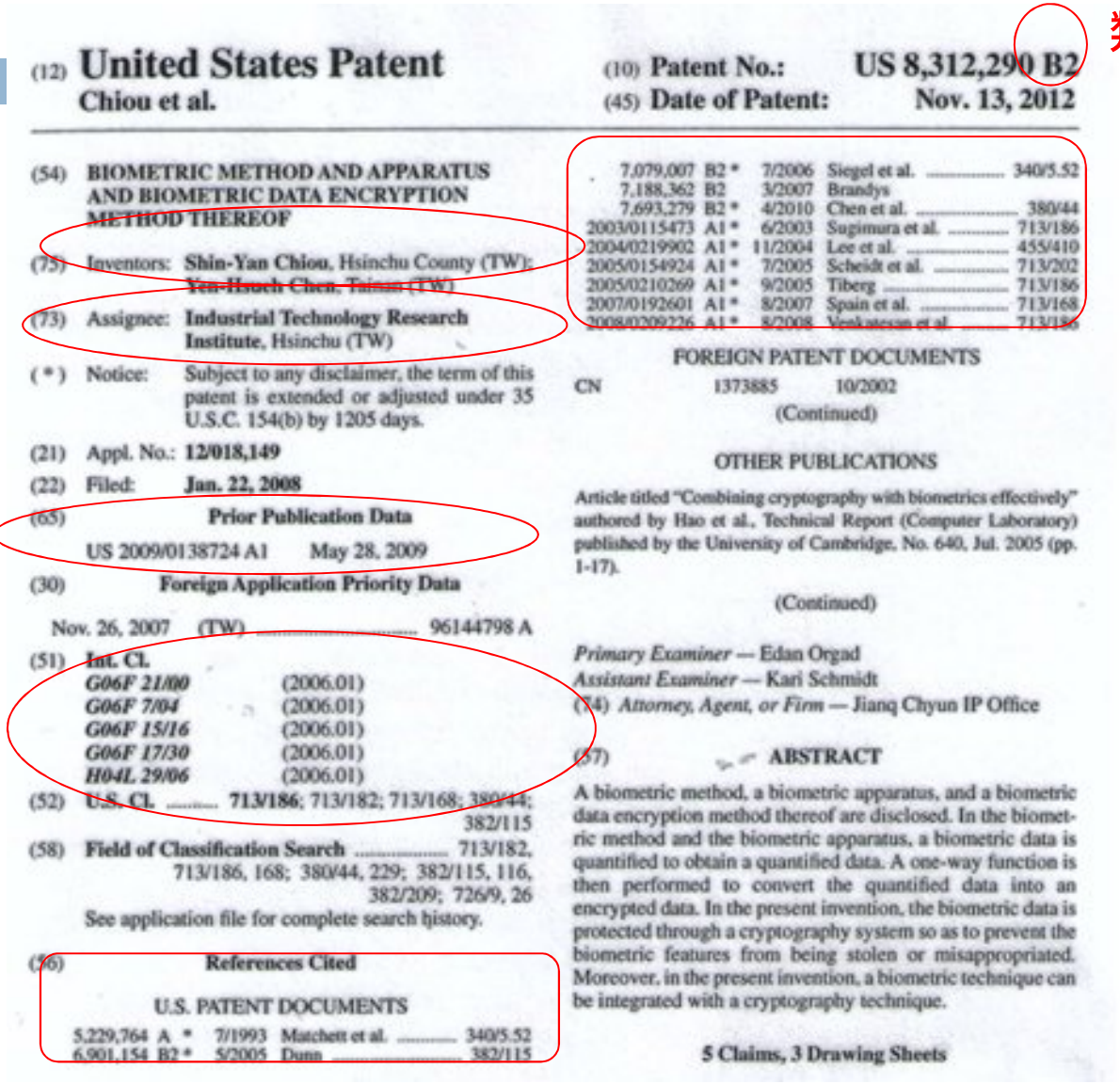
發明人

申請人

公開日

技術分類號

美國專利前案



(12) **United States Patent**
Chiou et al.

(10) **Patent No.: US 8,312,290 B2**
(45) **Date of Patent: Nov. 13, 2012**

(54) **BIOMETRIC METHOD AND APPARATUS AND BIOMETRIC DATA ENCRYPTION METHOD THEREOF**

(75) Inventors: **Shin-Yan Chiou**, Hsinchu County (TW); **Yea-Hsuch Chen**, Taiwan (TW)

(73) Assignee: **Industrial Technology Research Institute**, Hsinchu (TW)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1205 days.

(21) Appl. No.: **12/018,149**

(22) Filed: **Jan. 22, 2008**

(65) **Prior Publication Data**

US 2009/0138724 A1 May 28, 2009

(30) **Foreign Application Priority Data**

Nov. 26, 2007 (TW) ..... 96144798 A

(51) **Int. Cl.**
G06F 21/00 (2006.01)
G06F 7/04 (2006.01)
G06F 15/16 (2006.01)
G06F 17/30 (2006.01)
H04L 29/06 (2006.01)

(52) **U.S. Cl.** **713/186**; 713/182; 713/168; 380/44; 382/115

(58) **Field of Classification Search** 713/182, 713/186, 168; 380/44, 229; 382/115, 116, 382/209; 726/9, 26
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,229,764	A *	7/1993	Matchett et al.	340/5.52
6,901,154	B2 *	5/2005	Dunn	382/115
7,079,007	B2 *	7/2006	Siegel et al.	340/5.52
7,188,362	B2	3/2007	Brandys	
7,693,279	B2 *	4/2010	Chen et al.	380/44
2003/0115473	A1 *	6/2003	Sugimura et al.	713/186
2004/0219902	A1 *	11/2004	Lee et al.	455/410
2005/0154924	A1 *	7/2005	Scheidt et al.	713/202
2005/0210269	A1 *	9/2005	Tiberg	713/186
2007/0192601	A1 *	8/2007	Spain et al.	713/168
2008/0209226	A1 *	8/2008	Venkatesan et al.	713/186

FOREIGN PATENT DOCUMENTS

CN 1373885 10/2002

(Continued)

OTHER PUBLICATIONS

Article titled "Combining cryptography with biometrics effectively" authored by Hao et al., Technical Report (Computer Laboratory) published by the University of Cambridge, No. 640, Jul. 2005 (pp. 1-17).

(Continued)

Primary Examiner — Edan Orgad
Assistant Examiner — Kari Schmidt
(74) *Attorney, Agent, or Firm* — Jianq Chyun IP Office

(57) **ABSTRACT**

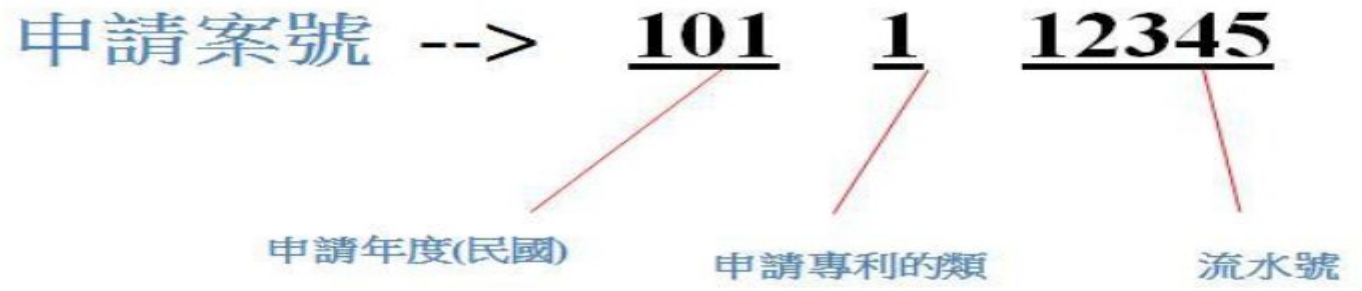
A biometric method, a biometric apparatus, and a biometric data encryption method thereof are disclosed. In the biometric method and the biometric apparatus, a biometric data is quantified to obtain a quantified data. A one-way function is then performed to convert the quantified data into an encrypted data. In the present invention, the biometric data is protected through a cryptography system so as to prevent the biometric features from being stolen or misappropriated. Moreover, in the present invention, a biometric technique can be integrated with a cryptography technique.

5 Claims, 3 Drawing Sheets

專利號碼的種類-公開號

- **公開號**:台灣專利案的公開號共有9碼，前四碼代表西元幾年公開的發明案子，其餘後五碼則為流水序號

專利號碼的種類-申請案號

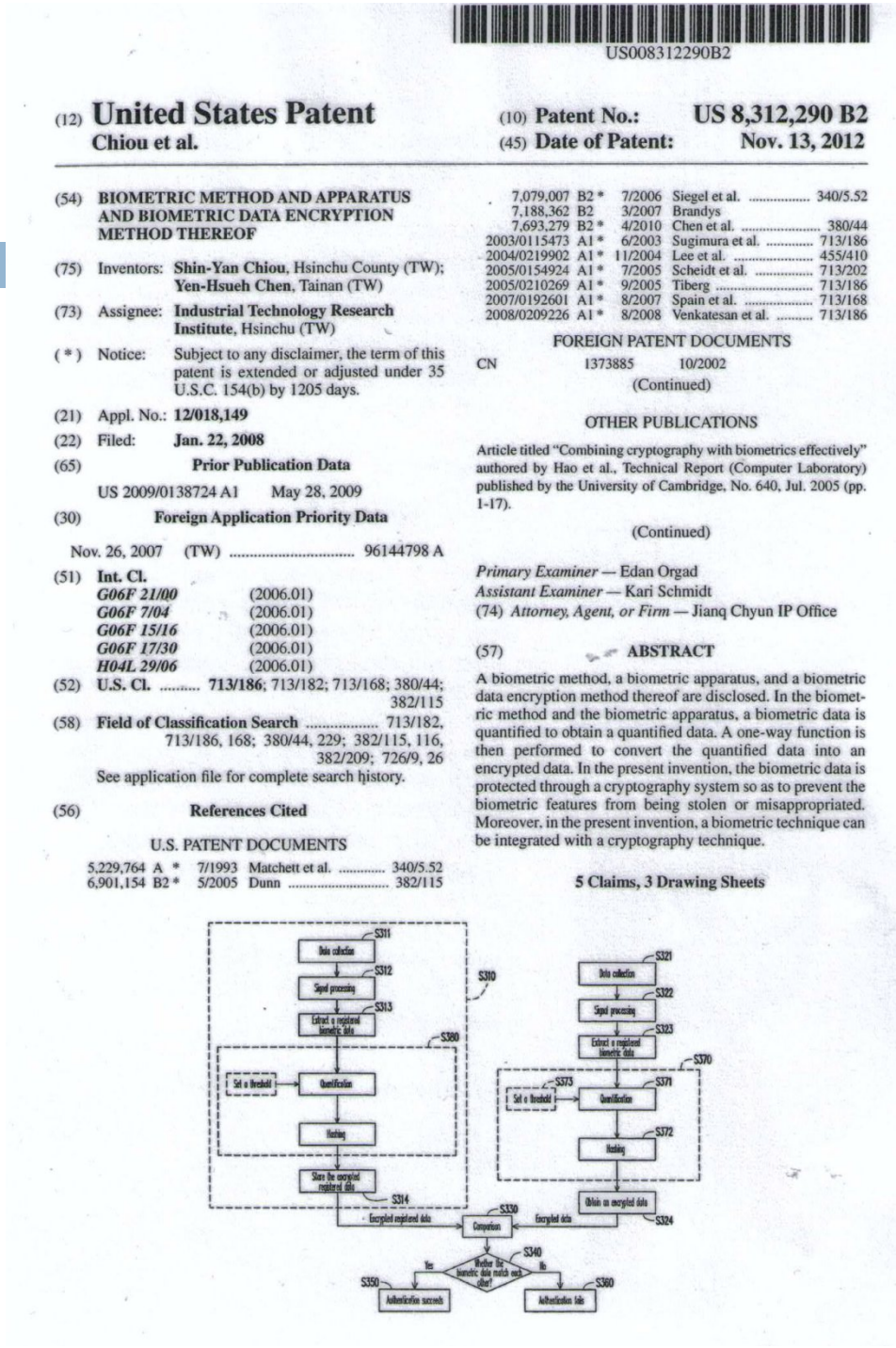


- 台灣專利案的申請案號共有9碼，前三碼代表民國幾年申請的案子，第四碼係為申請專利的類型，其中1:代表發明專利，2:代表新型專利，3:代表設計(新式樣)專利，其餘後五碼則為流水序號

專利首頁資訊

- 獲證號US 8,312,290 B2 前兩碼是國碼(country code)，中間的數字為公開號序號/專利序號，最後即為Kind Code

- 公開號"US 2003/1234567 A1"是美國專利早期公開(A1)第2003/1234567號，並可清楚知道此案公開於西元2003年



US008312290B2

(12) **United States Patent**
Chiou et al.

(10) **Patent No.: US 8,312,290 B2**
(45) **Date of Patent: Nov. 13, 2012**

(54) **BIOMETRIC METHOD AND APPARATUS AND BIOMETRIC DATA ENCRYPTION METHOD THEREOF**

(75) Inventors: **Shin-Yan Chiou**, Hsinchu County (TW); **Yen-Hsueh Chen**, Tainan (TW)

(73) Assignee: **Industrial Technology Research Institute**, Hsinchu (TW)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1205 days.

(21) Appl. No.: **12/018,149**

(22) Filed: **Jan. 22, 2008**

(65) **Prior Publication Data**

US 2009/0138724 A1 May 28, 2009

(30) **Foreign Application Priority Data**

Nov. 26, 2007 (TW) ..... 96144798 A

(51) **Int. Cl.**
G06F 21/00 (2006.01)
G06F 7/04 (2006.01)
G06F 15/16 (2006.01)
G06F 17/30 (2006.01)
H04L 29/06 (2006.01)

(52) **U.S. Cl.** **713/186**; 713/182; 713/168; 380/44; 382/115

(58) **Field of Classification Search** 713/182, 713/186, 168; 380/44, 229; 382/115, 116, 382/209; 726/9, 26

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,229,764 A * 7/1993 Matchett et al. 340/5.52
6,901,154 B2 * 5/2005 Dunn 382/115
7,079,007 B2 * 7/2006 Siegel et al. 340/5.52
7,188,362 B2 3/2007 Brandys
7,693,279 B2 * 4/2010 Chen et al. 380/44
2003/0115473 A1 * 6/2003 Sugimura et al. 713/186
2004/0219902 A1 * 11/2004 Lee et al. 455/410
2005/0154924 A1 * 7/2005 Scheidt et al. 713/202
2005/0210269 A1 * 9/2005 Tiberg 713/186
2007/0192601 A1 * 8/2007 Spain et al. 713/168
2008/0209226 A1 * 8/2008 Venkatesan et al. 713/186

FOREIGN PATENT DOCUMENTS

CN 1373885 10/2002

(Continued)

OTHER PUBLICATIONS

Article titled "Combining cryptography with biometrics effectively" authored by Hao et al., Technical Report (Computer Laboratory) published by the University of Cambridge, No. 640, Jul. 2005 (pp. 1-17).

(Continued)

Primary Examiner — Edan Orgad
Assistant Examiner — Kari Schmidt
(74) *Attorney, Agent, or Firm* — Jianq Chyun IP Office

(57) **ABSTRACT**

A biometric method, a biometric apparatus, and a biometric data encryption method thereof are disclosed. In the biometric method and the biometric apparatus, a biometric data is quantified to obtain a quantified data. A one-way function is then performed to convert the quantified data into an encrypted data. In the present invention, the biometric data is protected through a cryptography system so as to prevent the biometric features from being stolen or misappropriated. Moreover, in the present invention, a biometric technique can be integrated with a cryptography technique.

5 Claims, 3 Drawing Sheets

美國專利類別碼(Kind codes)

- Kind Codes，用來分辨各種專利文件類型

類別碼	說明
A1	早期公開的案子(核准前)
A2	"再公開"的案子，申請人可於修改已申請的說明書後(比如重新撰寫說明書)，要求再公開
A9	更正後的公開案，經過校正過的公開案，可能是USPTO主動要求的修正
B1	沒有早期公開即核准的案子
B2	有早期公開過的專利核准案
C1,2,3	經過"再審(reexamination)"的案子，號碼會跟著B1,B2而變動
E	再領證案，但是沒有任何改變
H	經過專利局註冊公開的案子(SIR)，沒有經過實質審查的
P	經過專利局註冊公開的案子(SIR)，沒有經過實質審查的
S	代表設計專利

專利公開說明書

US 20010000044A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2001/0000044 A1**

Lin (43) **Pub. Date: Mar. 15, 2001**

題目

(54) **SYSTEMS AND METHODS FOR TRANSACTING BUSINESS OVER A GLOBAL COMMUNICATIONS NETWORK SUCH AS THE INTERNET**

發明人

(76) Inventor: **Wayne W Lin**, Irvine, CA (US)

Correspondence Address:
Neal M. Cohen
2424 S.E. Bristol Street, Suite 300
Newport Beach, California CA (US)

申請日

(21) Appl. No.: **09/342,866**

(22) Filed: **Jun. 29, 1999**

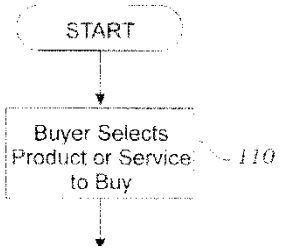
Publication Classification

(51) **Int. Cl.**[7] **G06F 17/60**

(52) **U.S. Cl.** **705/26**; 705/37

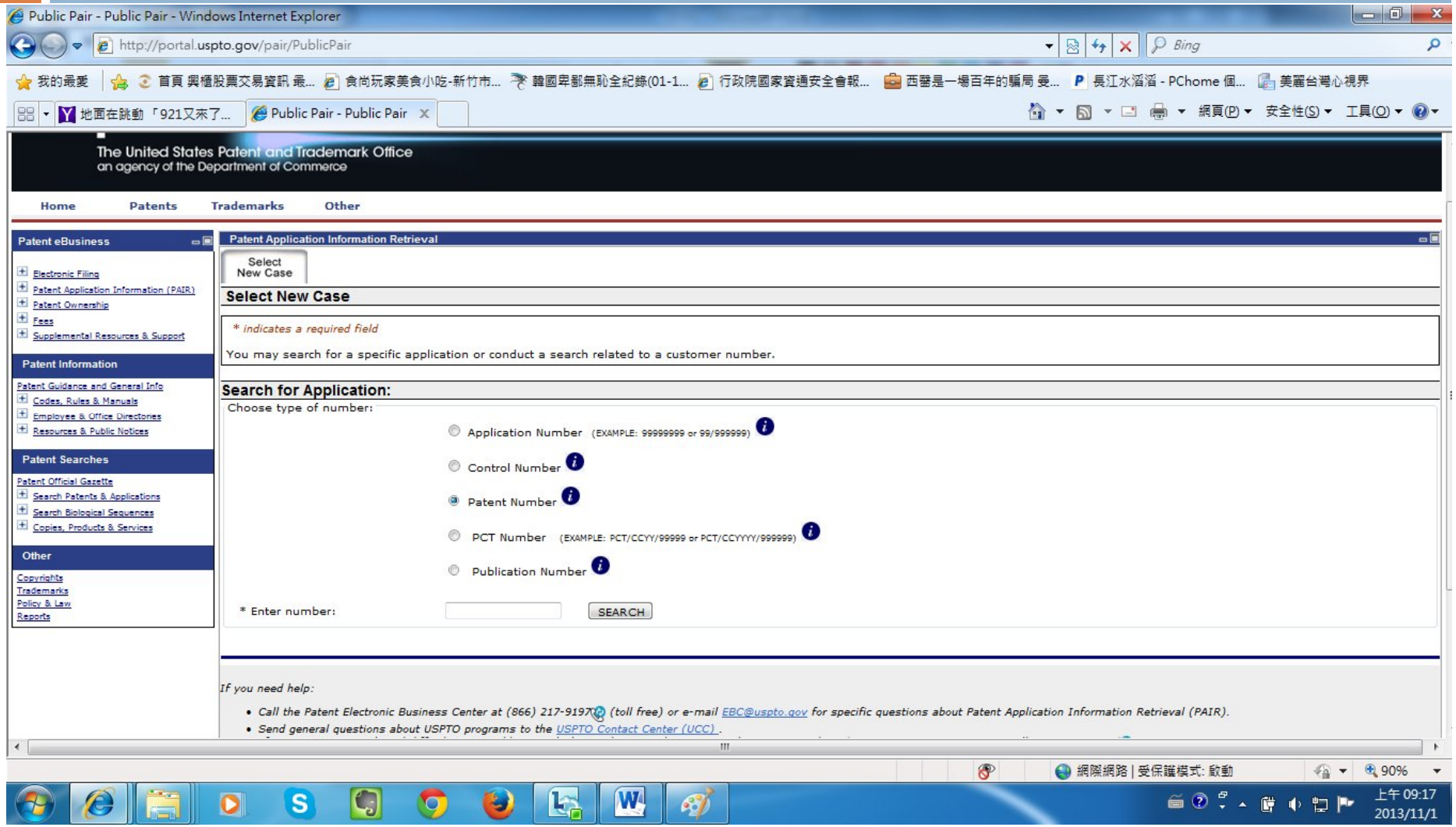
(57) **ABSTRACT**

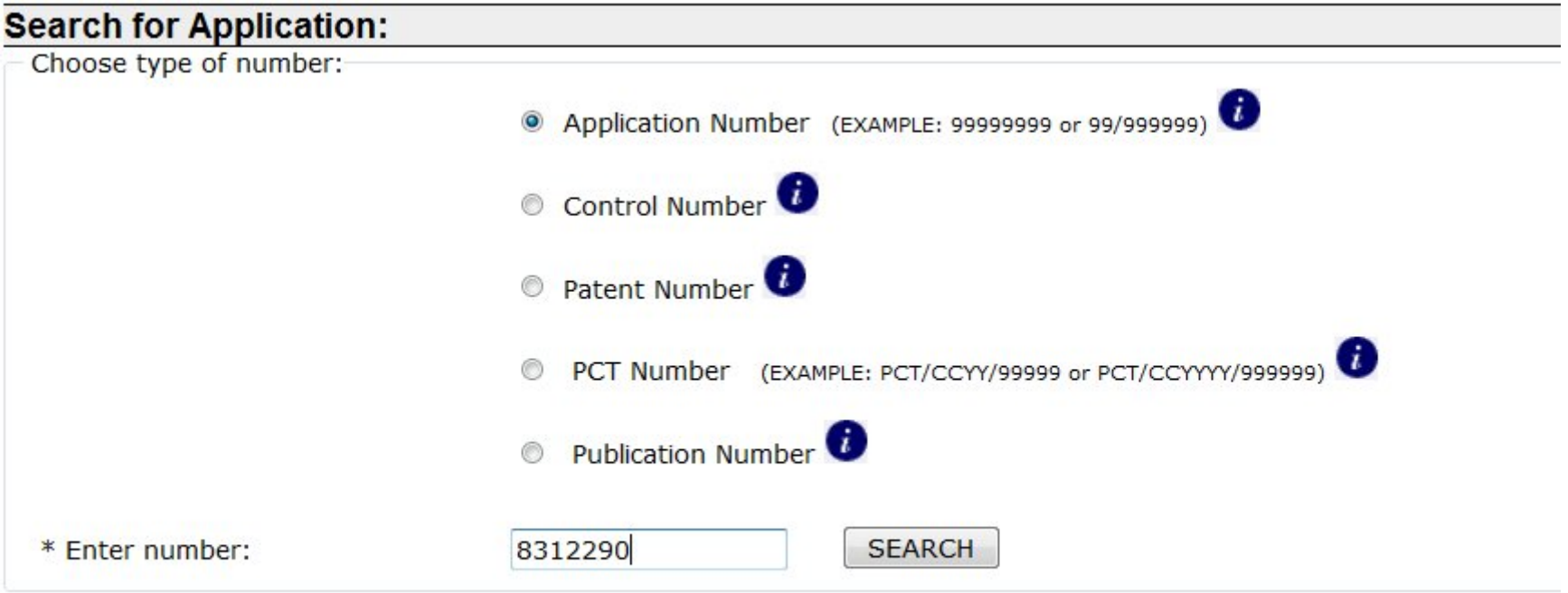
A business model / process is described for conducting business transactions over the Internet, allowing buyers to reduce the price of the selected product / service based on the buyer's performance during a collateral activity. Sellers offer the product / service within a specified price range, and buyers accept the offer, in exchange for the opportunity to close the transaction at the lowest price offered by achieving a high score during the collateral activity. The ultimate price is within the agreed upon range, but is determined based upon the buyer's performance during the collateral activity. The activity may be a video game, electronic board game, sports bet, card game, or any other activity, and may be performed against the seller, a pre-programmed software opponent, a computer opponent, another buyer competing for the same or a different product, a player participating as a player only and not as a buyer, or anyone or anything else.

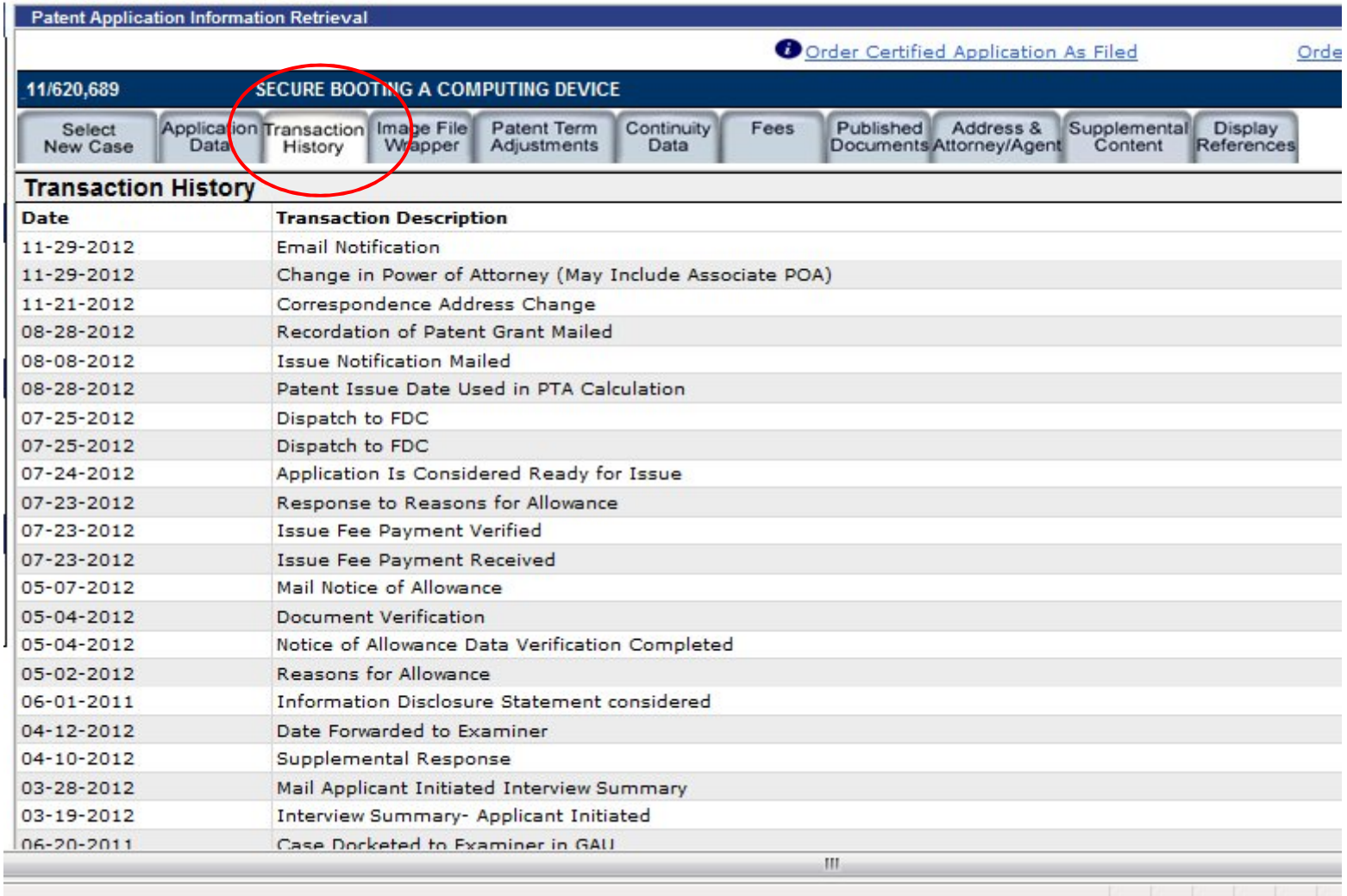


專利溝通歷史

- http://portal.uspto.gov/pair/PublicPair
- Google serach(UPSPO及 Pair)


Public Pair - Public Pair - Windows Internet Explorer
http://portal.uspto.gov/pair/PublicPair
Public Pair - Public Pair
The United States Patent and Trademark Office
an agency of the Department of Commerce
Home
Patents
Trademarks
Other
Patent eBusiness
Electronic Filing
Patent Application Information (PAIR)
Patent Ownership
Fees
Supplemental Resources & Support
Patent Information
Patent Guidance and General Info
Codes, Rules & Manuals
Employee & Office Directories
Resources & Public Notices
Patent Searches
Patent Official Gazette
Search Patents & Applications
Search Biological Sequences
Copies, Products & Services
Other
Copyrights
Trademarks
Policy & Law
Reports
Patent Application Information Retrieval
Select New Case
Select New Case
* indicates a required field
You may search for a specific application or conduct a search related to a customer number.
Search for Application:
Choose type of number:
Application Number (EXAMPLE: 99999999 or 99/999999)
Control Number
Patent Number
PCT Number (EXAMPLE: PCT/CCYY/99999 or PCT/CCYYYY/999999)
Publication Number
* Enter number:
SEARCH
If you need help:
Call the Patent Electronic Business Center at (866) 217-9197 (toll free) or e-mail EBC@uspto.gov for specific questions about Patent Application Information Retrieval (PAIR).
Send general questions about USPTO programs to the USPTO Contact Center (UCC).
網際網路 | 受保護模式: 啟動
90%
上午 09:17
2013/11/1


Search for Application:
Choose type of number:
Application Number (EXAMPLE: 99999999 or 99/999999)
Control Number
Patent Number
PCT Number (EXAMPLE: PCT/CCYY/99999 or PCT/CCYYYY/999999)
Publication Number
* Enter number:
8312290
SEARCH



Patent Application Information Retrieval

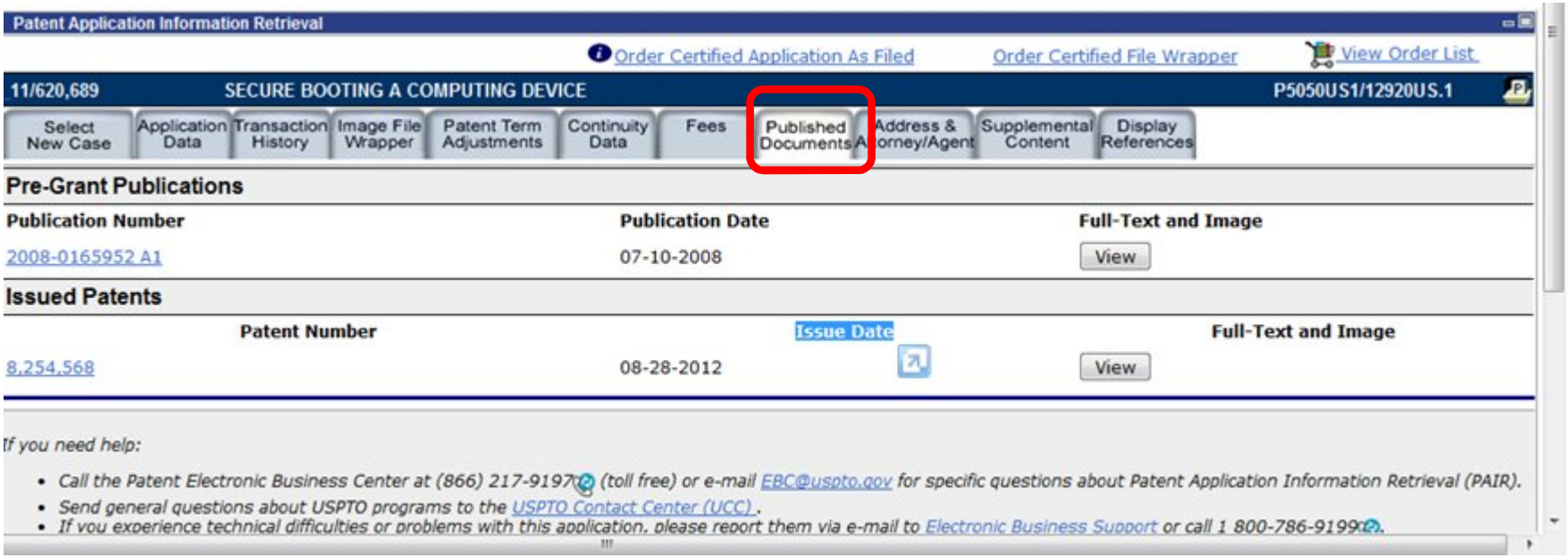
Order Certified Application As Filed Orde

11/620,689 SECURE BOOTING A COMPUTING DEVICE

Select New Case | Application Data | Transaction History | Image File Wrapper | Patent Term Adjustments | Continuity Data | Fees | Published Documents | Address & Attorney/Agent | Supplemental Content | Display References

Transaction History

Date	Transaction Description
11-29-2012	Email Notification
11-29-2012	Change in Power of Attorney (May Include Associate POA)
11-21-2012	Correspondence Address Change
08-28-2012	Recordation of Patent Grant Mailed
08-08-2012	Issue Notification Mailed
08-28-2012	Patent Issue Date Used in PTA Calculation
07-25-2012	Dispatch to FDC
07-25-2012	Dispatch to FDC
07-24-2012	Application Is Considered Ready for Issue
07-23-2012	Response to Reasons for Allowance
07-23-2012	Issue Fee Payment Verified
07-23-2012	Issue Fee Payment Received
05-07-2012	Mail Notice of Allowance
05-04-2012	Document Verification
05-04-2012	Notice of Allowance Data Verification Completed
05-02-2012	Reasons for Allowance
06-01-2011	Information Disclosure Statement considered
04-12-2012	Date Forwarded to Examiner
04-10-2012	Supplemental Response
03-28-2012	Mail Applicant Initiated Interview Summary
03-19-2012	Interview Summary- Applicant Initiated
06-20-2011	Case Docketed to Examiner in GAU


Patent Application Information Retrieval
Order Certified Application As Filed
Order Certified File Wrapper
View Order List
11/620,689
SECURE BOOTING A COMPUTING DEVICE
P5050US1/12920US.1
Select New Case
Application Data
Transaction History
Image File Wrapper
Patent Term Adjustments
Continuity Data
Fees
Published Documents
Address & Attorney/Agent
Supplemental Content
Display References
Pre-Grant Publications
Publication Number
Publication Date
Full-Text and Image
2008-0165952 A1
07-10-2008
View
Issued Patents
Patent Number
Issue Date
Full-Text and Image
8,254,568
08-28-2012
View
If you need help:
Call the Patent Electronic Business Center at (866) 217-9197 (toll free) or e-mail EBC@uspto.gov for specific questions about Patent Application Information Retrieval (PAIR).
Send general questions about USPTO programs to the USPTO Contact Center (UCC).
If you experience technical difficulties or problems with this application, please report them via e-mail to Electronic Business Support or call 1 800-786-9199.

05-07-2012	FWCLM	Index of Claims	PROSECUTION	2	
04-10-2012	SA..	Supplemental Response or Supplemental Amendment	PROSECUTION	1	
04-10-2012	CLM	Claims	PROSECUTION	8	
04-10-2012	REM	Applicant Arguments/Remarks Made in an Amendment	PROSECUTION	1	
04-10-2012	N417	EFS Acknowledgment Receipt	PROSECUTION	2	
04-10-2012	WFEE	Fee Worksheet (SB06)	PROSECUTION	1	
03-28-2012	INTV.SUM.APP	Applicant Initiated Interview Summary (PTOL-413)	PROSECUTION	3	
06-01-2011	RCEX	Request for Continued Examination (RCE)	PROSECUTION	3	
06-01-2011	AMSB	Amendment Submitted/Entered with Filing of CPA/RCE	PROSECUTION	1	
06-01-2011	CLM	Claims	PROSECUTION	12	
06-01-2011	REM	Applicant Arguments/Remarks Made in an Amendment	PROSECUTION	9	
06-01-2011	TRAN.LET	Transmittal Letter	PROSECUTION	2	
06-01-2011	IDS	Information Disclosure Statement (IDS) Form (SB08)	PROSECUTION	1	
06-01-2011	FOR	Foreign Reference	PRIOR ART	19	
06-01-2011	WFEE	Fee Worksheet (SB06)	PROSECUTION	2	
06-01-2011	N417	EFS Acknowledgment Receipt	PROSECUTION	3	
06-01-2011	WFEE	Fee Worksheet (SB06)	PROSECUTION	1	
05-05-2011	EXIN	Examiner Interview Summary Record (PTOL - 413)	PROSECUTION	3	
03-01-2011	CTFR	Final Rejection	PROSECUTION	74	
03-01-2011	892	List of references cited by examiner	PRIOR ART	1	
03-01-2011	SRNT	Examiner's search strategy and results	PROSECUTION	3	
03-01-2011	FWCLM	Index of Claims	PROSECUTION	1	
03-01-2011	SRFW	Search information including classification, databases and other search related notes	PROSECUTION	2	
03-01-2011	1449	List of References cited by applicant and considered by examiner	PRIOR ART	1	
03-01-2011	1449	List of References cited by applicant and considered by examiner	PRIOR ART	1	
02-15-2011	SRNT	Examiner's search strategy and results	PROSECUTION	1	

[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06F 9/30
G06F 9/312

[12] 发明专利申请公开说明书

[21] 申请号 03142392.2

[43] 公开日 2004 年 12 月 8 日

[11] 公开号 CN 1553315A

[22] 申请日 2003.6.6 [21] 申请号 03142392.2

[71] 申请人 微软公司
地址 美国华盛顿州
[72] 发明人 D·莫兰斯 J·兰格 D·西蒙
陈 陵 J·D·贝纳勒

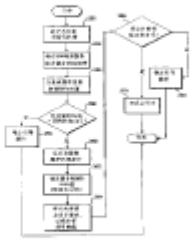
[74] 专利代理机构 上海专利商标事务所
代理人 李家麟

权利要求书 5 页 说明书 9 页 附图 3 页

[54] 发明名称 在安全引导装载程序中使用散列技术

[57] 摘要

包括引导程序代码的机器指令被埋在电子游戏控制台的一个关键部件内，在那里，这些机器指令不容易被使用或修改。引导程序代码对只读存储器(ROM)中的预装载程序部分实施散列技术，将结果与引导程序代码中所保存的预期的散列值进行比较。预装载程序进一步验证引导过程，这对 ROM 中的代码实施散列技术，以便为代码获得一个散列值。按照为这个散列码定义预期值的数字签名值来验证结果。若无法获得任何预期的结果，则终止引导过程。由于引导程序代码确认预装载程序，并且预装载程序确认 ROM 中的代码的剩余部分，因此，该技术可用来确保，用于引导设备的代码还没有被修改或取代。



ISSN1008-4274

知识产权出版社出版

專利、文獻等前案搜尋

- 搜尋已核准之專利或是公開資料
- 經濟部智慧財產局
  - http://twpat3.tipo.gov.tw/tipotwoc/tipotwkm?000FECAE000000000000000000000A00000001E000000000
- Google patent
  - https://www.google.com/?tbm=pts
- USPTO
  - http://patft.uspto.gov/netahtml/PTO/search-bool.html(Abtrsact)
  - http://patft.uspto.gov/netahtml/PTO/patimg.htm(PDF檔)
- IEEE (論文)
  - http://ieeexplore.ieee.org/Xplore/home.jsp

專利文獻著錄項目代碼

(Internationally agreed Numbers for the Identification of (bibliographic) Data, INID)

〔10〕文件標誌
- 〔11〕文件編號(如申請號、公開號、公告號)
- 〔12〕文件類別
- 〔19〕國別

〔20〕本國登記項目
- 〔21〕申請號
- 〔22〕申請日

〔30〕國際優先權
- 〔31〕優先權申請號
- 〔32〕優先權申請日
- 〔33〕優先權申請國家

〔40〕提交公眾審查應用日期
- 〔43〕未授權專利文獻公佈日期
- 〔45〕已授權專利文獻公佈日期

〔50〕技術情報項目
- 〔51〕國際專利分類號
- 〔52〕本國專利分類號
- 〔54〕發明名稱
- 〔55〕主題詞(關鑑字)
- 〔56〕引用文獻
- 〔57〕摘要或申請專利範圍
- 〔58〕檢索範圍

〔60〕與申請有關之法律文件

〔70〕人事項目
- 〔71〕申請人
- 〔72〕發明人
- 〔73〕受讓人
- 〔74〕代理人
- 〔75〕發明人兼申請人
- 〔76〕發明人兼申請人及受讓人

〔81〕國際申請指定國

〔82〕選擇國

〔84〕歐洲專利指定國

US008312290B2

(12) **United States Patent**
Chiou et al.

(10) **Patent No.: US 8,312,290 B2**
(45) **Date of Patent: Nov. 13, 2012**

(54) **BIOMETRIC METHOD AND APPARATUS AND BIOMETRIC DATA ENCRYPTION METHOD THEREOF**

(75) Inventors: **Shin-Yan Chiou**, Hsinchu County (TW); **Yen-Hsueh Chen**, Tainan (TW)

(73) Assignee: **Industrial Technology Research Institute**, Hsinchu (TW)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1205 days.

(21) Appl. No.: **12/018,149**

(22) Filed: **Jan. 22, 2008**

(65) **Prior Publication Data**

US 2009/0138724 A1 May 28, 2009

(30) **Foreign Application Priority Data**

Nov. 26, 2007 (TW) ..... 96144798 A

(51) **Int. Cl.**
G06F 21/00 (2006.01)
G06F 7/04 (2006.01)
G06F 15/16 (2006.01)
G06F 17/30 (2006.01)
H04L 29/06 (2006.01)

(52) **U.S. Cl.** **713/186**; 713/182; 713/168; 380/44; 382/115

(58) **Field of Classification Search** 713/182, 713/186, 168; 380/44, 229; 382/115, 116, 382/209; 726/9, 26

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,229,764	A *	7/1993	Matchett et al.	340/5.52
6,901,154	B2 *	5/2005	Dunn	382/115
7,079,007	B2 *	7/2006	Siegel et al.	340/5.52
7,188,362	B2	3/2007	Brandys	
7,693,279	B2 *	4/2010	Chen et al.	380/44
2003/0115473	A1 *	6/2003	Sugimura et al.	713/186
2004/0219902	A1 *	11/2004	Lee et al.	455/410
2005/0154924	A1 *	7/2005	Scheidt et al.	713/202
2005/0210269	A1 *	9/2005	Tiberg	713/186
2007/0192601	A1 *	8/2007	Spain et al.	713/168
2008/0209226	A1 *	8/2008	Venkatesan et al.	713/186

FOREIGN PATENT DOCUMENTS

CN 1373885 10/2002

(Continued)

OTHER PUBLICATIONS

Article titled "Combining cryptography with biometrics effectively" authored by Hao et al., Technical Report (Computer Laboratory) published by the University of Cambridge, No. 640, Jul. 2005 (pp. 1-17).

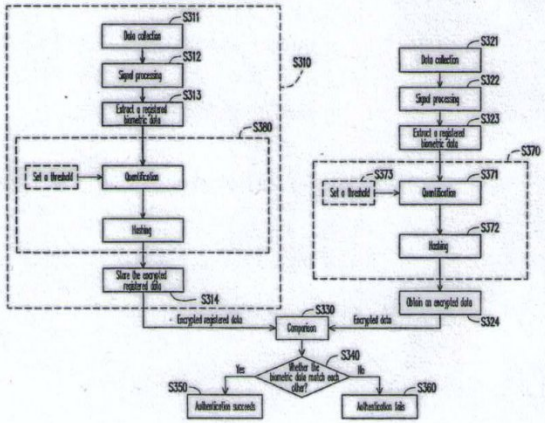
(Continued)

Primary Examiner — Edan Orgad
Assistant Examiner — Kari Schmidt
(74) *Attorney, Agent, or Firm* — Jianq Chyun IP Office

(57) **ABSTRACT**

A biometric method, a biometric apparatus, and a biometric data encryption method thereof are disclosed. In the biometric method and the biometric apparatus, a biometric data is quantified to obtain a quantified data. A one-way function is then performed to convert the quantified data into an encrypted data. In the present invention, the biometric data is protected through a cryptography system so as to prevent the biometric features from being stolen or misappropriated. Moreover, in the present invention, a biometric technique can be integrated with a cryptography technique.

5 Claims, 3 Drawing Sheets



專利申請案例簡介-
數位版權管理物件的加密方法

專利申請思考及先前案例搜尋分析參考範例

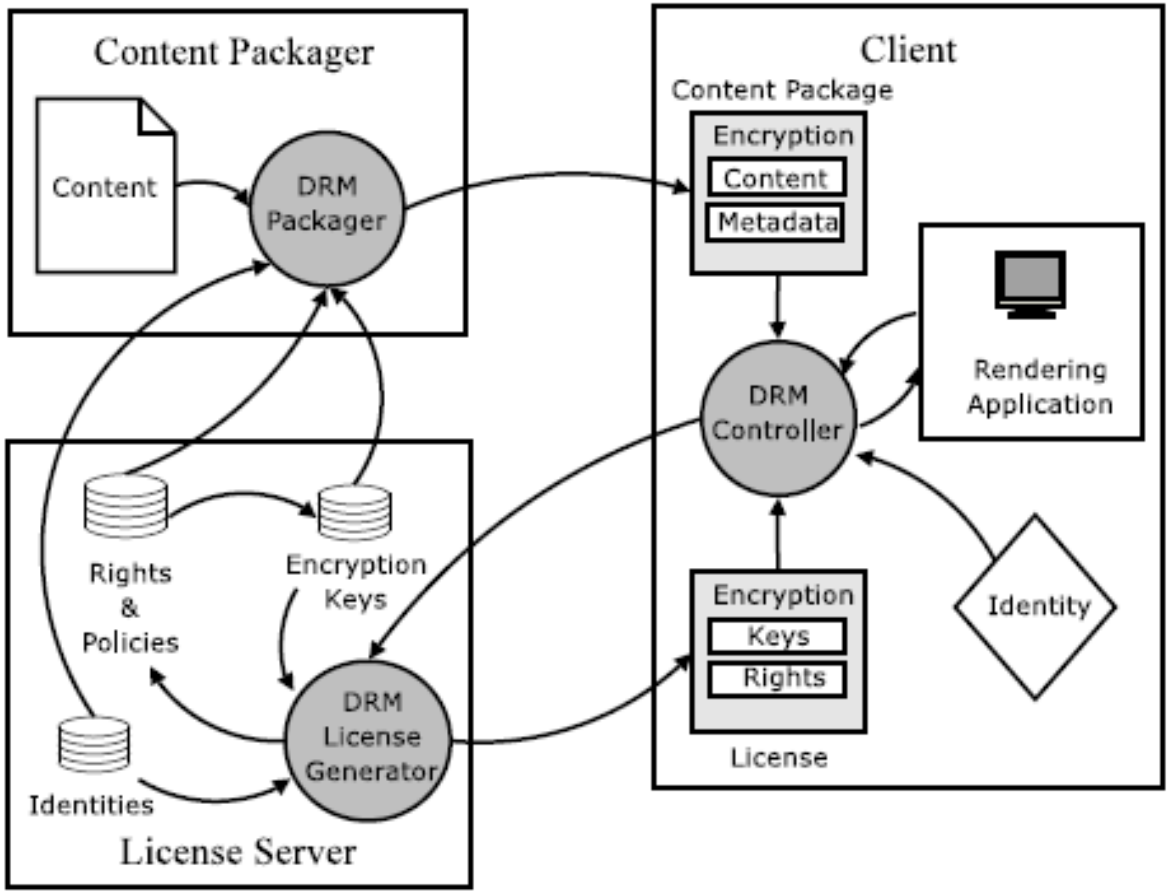
Outline

- 背景與動機
- 本案提出之方法
- 本案特點
- 前案比較
- 專利範圍
- 侵權認定
- 附錄

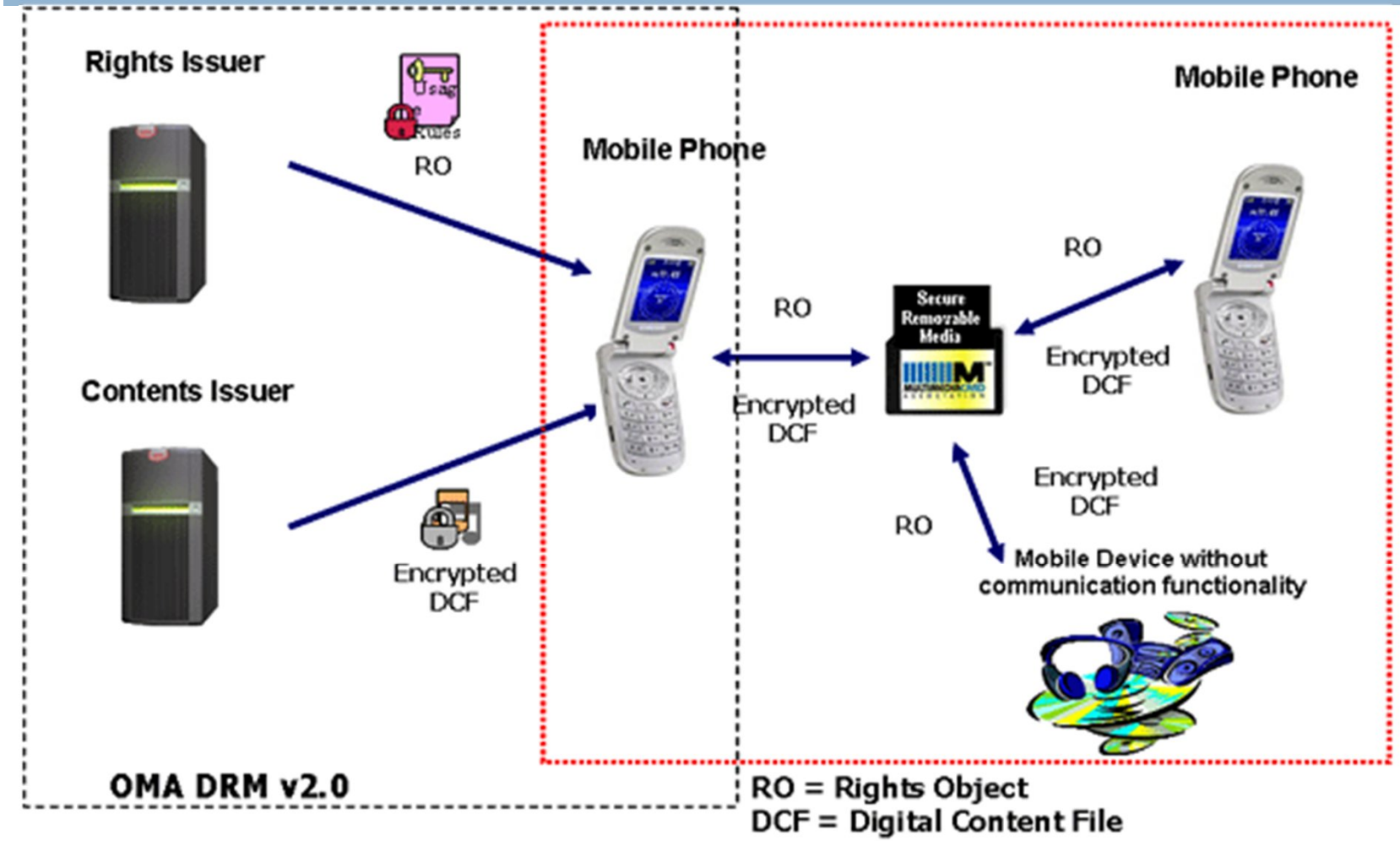
背景與動機-1

- 數位版權管理(DRM)中保護方式
  - 一份完整的content，單獨或與其他content置於一個獨立的加密檔案中(Encrypted DCF)
    - 使用一份content，需要解Encrypted DCF
  - 加密檔案可使用在註冊同一領域中(Domain)的所有裝置(one domain-one user)
  - Domain中的使用情形，需要回傳資訊至server方能進一步管理

背景與動機-2
DRM System



背景與動機-3
Domain Scenario



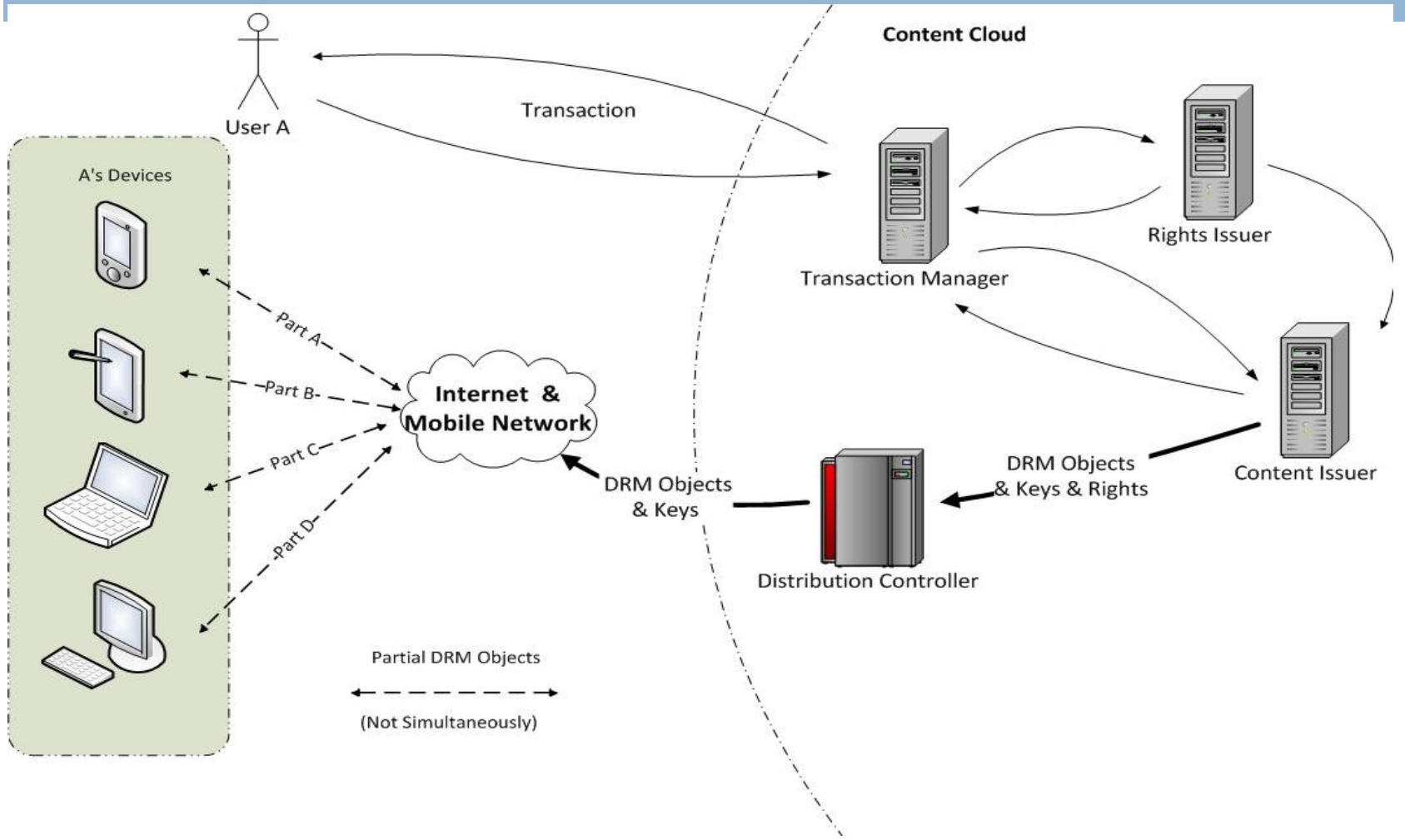
背景與動機-4

- 應用上遭遇的問題：
  1. 每次接收/解密一個content→ 需解開一完整的DCF，對系統資源的需求大
  2. Domain中的裝置可任意使用與傳遞→ 多使用者共存於一個Domain中形成multi-user with multi-device in a domain，則原本DRM系統的設計無法管理
  3. Domain中DRM檔案於任一裝置被破解→ 所有在此Domain中的裝置及content均失效

本案提出之方法-1

- 定義DRM系統中之文件(Content)依照內文的格式與文意架構等，分隔為多個區段(segment)，每一區段為一單獨之內文物件並加入適當關聯與版權相關資訊後，包裝為一個版權管理物件(DRM Object)
  - ITRI前案已提出以DRM Object為基礎之觀念與管理遞送之模式但前頁所述問題亦可用另一機制解決(加密機制)
  - 加入裝置或交易中之特定資訊進行保護，在不額外影響效能情況下，使前案與本案所提之DRM Object對裝置之遞送管理，能有對裝置之獨特性(具備特定資訊)，可在Server端即具備版權管理之能力，而實現雲端的DRM架構

本案提出之方法-2


Content Cloud
User A
Transaction
A's Devices
Transaction Manager
Rights Issuer
Content Issuer
Part A
Part B
Part C
Part D
Internet &
Mobile Network
DRM Objects
& Keys
DRM Objects
& Keys & Rights
Distribution Controller
Partial DRM Objects
(Not Simultaneously)

本案提出之方法-3

- Content Segmentation

  --數位內容分割為多個物件(content object)，在傳遞時以物件為單位(DRM Object)

- Distinguished DRM Object Delivery

  --DRM Object 在包裝加密時，加入額外資訊(DRM Vector)，其中包含使用資訊(如時間戳記、使用者資訊等)、物件關聯資訊以及與裝置相關之資訊，交易時間與紀錄等，對content包裝成DRM Object並傳遞到對應的裝置中

- User Exclusive and User-Device Identification Mechanism

  --物件傳遞的對應關係是DRM Object to "User-Device"亦即使用者與裝置，DRM Object亦不可在不同裝置間流通

本案特點-1
創新部份

- Content Segmentation

  --數位內容分割為多個物件(content object)，在傳遞時以物件為單位(DRM Object)，DRM Object之遞送與保護即為實現DRM系統相關權限的方式

- Distinguished DRM Object Delivery

  --DRM Object 在包裝加密時，加入額外資訊(DRM Vector)，其中包含使用資訊(如時間戳記、使用者資訊等)、物件關聯資訊以及與裝置相關之資訊，交易時間與紀錄等，對content包裝成DRM Object並傳遞到對應的裝置中，DRM Vector對每一DRM Object均不同，具有唯一性(應用於AES加密中取代IV時，可增加安全性)

- User Exclusive and User-Device Identification Mechanism

  --物件傳遞的對應關係是Object to User-Device 亦即物件同時與使用者與裝置間有關聯，DRM Object不可在不同裝置間流通

本案特點-2
優點與所解決之問題

- **唯一使用者機制**
  - Distinguished DRM Object Delivery + User Exclusive and User-Device Identification Mechanism
- **領域內裝置數位內容共用問題**
  - Distinguished DRM Object Delivery + User Exclusive and User-Device Identification Mechanism
- **減少裝置容量需求**
  - Content Segmentation
- **增進安全性**
  - Distinguished DRM Object Delivery + User Exclusive and User-Device Identification Mechanism
- **改善效能**
  - Content Segmentation

相關專利與論文檢索 -1

- 檢索策略：
  - 關鍵字：
    - “drm encryption ”
    - ”data loss protection encryption ”
    - “e-book ”and “encryption ”
  - 檢索資料庫：
    - IEEE XPLORE（http://ieeexplore.ieee.org）
    - USPTO（http://www.uspto.gov/ ）
    - 中華民國專利資訊檢索系統（http://www.tipo.gov.tw ）

相關專利與論文檢索 -2

- 論文關鍵字搜尋(2010/08/23前)
  - 關鍵字 “drm encryption”→96項，其中4項有關
  - 關鍵字 ”data loss protection encryption”→26項，1項有關
  - 關鍵字 “ “e-book ”and “encryption”→1項，0項有關
- 美國專利關鍵字搜尋已公告專利 (2010/08/23前)
  - 關鍵字 “drm encryption”→12項，其中5項有關
  - 關鍵字 ”data loss protection encryption”→0項
  - 關鍵字 “e-book ”and “encryption”→0項
- 美國專利關鍵字搜尋已公開專利 (2010/08/23前)
  - 關鍵字 “drm encryption”→47項，其中4項有關
  - 關鍵字 ”data loss protection encryption”→0項
  - 關鍵字 “e-book ”and “encryption”→0項
- 中華民國專利關鍵字搜尋(2010/08/23前)
  - 關鍵字 “drm encryption”→70項，2項有關。
  - 關鍵字 ”data loss protection encryption”→0項
  - 關鍵字 “ “e-book ”and “encryption”→0項，

相關專利與論文檢索 -3

- 論文部分
  - ”An Efficient Key Distribution Method Applying to OMA DRM 2.0 with Device Identifier ,” Sep,2008.
    - 此論文主要主要提出用Device Identifier當對稱式加密的金論來取代原來DRM系統的非對稱式加密演算法，與本專利目的類似但本專利使用物件取用順序來當加密金鑰的方法不相同
  - ”Extending an OMA-based DRM framework with non-repudiation services ”, Dec. 2005
    - 此論文主要提出在DRM系統內容可以自由傳遞，但權力物件卻不具有不可否認性，因此延伸現有的DRM架構使其具有不可否認性服務，其目的與方法與本案不相同

相關專利與論文檢索 -4

- ”A New DRM System Based on Graded Contents Sharing and Time-Block Distribution for Home Networks ”, July, 2007
  - 此論文設計一系統，對於content以固定size的block來進行加解密，並達成收費計價的計算(用多少比例收多少)，其中加解密的key的等級也依照內容的價值性來衡量
  - 本發明案主張依照content文意或使用習慣來進行文件段落的分割，並以部份傳遞的機制來追蹤文件的使用與管理，與此篇論文的作法及目標均不相同
- ”Design of Secure Issue System for Part Page of E-Document in Certified Electronic Document Authority ”, Nov. 2009
  - 論文設計之系統為如何將一份文件拆成多個分頁來傳給不同使用者的議題，透過一個一次性金鑰和每個分頁的分頁金鑰和認證伺服器來達成，其闡述之主要目的均與本案類似但是方法不同

相關專利與論文檢索 -5

- ”Design and Development of PDF Document Protection System Based on DRM Technology ”, Dec, 2009
  - 此論文之目的為開發Plug-in來將PDF加入DRM功能，其處理方式為將出版者將PDF單純加密，並加入權限資訊，而當使用者開啟文件時Plug-in將連線到授權伺服器驗證，加密的方法為單純將整份文件加密，其目的與作法與本案不同

- 美國已公告專利
  - Method for obtaining a black box for performing decryption and encryption functions in a digital rights management (DRM) system, US 7051005, Nov, 2010
    - 目的不同，此專利目的在於闡述如何在一DRM運算裝置，如何透過非對稱金鑰的方式，從黑盒子伺服器中取得黑盒子並安裝在DRM運算裝置中
    - 此專利中將權力物件寫成黑盒子，其加密方法是透過非對稱金鑰的方式，和本專利利用物件取得順序關係加密的方式，無論在目的與方法皆不相同

相關專利與論文檢索 -6

- Method and system for digital rights management brokering and digital asset security transcoding, US 7822685, October , 2010
  - 目的類似，此專利目的在於闡述DRM系統中，利用一個代理人來將一份數位內容文件的格式做轉換和切割成多份的數位內容文件，並透過此代理人利用加密金鑰的方式來對數位內容保護和追蹤
  - 而本專利強調的是利用物件的取用順序來達到數位內容的保護和追蹤，目的類似但方法不一樣
- Content encryption schema for integrating digital rights management with encrypted multicast, US 7978848, July, 2011
  - 此專利中提到利用加入一個整合加密金鑰架構到DRM中的數位內容金鑰中來做到DRM廣播加密系統，與本專利之目的與作法均不相同

相關專利與論文檢索 -7

- Content distribution for multiple digital rights management, US 7120250, Oct, 2006
  - 此專利中提到多個content provider在DRM系統中(或多個DRM)，要如何整合傳遞client給一個群組，其中亦提到segment，但其segment為組合多個DRM的文件傳遞，如何與device端的解碼元件配合，順利解出需求之DRM content，與本專利之目的與作法均不相同
- System and method for processing DRM-enabled files, US 7748044, June, 2010
  - 此專利中有兩把加密金鑰第一加密金鑰和第二加密金鑰，將第一加密金鑰加密過的數位內容下載到電腦中，接著在電腦中用第一加密金鑰解開並轉換，然後用第二加密金鑰加密接著下載到撥放裝置中，與本專利之目的與作法均不相同

相關專利與論文檢索 -8

- 美國已公開專利
  - Process and apparatus for securing and retrieving digital data with a Portable Data Storage Device (PDSD) and Playback Device (PD), 20080279533, Nov, 2008
    - 此專利目的透過將數位內容物件下載到可攜式存儲裝置(PDSD)中，然後播放裝置(PD)從PDSD中取得加密的數位內容，解密之後撥放，其中DRM中相關的加密金鑰，透過PDSD的私密金鑰加密儲存在PDSD中，目的與方法皆和本案不相同
  - DIGITAL RIGHTS MANAGEMENT METHOD FOR TERMINAL, 20080163378, July , 2008
    - 此專利為在客戶裝置中針對權力物件的管理流程，每次下載數位內容物件到客戶裝置中時，檢查其是否之前已經有此數位內容物件對應的權力物件，如有則將其權力物件的計數加一，並改變其時間標記
    - 本專利強調的是利用物件的取用順序來達到數位內容的保護和追蹤，目的和方法皆不一樣

相關專利與論文檢索 -9

- Method to protect digital data using the open mobile alliance digital rights management standard, 20070174197, July, 2007
  - 此專利在現有OMA DRM架構中，加入一個使用者ID，當傳遞數位內容物件到客戶裝置中時，同時傳遞使用者ID到客戶裝置中，並在權力物件中加入此使用者ID，而當要解密數位內容物件前，將權力物件中的使用者ID和之前傳遞的使用者ID比對，一樣時才解密數位內容物件，與本專利之目的與作法均不相同
- Apparatus and method for sending and receiving digital rights objects in converted format between device and portable storage, 20050267845, December, 2005
  - 此專利中在客戶裝置中將權力物件轉換格式成可移轉的權力物件並儲存在記憶卡中，而將此記憶卡移到另一客戶裝置時，可以使用這可移轉的權力物件播放數位內容，與本專利之目的與作法均不相同

相關專利與論文檢索 -10

中華民國專利

- ARCHITECTURE AND METHOD OF MULTILAYERED DRM PROTECTION FOR MULTIMEDIA SERVICE, TW I256212, June, 2006
  - 此專利包含一多層次DRM加密結構和一多層次DRM解密結構。將輸入的多媒體服務經由多媒體服務分解單元和多層次DRM組織單元，來產生經加密的多媒體服務資料串流，與本專利之目的與作法均不相同
- METHOD FOR SHARING RIGHTS OBJECTS BETWEEN USERS, TW I244313, Nov , 2005
  - 此專利為一種可將與內容相關的一使用者的版權物件的全部或部分傳送至其他使用者之方法。該方法包括下列步驟：在第一使用者所握有的版權物件的限制範圍之內，產生一個即將傳送給第二使用者的版權物件；以及將所產生的版權物件，傳送給第二使用者。該方法不需經過伺服器驗證，即可允許每一使用者在版權物件的限制範圍之內，與其他使用者分享其版權物件，與本專利之目的與作法均不相同

論文前案比較 -1

- An Efficient Key Distribution Method Applying to OMA DRM 2.0 with Device Identifier ", Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing on Ninth ACIS International Conference ,pp 3~7, Sep,2008.
  - 此論文主要主要提出用Device Identifier當對稱式加密的金論來取代原來DRM系統的非對稱式加密演算法，與本專利目的類似但本專利使用物件取用順序來當加密金鑰的方法不相同

論文前案比較 -2

- ”A New DRM System Based on Graded Contents Sharing and Time-Block Distribution for Home Networks ”, 6th IEEE/ACIS International Conference on Computer and Information Science, pp. 830~833, July, 2007.
  - 此論文設計一系統，對於content以固定size的block來進行加解密，並達成收費計價的計算(用多少比例收多少)，其中加解密的key的等級也依照內容的價值性來衡量
  - 本發明案主張依照content文意或使用習慣來進行文件段落的分割，並以部份傳遞的機制來追蹤文件的使用與管理，與此篇論文的作法及目標均不相同

論文前案比較 -3

- ”Design of Secure Issue System for Part Page of E-Document in Certified Electronic Document Authority ”, Fourth International Conference on Computer Sciences and Convergence Information Technology, pp 1052 ~ 1056, Nov. 2009
  - 此論文設計之系統為如何將一份文件拆成多個分頁來傳給不同使用者的議題，透過一個一次性金鑰和每個分頁的分頁金鑰和認證伺服器來達成，其闡述之主要目的均與本案類似但是方法不同

專利前案比較-1
外部檢索案

專利編號	公開/公告日期	名稱	比較
US 20100281262	2010.11.04	Method for Digital Rights Management in a Mobile Communications Network	其認證向量Vector之產生與使用方式與本案不同
US 7222232	2007.05.22	License-based cryptographic technique particularly suited for use in a digital rights management system for controlling access and use of bore resistant software objects in a client computer	其權限向量Rights Vector之產生與使用方式與本案不同 Rights Vector為client向server取用資料之權限

專利前案比較-2
外部檢索案

專利編號	公開/公告日期	名稱	比較
TW 200746830	2007.12.16	輸入具有多個部份的內容的方法及其裝置 METHOD AND APPARATUS FOR IMPORTING CONTENT HAVING PLURALITY OF PARTS	其描述為多個content共存於一個檔案時，如何進行權限管理與關聯，目的與方式均與本案不同
TW 200535591	2005.11.01	內容項目之多用戶條件存取 MULTI-USER CONDITIONAL ACCESS TO A CONTENT ITEM	描述多用戶對數個內容存取的權限控管，目的與方式均與本案不同

外部檢索案

- 第三方外部檢索
  - 與工研院合作之專利事務所有利害關係
  - 透過非合作的第三方提供最客觀的資訊，檢索相關專利前案
  - 讓專利申請比較順利
    - 答辯次數(時間、成本、…)
    - 通過的可能性(專利前案搜尋)

專利前案比較-3

專利編號	公開/公告日期	名稱	比較
US 7822685	October , 2010	Method and system for digital rights management brokering and digital asset security transcoding	利用一個代理人來將一份數位內容文件的格式做轉換和切割成多份的數位內容文件，並利用加密金鑰對數位內容保護和追蹤
US 7978848	July,2011	Content encryption schema for integrating digital rights management with encrypted multicast	利用加入一個整合加密金鑰架構到DRM中的數位內容金鑰中來做到DRM廣播加密系統
US 20080163378	July,2008	DIGITAL RIGHTS MANAGEMENT METHOD FOR TERMINAL	在客戶裝置中針對權力物件的管理流程，每次下載至客戶裝置時，檢查其是否之前已經有此數位內容物件對應的權力物件，如有則將其權力物件的計數加一，並改變其時間標記

專利範圍 -1

- 本發明可作為文件整體儲存於雲端(或伺服器)上，針對使用者授權使用數位版權管理文件之使用與保護方式。其中可作為專利之Claim為：
  1. 一個可進行文件分割與加密之數位版權管理系統，其中包含Content Segmentation、Encapsulation Module、DRM License Server與DRM Packager等元件
  2. 範圍1所屬之功能元件，可存在於同一台機器或分散於不同之機器但以相同之邏輯關係存在
  3. 具備自動或半自動分割數位文件能力之content segmentation元件，應該包含：
     - 依據描述語言或預設能力分割數位內容
     - 對所分割之數位內容，建立前後相關連之序號或標示

專利範圍 -2

4. Encapsulation Module可依照設定之需求，產生一固定長度之DRM Vector
5. Claim 4中所述之DRM Vector，可使用一預設運算邏輯，將資訊整合成固定長度之數位資訊
6. Claim 4中所述之DRM Vector可包含由content segmentation元件所產生之內文物件關聯資訊
7. Claim 4中所述之DRM Vector可包含由交易資訊系統或content info database所紀錄之使用者資訊、裝置資訊與請求時間戳記
8. Claim 4中所述之DRM Vector可包由DRM License Server所紀錄之版權相關資訊、裝置資訊
9. DRM Packager使用已知或其他相關必須之運算，組合content object、key與DRM Vector，產生DRM Objects
10. Client端藉由網路只得到DRM Objects與解密之key，DRM Vector則依照前置之註冊紀錄，交易紀錄，與本身所帶之資訊產生

侵權認定

- 本發明之主要Claim在於針對文件內容切割、加密包裝之方法，並在加密資訊中加入使用者資訊、裝置資訊與物件請求關聯資訊，可判定侵權之要點如下：
  - 一份完整內容依據使用者習性或內容文意進行分段切割包裝成DRM物件，並均採用不同或相同之加密金鑰
  - 使用者裝置每次只可取得與保存部分DRM內容物件，且相同內文之DRM Object於使用者所擁有之不同裝置中，解密需求之訊息不同
  - 相同之DRM Object中，依照不同裝置請求物件之順序不同，除解密訊息不同之外，同一物件亦無法在使用者另一合法裝置中解密

侵權判斷

- 勾選本案之判斷侵權的方式，並詳實敘述判斷方式
  - ■由外觀可判斷 ■需還原工程 ■藉由測試判斷 □其他

技術可利用領域

- 網路數位媒體(數位內容)系統平台的軟硬體供應商
  - 出版商
  - 電子書城
  - 電子書閱讀器
  - Smart phone
- 學習平台
  - 多人線上學習或共同閱讀的進度掌控
- 企業級數位版權管理(DRM)與數位資料防護(DLP)
  - 每一使用者與裝置均取得不同DRM Object

專利撰寫

一、發明名稱：（中文/英文）

數位版權管理物件之加密/解密方法、數位版權管理物件加密/解密裝置/ METHOD AND APPARATUS FOR ENCIPHERING/DECIPHERING DIGITAL RIGHTS MANAGEMENT OBJECT

二、中文發明摘要：

一種數位版權管理物件之加密方法、數位版權管理物件之解密方法、數位版權管理物件加密裝置及數位版權管理物件解密裝置。數位版權管理物件之加密方法包括：接收由由數位內容(Content)切割而成之數個內文物件；根據數位版權管理物件加密裝置與數位版權管理物件解密裝置之間的默契資訊產生數個數位版權管理向量（DRM Vector）；以及分別根據數個數位版權管理向量加密數個內文物件以產生數個數位版權管理物件。

三、英文發明摘要：

Method and apparatus for enciphering/deciphering digital rights management (DRM) object are disclosed. The enciphering method comprises following steps. A plurality of content objects which are divided from a digital content are received. DRM vectors are generated according to tacit information between the DRM enciphering apparatus and the DRM deciphering apparatus. The content objects are respectively enciphered to generate DRM objects base on the DRM vectors.

四、指定代表圖：

(一)本案指定代表圖為：第（ 2 ）圖。

(二)本代表圖之元件符號簡單說明：

21～23：步驟

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無

專利撰寫

六、發明說明：

【發明所屬之技術領域】

本揭露是有關於一種數位版權管理物件之加密方法、數位版權管理物件之解密方法、數位版權管理物件加密裝置及數位版權管理物件解密裝置。

【先前技術】

隨著數位內容服務的普及與多樣化，數位版權管理(Digital Rights Management, DRM)開始廣泛的應用於各項電子產品或是網路服務中。數位版權管理的目的在於保障數位內容的散播過程，以防任意複製或使用的侵權行為。並依據數位內容的形式與相關電子產品的功能，定義了商業經營模式。目前之數位版權系統多半與線上付費系統整合為一個完整的數位線上服務。

…

【發明內容】

本揭露係有關於一種數位版權管理物件之加密方法、數位版權管理物件之解密方法、數位版權管理物件加密裝置及數位版權管理物件解密裝置。

本揭露的一實施例是關於一種數位版權管理物件（DRM Object）之加密方法。數位版權管理物件之加密方法適應於數位版權管理物件加密裝置，係以一處理器來實施。數位版權管理物件之加密方法包括：接收由數位內容(Content)切割而成之數個內文物件；根據數位版權管理物件加密裝置與數位版權管理物件解密裝置之間的默契資訊產生數個數位版權管理向量（DRM Vector）；以及分別根據數個數位版權管理向量加密數個內文物件以產生數個數位版權管理物件。

專利撰寫

為了對本揭露之上述及其他方面有更佳的瞭解，下文特舉實施例，並配合所附圖式，作詳細說明如下：

【實施方式】

請同時參照第1圖、第2圖及第3圖，第1圖繪示係為數位版權管理物件加密裝置及數位版權管理物件解密裝置之示意圖，第2圖繪示係為數位版權管理物件（DRM Object）之加密方法之流程圖，第3圖繪示係為數位版權管理物件之解密方法之流程圖。數位版權管理物件（DRM Object）加密裝置11包括接收單元111、數位版權管理向量產生單元112及數位版權管理物件產生單元113，而具有數位內容(Content)之交易號碼的數位版權管理物件解密裝置12包括數位版權管理向量產生單元121及內文物件產生單元122。數位版權管理物件加密裝置11可以是伺服端(Server)或用戶端(Client)，或由處理器來實施。而數位版權管理物件解密裝置12可以是用戶端(Client)或伺服端(Server)，或由處理器來實施。當數位版權管理物件加密裝置11為伺服端時，則數位版權管理物件解密裝置12為用戶端。相反地，當數位版權管理物件加密裝置11為用戶端時，則數位版權管理物件解密裝置12為伺服端。用戶端例如為家用電腦、平板電腦、筆記型電腦或手持式電子裝置。數位版權管理物件之加密方法能適應於數位版權管理物件加密裝置11，且包括如下步驟：

專利撰寫

【主要元件符號說明】

11：數位版權管理物件加密裝置

12：數位版權管理物件解密裝置

21～23、31～32、231～234、321～324：步驟

111：接收單元

112：數位版權管理向量產生單元

113：數位版權管理物件產生單元

121：數位版權管理向量產生單元

122：內文物件產生單元

1121、1124：向量加密單元

1122：金鑰加密單元

1123、1223：加密向量產生單元

1221：金鑰解密單元

1222、1224：向量解密單元

S1：數位內容

S2：內文物件

S3：數位版權管理向量

S4：默契資訊

S5：數位版權管理物件

S6：向量加密物件

S7：金鑰資訊

S41、S41 '：數位版權管理物件解密裝置之前次最後請求物件識別碼

S42、S42 '：數位版權管理物件解密裝置之使用者資訊

S43、S43 '： 數位版權管理物件解密裝置之識別碼

S44、S43 '：數位版權管理物件解密裝置之請求時間

專利撰寫

七、申請專利範圍：

1. 一種數位版權管理物件（DRM Object）之加密方法，適應於一數位版權管理物件加密裝置，係以一處理器來實施，包括：

接收由一數位內容(Content)切割而成之複數個內文物件；

根據一數位版權管理物件加密裝置與一數位版權管理物件解密裝置之間的一默契資訊產生複數個數位版權管理向量（DRM Vector）；以及

分別根據該些數位版權管理向量加密該些內文物件以產生複數個數位版權管理物件。

2. 如申請專利範圍第1項所述之數位版權管理物件之加密方法，其中該加密步驟包括：

分別根據該些數位版權管理向量加密該些內文物件產生複數個向量加密物件；以及

根據一金鑰資訊加密該些向量加密物件以產生該些數位版權管理物件。

3. 如申請專利範圍第1項所述之數位版權管理物件之加密方法，其中該加密步驟包括：

根據一金鑰資訊及該些數位版權管理向量產生複數個加密向量；以及

根據該些加密向量加密該些內文物件以產生該些數位版權管理物件。

4. 如申請專利範圍第1項所述之數位版權管理物件之加密方法，其中該默契資訊包括複數個默契值，該些數位版權管理向量係由該些默契值係經一邏輯運算所產生。

5. 如申請專利範圍第4項所述之數位版權管理物件之加密方法，其中該邏輯運算係為互次或（XOR）運算或雜湊函數(Hash Function)運算。

6. 如申請專利範圍第4項所述之數位版權管理物件之加密方法，其中該些默契值包括該些內文物件之關聯資訊、該數位版權管理物件解密裝置之識別碼、該數位內容之交易號碼(Transaction Number)、該數位版權管理物件解密裝置之請求時間(Request Time)、該數位版權管理物件解密裝置之前次最後請求物件識別碼（Last Requested Object ID）、或該數位版權管理物件解密裝置之使用者資訊、或以上任意組合。

結論

- 專利vs營業秘密
- 專利 vs公開發表
- 專利vs成本
- 專利vs effort
- 專利vs 時間點
- …
- 大廠玩的遊戲?