植基於二維行動條碼之校園小額付費系統

Campus Micropayment System by Mobile Barcode

楊慶隆　顏昭恩　王靖皓　陳志銘　陳澤世 李宇峰
國立東華大學資訊工程系 國立東華大學計算機與網路中心
cnyang@mail.ndhu.edu.tw

摘要

本論文採用二維條碼與行動裝置介面結合，實作出可運用於校園中之小額付款 (諸如：影印、餐券、場地借用等) 機制，並考量校園中之特殊需求，將小額付款機制與校園生活整合。本論文提出 QR Code 行動條碼之校園小額付費機制，結合手機端 J2ME 平台，實作有效且完善的校園小額付費系統，提升校園小額付款之便捷性，由於所採用的 QR Code 二維條碼，其資料容量大、可快速讀取、有抗損性等特質，因此，掃描器不需與後端資料庫建立即時連線，僅需定期更新資料，使得本系統可達到節省人力資源、降低管理成本、增加安全性等目的。

關鍵詞：二維條碼、QR Code、校園小額付款、公開金鑰系統

1. 前言

現今實用之條碼系統可分為一維條碼(如：EAN 等)以及二維條碼(如：PDF417、QR-Code 等)，這些條碼的使用目的均是為了方便管理商品或是控制商品品質等工業與商業上的用途。近年來，二維條碼的應用更加擴展到付款機制的實行，日本 NTT DoCoMo[1]公司所提供的商業平台，即成功的整合二維條碼 QR Code[2]與小額付款機制，為市場帶來一種新的商業機制。日常生活中所常用的一維條碼，如常見的 EAN 碼，多是由黑白線條粗細來定義資訊內容，最左右兩邊的黑線用來定義條碼總長度與寬度參考，並利用寬度定義出字碼內容。由於長度的侷限，所儲存的資訊內容較少，且條碼所含資料僅代表資料庫搜尋之索引值，如果在缺乏網路或資料庫的狀況下，一維條碼便失去意義。然而，二維條碼不僅僅資料儲存量遠大於一維條碼，且因本身即類似一個可攜帶資訊的小型資料庫，所以不會受到網路的侷限。再者，二維條碼本身兼具了錯誤糾正碼技術，可修正一定比例的錯誤字碼，其種種特性皆優於一維條碼，下表 1 中我們列出一維與二維條碼之簡單比較。顯而易見的，二維條碼無論在儲存量、安全性、效益性、追蹤性以及抗損性等各個比較層面，均遠遠優於一維條碼機制。

表 1. 一維條碼與二維條碼之比較

	一維條碼	二維條碼
儲存量	不超過 15 個字元。	一維條碼 100 倍以上。
安全性	憑肉眼即可判別一維條碼粗細線意義。	可在編碼及解碼時加密，亦稱安全條碼。
效益性	資訊在資料庫中，無法直接取得資訊。	可直接解回資訊。
追蹤性	無資料庫即無法取得資訊。	資訊跟著產品走，可追蹤產品的流向。
抗損性	磨損即無法讀取。	擁有錯誤改正能力。

本論文所提之校園行動條碼小額付費機制，則是將二維條碼透過使用者的手機或是電腦連接網路，於登入系統驗證為合法使用者後，即可選擇所需之付費項目，緊接著系統會依據使用者需求，將二維條碼透過網路傳至使用者手機或電腦中；其中二維條碼已攜帶付費金額之相關資訊，使用者可將其列印下來或存至手機顯示，再於相關付費單位出示二維條碼透過讀碼器掃瞄，即完成該次小額付費之服務。此一小額付費流程於校園中十分有效，這是由於學生於校園中常常需要影印、圖書借閱、餐券、游泳券等，傳統流程均採用預售模式或是現場售票，各單位均需有分離的管理機制，本系統即是針對此部分應用，整合各類付款，使校園生活更加便利。本論文架構如下：第二章介紹二維條碼以及小額付費，第三章論敘本文提及之校園行動條碼小額付費機制，第四章探討本系統機制之安全性，結論述於第五章。

2. 二維條碼

近年來二維條碼已被廣泛的運用於各行各業，諸如：郵務、商品管理、付款等，其優勢主要在於儲存量大及抗損性，不僅僅無須後端資料庫的配合藉此降低了建置成本，具抗損性的性質也使得二維條碼可用在較為嚴苛的環境中。二維條碼可儲存許多資料，如：圖片、文字、記號等各類型資料皆不受限制，條碼本身類似一個小型檔案隱含各類資訊。此外，大部份的二維條碼皆具有錯誤更正能力，即條碼本身具有容錯演算法，可使條碼擁有抗損性；不論是污損、斷裂、折疊，只要受損面積在可容忍之範圍內，皆能將其解碼並正確讀出。

現今二維條碼的兩大類型，可分為堆疊式

(Stacked)與矩陣式(Matrix)二維條碼。堆疊式是植基於一維條碼的基礎上向二維條碼擴展，通常是將一維條碼層疊起來表示資料，其中，較具代表性的堆疊式二維條碼為 PDF417；矩陣式則是利用圖像識別原理，採用幾何結構設計出二維條碼，如：QR Code、Maxi Code、Data Matrix 等。表 2 列舉幾種二維條碼比較，其中 PDF417[3]為歐美常用之工業標準而 QR Code 則被日本業界採用實行於小額付款，因此，我們接下來將繼續深入討論 QR Code 與 PDF417。

表 2. 二維條碼種類

條碼種類		QR Code	PDF417	Maxi Code	Data Matrix
類型		矩陣式	堆疊式	矩陣式	矩陣式
發行商		Denso	Symbol technologies	UPS	RVSI
國際標準		AIM International ／ISO／JIS	AIM International ／ISO	AIM International ／ISO	AIM International ／ISO
資料容量	數值	7089	2710	138	3116
	字元	4096	1850	93	2355
	位元	2953	1018		1556
	日文	1817	554		778
主要特徵		容量大以及較小列印面積並有高速辨識機制	容量大	高速辨識	列印面積

2.1 PDF417

PDF417 是一種堆疊式的二維條碼，由美國 Symbol Technologies, Inc. 所設計[3]。目前，PDF417、Maxi Code、Data Matrix 同被美國國家標準協會(American National Standards Institute, ANSI)選為二維條碼國際標準制定範圍，其中 PDF417 主要應用於工業運輸包裹的分類與追蹤以及商品資料標籤。另外，PDF417 亦具備錯誤偵測能力，可從受損的條碼中讀回完整的資料，其錯誤復原率最高可達 50%。

其中，PDF417 受到大量採用的主要原因是由於它是一個公開碼，其全名為 Portable Data File 的縮寫，其條碼類似一個小型檔案，可儲存大量資料並能將資料跟隨產品標示。此外，417 則是其編碼方式(如圖 2)，表示每個字碼包含 17 個模組，而 17 個模組是由 4 個黑線及 4 個空白(4 黑 4 白)組成，4 黑 4 白至多皆不能超過 6 個模組寬。單一字碼的組成約如圖 1 下方所示，一張 PDF417 條碼由多組字組結合而成，可透過掃描器掃瞄讀取，由於 PDF417 為一種堆疊碼，因此可透過單向掃瞄解碼。而 PDF417 的錯誤更正能力則分為 9 個等級，級數愈高，錯誤糾正能力愈強，但可存放資料量就愈少。

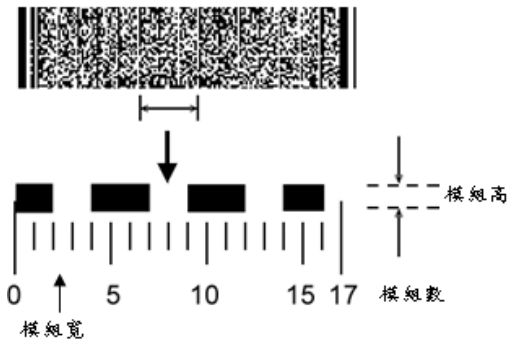


圖 1. PDF417 字碼組成

2.2 QR Code

QR Code 是一種矩陣式二維條碼，於 1994 年由日本 Denso-Wave 公司發明。QR 是英文“Quick Response”的縮寫，為快速反應的意思，此條碼是現今日本最流行的二維條碼。QR Code 的外觀呈正方形並由黑白兩色組成，如圖 2 (a)所示，在 4 個角落的其中 3 個印有正方圖案。其中，正方圖案是用於幫助解碼軟體定位，因此，使用者不需要很精確的對準即可高速讀取並解碼 QR Code。圖 2 (b)中則是受到磨損後的情形，由於 QR Code 一樣擁有可設定抗損等級的機制，只要毀損面積小於抗損能力，原始資料即可以透過解碼錯誤更正碼完整取回。

(a) QR Code symbol

(b) 抗污損能力

圖 2. QR Code

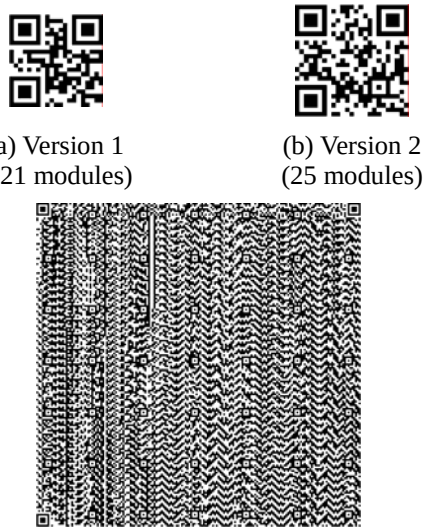
QR Code 共分有四種字碼種類，分別是 Numeric、Alphanumeric、binary、Kanji，並可以混合使用這四種字碼，以便達到最高的使用效益。在規格上如表 4 所示，於置入二進位資料時 QR Code 最高可以容量 2953 個字元(QR Code Version 40, ECC: L)，遠大於其他一維條碼的資料含量。此外，QR Code 支援四種容錯等級，分別為 L (7%)、M (15%)、Q (25%)、H (30%)，等級越高可以接受的污損率也更高。另外，使用者可自行選擇容錯等級，容錯率的大小會造成同一版本的 QR Code 內容含量數縮減或變大(如圖 3)。以最小的 QR Code (Version 1)來說(圖 3(a))，其長寬各有 21 個 module，而縮減或變大皆以 4 個 module 為單位，因此，

Version 2 則為 25 個 module(圖 3(b))，圖 3(c)則為 Version 40 擁有 177 個 module。一般而言，Level M 為較常選用的容錯等級。

表 4. QR Code Outline Specification

Symbol size	21 × 21 ~ 177 × 177 modules	
資料容量	Numeric(數字)	7,089 字元
	Alphanumeric(字母)	4,296 字元
	8-bit bytes (二進位)	2,953 字元
	Kanji (漢字/片假名)	1,817 字元
容錯等級	Level L	約 7%
	Level M	約 15%
	Level Q	約 25%
	Level H	約 30%

本論文中所提之二維行動條碼付款機制，由於所採用之行動裝置多為手機或是 PDA，其顯示裝置多為方形或是矩形，因此，採用 QR Code 是一個較合理的選擇，且在亞太地區 QR Code 的採用遠較於其他二維條碼普遍，較能被人們所接受。此外由於所採用的條碼顯示裝置為行動裝置，因此，錯誤更正率僅需採用較低等級 L 或是 M，無須考量條碼大量破損情況。



(a) Version 1 (21 modules)　(b) Version 2 (25 modules)

(c) Version 40 (177 modules)

圖 3. QR Code symbols

3. 校園行動條碼小額付費機制設計概念與系統實作

在校園生活中，常常有制式的小額付費，例如：停車費、各種設備使用/借用費、小額繳款、影印卡等。然而，卻缺乏一套有效、方便且安全的方法來整合。以東華大學為例，繳交電腦教室的影印費用需先至校內銀行轉帳後，依據收據再至電腦教室儲值，由於校地廣大來往十分不便與費時。因此，本論文中我們將二維條碼與小額付費兩種模式合併。意即，藉由二維條碼攜帶資訊的便利性與安全機制，帶給小額付費更簡便、安全的應用。本論文所提的小額付費機制，也與一般市面通行之小額付款機制略有差異，變的更為方便且兼顧校園使用之獨特性。由於本論文所提設計概念需要與校園生活中之各項消費結合，因此需考量校園生活中各項特殊需求，其系統示意圖如圖 4 所示，使用者可將購得統一規格之行動票券，於相對應的服務點(如：圖書館、電腦教室、餐廳等)消費支付相對應的費用(如：影印費、上網費用、餐券等)，使用者收款機制則可定期收取或於學生畢業/註冊時一併收取，藉以提供便利的繳費與消費模式。

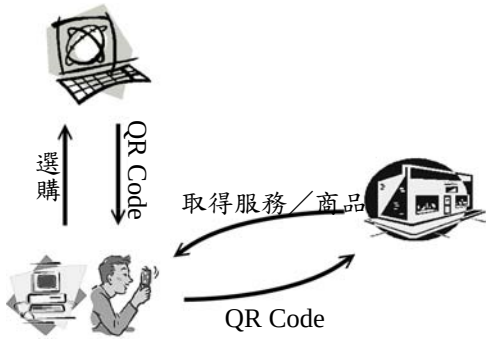


圖 4. 校園小額付費機制流程圖

3.1. 校園小額付費機制系統流程

本論文中所提之小額付款機制如圖 5 所示，使用者可用手機或電腦連上本系統網站並選擇需要的票券免費領取，網站立即傳送一個攜帶票券與驗證資訊的二維行動條碼給該使用者，該使用者可將其存於手機中攜帶。緊接著，使用者於適當的使用場合，出示行動條碼並經由讀碼器掃描驗證後，即得以使用。在此需特別強調的是，讀碼器於校園中的設置並不需要連線，這是由於我們所採用的二維條碼可藏有大量訊息所致，故有效之條碼可在其有效期限內被使用。

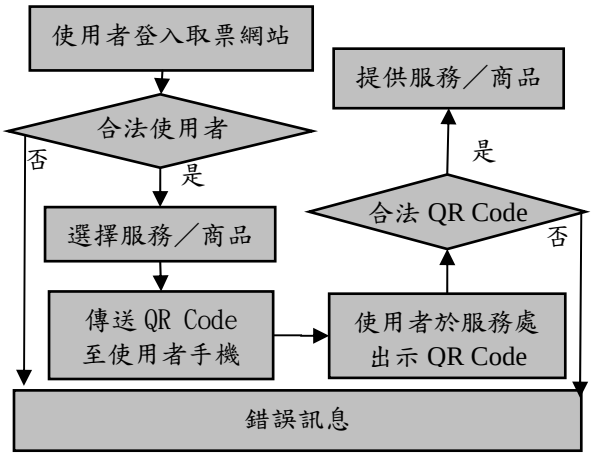


圖 5. 校園小額付費機制流程圖

於所提系統中，QR Code 二維條碼的內容欄位資料設計如圖 6 所示，其中各項參數定義如下：

DN： 票券面額
ED： 票券有效期限
ID： 使用者序號
SN： 票券序號
TP： 票券種類
$S_{KR}(\cdot)$： 簽章; *KR*: 收款中心私密金鑰
$V_{KP}(\cdot)$： 簽章驗證; *KP*: 收款中心公開金鑰

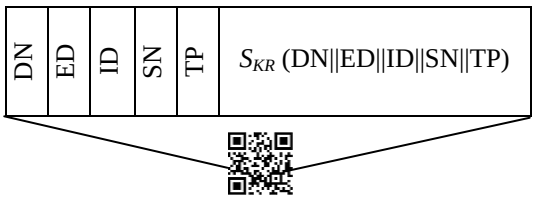


圖 6. 票券資料內容

票券內容中的簽章與簽章驗證採用公開金鑰系統，各個條碼掃描器中均有公開金鑰並可透過 V_{KP}(DN||ED||ID||SN||TP)驗證票券內容是否為收款中心簽署以及是否有受到竄改。於本系統中，由於票券中擁有唯一之票券序號，且單一序號於特定讀取器中僅允許提供一次服務，這可透過給予特定票券種類達成，例如：游泳池之票券種類為 S001、圖書館影印以及系所影印給予票券種類編號 X001 與 X002，讀取器 X001 即不會承認 X002 票券種類之票券，因此條碼掃描器僅需驗證其有效性，無須後端資料庫連線，藉此充分發揮二維條碼之優勢。此外，條碼掃描器僅需紀錄該使用者序號以及該票券序號，並於固定時間向收款中心回報即可，無須於線上即時回報。這種設計可以於校園中很有效的建置條碼讀取器，無須網路連線。此外，有效期限的有效時效設置需審慎考量，時限太長則在手機遺失時有被冒用之風險，時限太短則會增加使用者取票次數，增加使用上之不便。另外，使用者序號以及票券序號均為唯一，藉此區分使用者以及登錄票券使用資訊。

本論文所提之校園小額付費機制可分為三個主要部分，分別為：取票機制、消費機制以及付款機制。其中，本系統與一般小額付款機制的主要不同處在於取票機制中，本系統是不需先付費，而是於取票後有消費才對消費者扣款。此外，消費機制也採用離線式設計，這是由於連線設置條碼掃描器會增加設置成本，同時也會有網路維護問題。而付款機制則由於本系統實行於校園中，因此，可透過學期註冊或者是定期向消費者收取款項，緊接著我們將詳細介紹此三流程。

3.1.1 取票機制

使用者可於校園內透過手機，上網輸入個人密碼登入取票頁面後，選擇所要取得面額票券之項目下載至手機裡。於選定票券之後，使用者會收到一張影像格式的行動條碼，並可至服務點讀取器感應該二維條碼，即可完成交易動作，系統方塊圖如圖 7 所示。

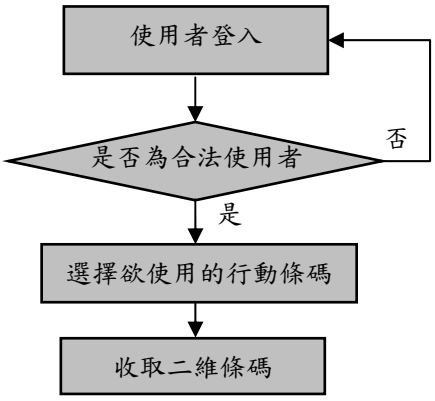


圖 7. 取票機制方塊圖

3.1.2 消費機制

使用者於條碼出示後會透過合法性驗證並於消費後於讀取器記憶體中紀錄條碼數，以供日後扣款之依據。系統方塊圖如圖 8 所示，使用者欲使用行動票券時需於手機輸入驗證密碼，密碼正確則手機會顯示該張二維條碼，此條碼可供掃描器讀取，並將消費記錄留存於掃描器中。

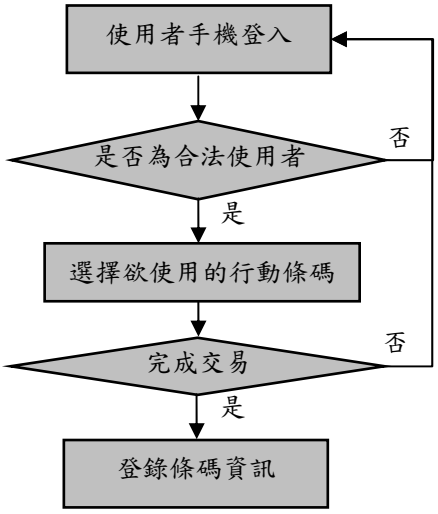


圖 8. 消費機制方塊圖

3.1.2 付款機制

由於本系統實作於校園中，因此可透過學雜費繳交時一併向學生收取其消費，此外，教職員消費也可於每月核薪時扣款，使用者不需於消費當時繳交費用，十分便捷。

3.2.系統建置環境

本論文中採用的實作系統平台建構軟體與軟

體版本如表 5，網頁伺服器主系統所採用的作業系統為 Windows XP、網頁伺服器使用 Apache、手機端程式採用 Sun 所提供的 Java Wireless Toolkit 模擬手機動作與傳送接收模式、資料庫則使用 My SQL，服務處於硬體方面結合二維條碼讀取器建置，這種建置平台的方式亦為一般普遍之設計，可使本論文的實作內容與現實小額付款商務更為貼近，讓本系統擁有市面小額付款機制的既有優點。

表 5. 系統實作平台

	平台單元	採用軟體與版本
系統實驗平台	資料庫	MySQL-5.1
	網頁互動	PHP5
	網頁伺服器	Apache-2.0.54
	手機端程式	Sun Java Wireless Toolkit 2.5.1
	作業系統	Windows XP
	二維條碼讀取器	2D-bar Code scanner (CCD)

3.2.1 服務點之消費機制建置

二維條碼使用者持著條碼至目的地服務處出示後，待掃描器掃瞄並解碼驗證簽章為合法後，即開放使用者使用該服務(如：影印、餐券等)，並於掃描器內記錄使用者票券使用歷程，待一定時間後一併回報收款中心。此外，掃描器可依照唯一的使用者序號以及票券序號，記錄其使用即可，唯一之序號僅可於單一特定讀取器中使用一次，藉此杜絕重複扣款之問題。此種設計模式可將掃描器設置成本降至最低，僅需紀錄使用歷程而不需即時回報，因此不需於掃描器端建置網路，有效降低建置成本。

3.2.2 手機端程式取票建置

手機端方面我們採用 Sun Java Wireless Toolkit 編寫用以模擬手機執行 JAVA 程式時的操作行為以及資料傳送模式，使用者可透過手機，上網輸入個人密碼後登入取票頁面，選擇所要之項目，並下載至手機裡，其程式選取畫面如圖 9 所示，此取票平台針對手機顯示畫面設計，方便使用者選取票券。於選定票券之後，使用者會收到一張影像格式的行動條碼，並可至服務點讀取器感應該二維條碼，即可完成交易動作。在此由於手機按鍵操作不便，且手機門號皆具備唯一 SIM 卡，使用者身份較無安全問題；故手機登入取票網站時，僅需輸入登入密碼。

圖 9. 手機端程式畫面

3.2.3 網頁伺服器取票建置

實作網頁伺服器部分，我們採用 Apache 系統架設，使用者可依照自己的需求，連線至校園行動條碼小額付款網頁購買選擇自己需要的商品。於開始時網頁會要求使用者登入，預設登入帳號即為使用者之學號，該密碼預設為身分證字號(如圖 11 所示)，使用者可於首次登入後更改。使用者在第一次登入時，本系統可透過簡訊完成手機號碼認證程序，藉此在往後的交易過程中，一個使用者帳號即僅對應一個手機號碼，藉此杜絕輸入錯誤或是惡意攻擊等行為。完成會員登入後，可選擇票券、查看個人資料以及服務說明等等。點選票券產品，取票頁面如圖 12 所示，使用者選擇想領取之票券，再點選票券名稱即可下載票券。

圖 11. 登入畫面

圖 12. 購買畫面

4. 安全機制

為建置本二維行動條碼小額付費系統，避免付款錯誤或遭人盜用，我們在本段討論網頁端與手機端資料傳輸安全、手機端程式安全以及票券等安全問題。此外，我們也針對一些與電子商務相關之安全議題分析本系統之安全性。針對行動小額付款機制的安全以及與各種其他付款機制比較，亦有學者[6][7]提出許多建議。

4.1 網頁端瀏覽與傳輸安全

於網頁瀏覽端部分，JAVA 提供與 SSL 相似的網頁安全傳輸機制，這個機制已經在 MIDP 2.0 中實行，因此，連線間的安全可透過此機制保障，使得取票時不會被無線通道中的惡意攻擊者監聽或是竊取。而使用者首次登入時所設計的簡訊認證機制，更可以進一步的防止惡意攻擊發生。

4.2 手機端程式安全

考慮到手機按鍵操作不便，又由於手機門號皆具備 SIM 卡卡號，使用者身份較無安全問題；故登入取票網站時，僅需輸入登入密碼即可取得票券。此外，使用過的行動條碼，將透過二維條碼讀取器於後端資料庫統一登錄其使用，每一條碼皆具備獨立序號，故可防止登錄與扣款上的錯誤；行動條碼於手機端之刪除與否，則由使用者決定。於本系統中，手機端程式僅提供操作與顯示介面，對後端資料安全較無威脅性。

4.3 票券安全機制

票券安全可分兩部份探討，首先，於票券內容部分，本系統採用公開金鑰系統對票券內容簽章，可以有效的杜絕竄改，因此，惡意的使用者無法竄改票券內容，達到防止冒用的危險。此外，重製票券也因攻擊者沒有收款中心之私密金鑰，因此無法任意製作扣款條碼，而若是由於遺失手機所造成的票券冒用，則可透過掛失機制避免。

另一方面，票券有效期限的設置可由使用者自訂，這是由於使用者的行動裝置若發生遺失的狀況，則票券很有可能會被冒用，這種被冒用的風險可以透過手機軟體的設計，如：顯示票券時須輸入密碼，或是設定較短的有效期限來防止這類情形的發生。一個合理的有效期限設置可以有效的降低風險並且節省使用者取票時的連線費用，提升使用者的使用意願，如：影印費用設置為一個月、餐券設置為一週。

4.4 使用者安全性

在此我們針對一般電子商務系統中常討論的議題逐一探討，諸如：不可否認性、不可偽造性、防止盜用等加以討論。

a. 不可否認性：使用者於掃描器前輸入對應之密碼藉此顯示行動裝置中的二維條碼，並完成消費記錄，此一動作僅有手機持有者可以完成。此外，條碼內容內含使用者資訊，因此本系統具有消費之不可否認性。
b. 不可偽造性：由於本系統之特殊設計，使用者於領取票券時需要設定特定門號，此外，票券內容也經由簽章確保其完整性，因此，票券之內容極難偽造或是更動。
c. 防止盜用：由於本系統之二維條碼存放於使用者之手機，因此若是發生手機遺失情形，二維條碼是否會被盜用？由於本系統於手機端條碼顯示介面之設計，既使是在手機遺失的狀況下，惡意的使用者也需要猜測二維條碼的取用密碼，因此可以確保該條碼不會因為手機遺失被輕易濫用。此外，掛失機制更可以進一步的阻絕因手機遺失而產生之種種問題。

經由以上各點之探討，本系統可確保在各個層面提供有效之相對應安全防護機制，使本系統可確實實用於校園。

5. 結論

本論文採用 QR Code，作為儲存消費金額及商品資訊相關資訊的行動條碼，並結合小額付費機制於校園中實行。其中，系統提供一般網頁與手機瀏覽兩個介面，使用者可利用電腦上網或手機 GPRS 隨時隨地連線至系統頁面，選取項目及金額後免費取得票券，再於付費之相關單位出示行動條碼，經過所採用的公開金鑰系統驗證簽章合法後，即完成該次小額付費之服務。讀取器會記錄下消費歷程並於一定時間後更新至收款中心。

經實作結果，本論文提出之小額付款機制非常適用於大學校園，以東華校園為例，建築物之間距離較遠，舊有付款機制十分不變且耗時，本系統可免去來回奔波付款所耗費的時間，不僅方便學生、教職員，省去付款所帶來的不便且兼顧付款安全性。此外，於校園職員下班時間，更可發揮此機制好處，隨時服務校園中人員。

參考文獻

[1] DoCoMo - www.nttdocomo.co.jp/english/
[2] QR Code - www.denso-wave.com/qrcode/index-e.html
[3] PDF417 - www.symbol.com
[4] Micro-payment - http://www.micro-payment.net/
[5] M.G. Gouda and A.X. Liu, “Formal Specification and Verification of a Micropayment Protocol,” 13th International Conference on Computer Communications and Networks 2004. ICCCN 2004. pp.489-494, 2004.
[6] A. Hasan and K. Raygan, “A Mobile Telephone Based, Secure Micro-Payment Technology using the Existing ICT Infrastructure,” CHINACOM 2007, International Conference in Communication and Networking, pp. 22-24, August 2007.
[7] M. E. Peters, “Emerging eCommerce Credit and Debit Card Protocols,” Proceedings of the 3rd International Symposium on Electronic Commerce. ISCE 2002. pp. 39-46, 2002.