逢 甲 大 學

資 訊 工 程 學 系 專 題 報 告

無線網路簡報管理系統

沈意芳(四甲)

學　生　：王國隆(四甲)

黃科維(四甲)

指導教授 ：李維斌

中華民國九十二年十二月

目錄

圖表目錄

摘要

由於資訊時代的來臨，似乎在現今的社會上，不管是要處理什麼事情，都要講求「效率」兩個字，隨著現今科技的日新月異，關於投影片的教學方式，從以前要花時間製作幻燈片，每當上台報告時，必須先將資料好好的保存及做排列，再作一一的放映，放映完的資料也得仔細的放置；到現在的單槍投影機直接連上 PC 或 NB，可從一個小小的磁片或是隨身碟中，經由現今的軟體技術，帶給人們大量的資訊，這著實給教育工作者或是企業的會議發表上，帶來了許多的便利性，也讓現今的簡報系統，變的更加的便利，使現今簡報的傳輸方式，有著大大的改善。

在這次的專題當中，也基於要讓簡報使用者，有更多的便利性為目的，所以製作出了關於無線簡報的相關程式，可讓簡報使用者免於上台作機械儀器的換置，可直接在原地作簡報的放表，不但省去了不必要的時間浪費，也能讓使用者以較為輕鬆的方式來發表自已的意見。在程式執行中做了資料的加密，所以可以放心資料的外洩問題，也許程式本身有待改進的地方，但對整體的便利性可言，是有發展性的一套軟體程式。

第一章　專題簡介

1.1　專題研究的動機與目的

在現今的社會裡，隨著電腦的普及化，各公司行號已經從以前的書面文件報告演變成單機作業，甚至透過網路傳輸溝通。而也隨著電腦型態的改變，筆記型電腦的使用性日趨增加，因此時常在會議上會使用自己的筆記型電腦放映投影片報告。但是每次要發表報告或是開會時，我們常會遇到一個困擾，那就是輪到自己上台報告時，就需要將單槍的連接線從上一位報告者的 notebook，拔裝至自己的 notebook，如此反覆動作，不但費時也費力。所以我們希望僅讓一台電腦連接單槍投影機當 server，使 server 端的電腦在不受到干擾影響之下，仍可讓其他電腦透過無線傳輸，將所要傳送的資料經由 server 投影到單槍上，以達到順利、流暢的簡報會議。

而在完成無線網路簡報傳輸之後，大家可能都會考慮到資料在傳輸的過程中，其安全性的問題，畢竟在企業界裡，開會的內容是關於公司的機密，所以我們也針對這一點做了加密的措施，另外也有對資料做壓縮的處理，以便減短資料傳送的時間。

1.2　開發工具與環境簡介

● 開發工具

專題實驗主要是用 JAVA 語言開發，介面的設計用到了 Swing，擷取螢幕 createScreenCapture, 並使用 JPEGCodec 將畫面轉成 JPG 檔。Server 與 Client 之間的連線使用 JAVA 的 Socket。加密則使用到 JCE 的 DES 演算法。

● 開發環境

具備兩台電腦, 均安裝 JDk1.4.1(內含 JCE 套件)和 JBuilder 工具，這樣就可以用 JDK 來編譯程式，實作我們的專題。

1.3 成果簡介

程式執行，決定 Server 端之後，其餘的電腦可以登入 Client 端連上 Server，並進行輪流撥放簡報的工作，且可以選擇使用撥放圖片或是抓螢幕的方式來報告。另外，也提供了線上聊天室的功能，可以在會議進行的同時，也能於底下討論，傳訊可以以廣播的方式告知全部，或以秘密聊天的兩人傳訊。所有的動作，Server 端均不會受限，且可以一起參與會議。此專題不受限於區域網路，在無線網路的環境下，依然達到順暢的目的，且目前正在申請專利中。

1.4 工作進度甘特圖

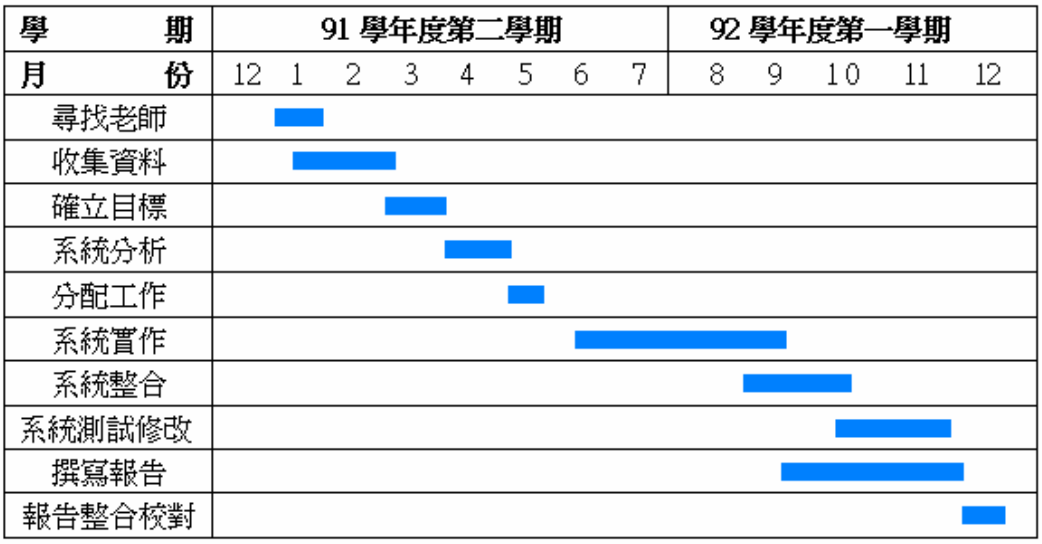


圖 1.1 工作進度甘特圖

1.5 章節概述

第一章是將整個專題前後作個簡介。內容包括了當初為何選擇作這個專題，以及所歷經的過程。所選擇的開發工具過程，還有編寫程式所用到的工具環境。最後程式所呈現出來的成果，包括了整體的操作介面，還有它的功能為何，可作何應用。整體開發所預定的工作甘特圖。

第二章所介紹的是此次專題的介面上，大致上所用到的基本 swing 功能，包括了 swing 的開發由來及其帶來的效能，並作有使用到的架構子階層介紹及其功能說明。最後介紹我們此專題所做的一些功能。

第三章介紹了 client 與 server 間的連線溝通方式，環境架構的設定，也有 client/server 的特性介紹及其應用功能。

第四章提及了密碼學的基本架構，以及在專題中所用到的演算法、加解密的過程介紹。

第五章是提供製作專題後的心得感想，並對這個系統未來的發展作了一番的討論。

另外附錄中有操作這個軟體的整個流程。

第二章 Swing

2.1 Swing 概述

Swing 是一種 JAVA 語言內的視窗工具，可提供廣泛的使用者介面的工具，但是它相較起來也較為複雜，由於 Swing 可以提供很多的視窗屬性變化，所以在寫的時候，可以作多樣化的變更，以 JavaBulider (JB)軟體為例，在作視窗的建構時，便會列出目前使用視窗的屬性，以供作更改用。

在 Swing 之前的，是所謂的 AWT(Abstract Window Tookit)套件，因為 AWT 在使用上難以變更已建構好的視窗內容，所以當我們只使用 AWT 來作一個視窗的時候，很難在上面作什麼變更，所以在要製作一個”優良的互動式視窗”時，只靠 AWT 實在很難達成所需要的目的，Swing 便因為此項的不便而漸漸形成，使 AWT 套件功能加強，但不是取而代之，可以說是相輔相成的 JAVA 視窗工具。

2.2 JAVA 元件介紹

在此會將專題所用到的視窗 Swing 元件作個介紹，會將比較重要的元件列出並作討論，下面圖 2.1 為在 javax.swing.JFrame 在 JB 的 Visual Javabeans designers 下所呈現的建構圖：

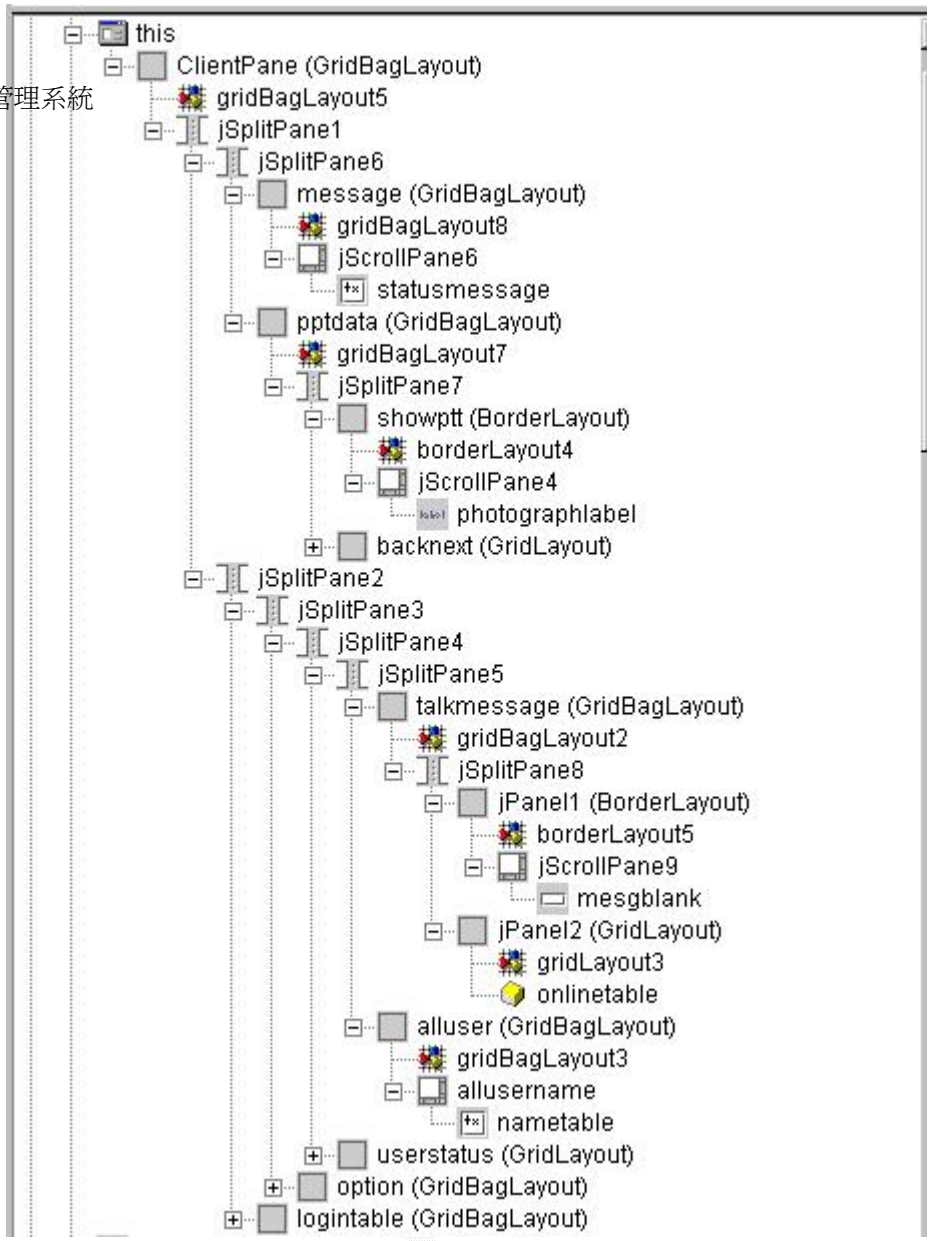


圖 2.1　整體建構圖

在圖 2.1 中，為整個視窗程式的整體架構圖，可以從上圖看到，每個名稱前都會有一個小的圖示，這就表示了其所使用的元件，如 JFrame、JPanel、JSplitPane 等等，會在下面的單元中作介紹。

2.2.1　JFrame 簡介

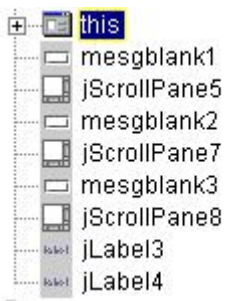


圖 2.2　JFrame

java.lang.Object

--java.awt.Component

--java.awt.Container

--java.awt.Window

--java.awt.Frame

--javax.swing.JFrame

在圖 2.2 中，”this”即為一個 JFrame 的元件，JFrame 可說是在設計 java 時最底層的一個容器元件，在此容器物件上則可以放置許多其他的元件(如 JLabel、JPanel 等…)，下面是此元件在類別階層圖裡所歸屬的類別，每個元件都有其階層圖。

2.2.2 JPanel 簡介

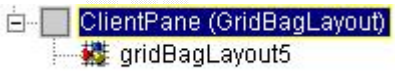


圖 2.3 JPanel

java.lang.Object

-java.awt.Component

-java.awt.Container

-javax.swing.JComponent

-javax.swing.JPanel

在圖 2.3 中，ClientPane 即為一 JPanel 元件，JPanel 常使用於版面管理上，並且可以用 panelx.add(物件)讓編號為 x 的 panel 上增加物件。

2.2.3 JsplitPane 簡介

圖 2.4 JsplitPane

java.lang.Object

-java.awt.Component

-java.awt.Container

-javax.swing.JcComponent

-javax.swing.JSplitPane

在圖 2.4 中，圖示類似於”工”的即為 JSplitPane 元件，顧名思義，它是一種可將面版作分割的元件，可在原本的 JFrame 或是 JPanel 上作分割，可選擇作 HORIZONTAL_SPLIT 或 VERTICAL_SPLIT 兩種常數，以便作水平或垂直的分割。

2.2.4 JScrollPane

圖 2.5 JScrollPane

圖 2.5 為 JScrollPane，一種捲動式的面版，就像我們平時在瀏覽網頁時，若畫面太長，就可用軸將視窗作捲動，藉由捲動的方式來將完整的內容作瀏覽。

2.3 其它元件

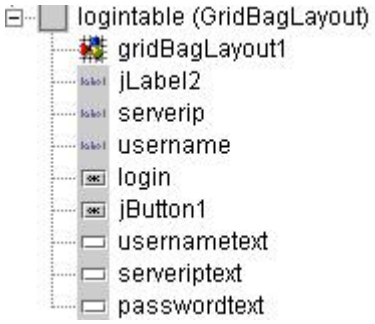


圖 2.6 其他元件

我們在此將介紹在圖 2.6”logintable”下的三個建構子：JLabel、JButton 及 JTextField。

對 JLabel 元件而言，我們通常在上面放上文字及圖示，為了讓視窗美觀，所以 JLabel 元件可加入位置的參數，以便作排列。

JButton 是常被使用在作選擇時的元件，亦可在上面加入文字及圖示，如最常見的”是”、”否”的選擇，或是像投影片內容的切換、傳送，或是作其他不同的事件處理(Event Handle)。

JTextField 元件常用於填資料上，在這次的專題內容中，我們就將它用在 ip、username 及密碼上的輸入，還有訊息的傳送上，也是要藉由 JTextField 元件來作輸入，配合 JButton 作傳送。

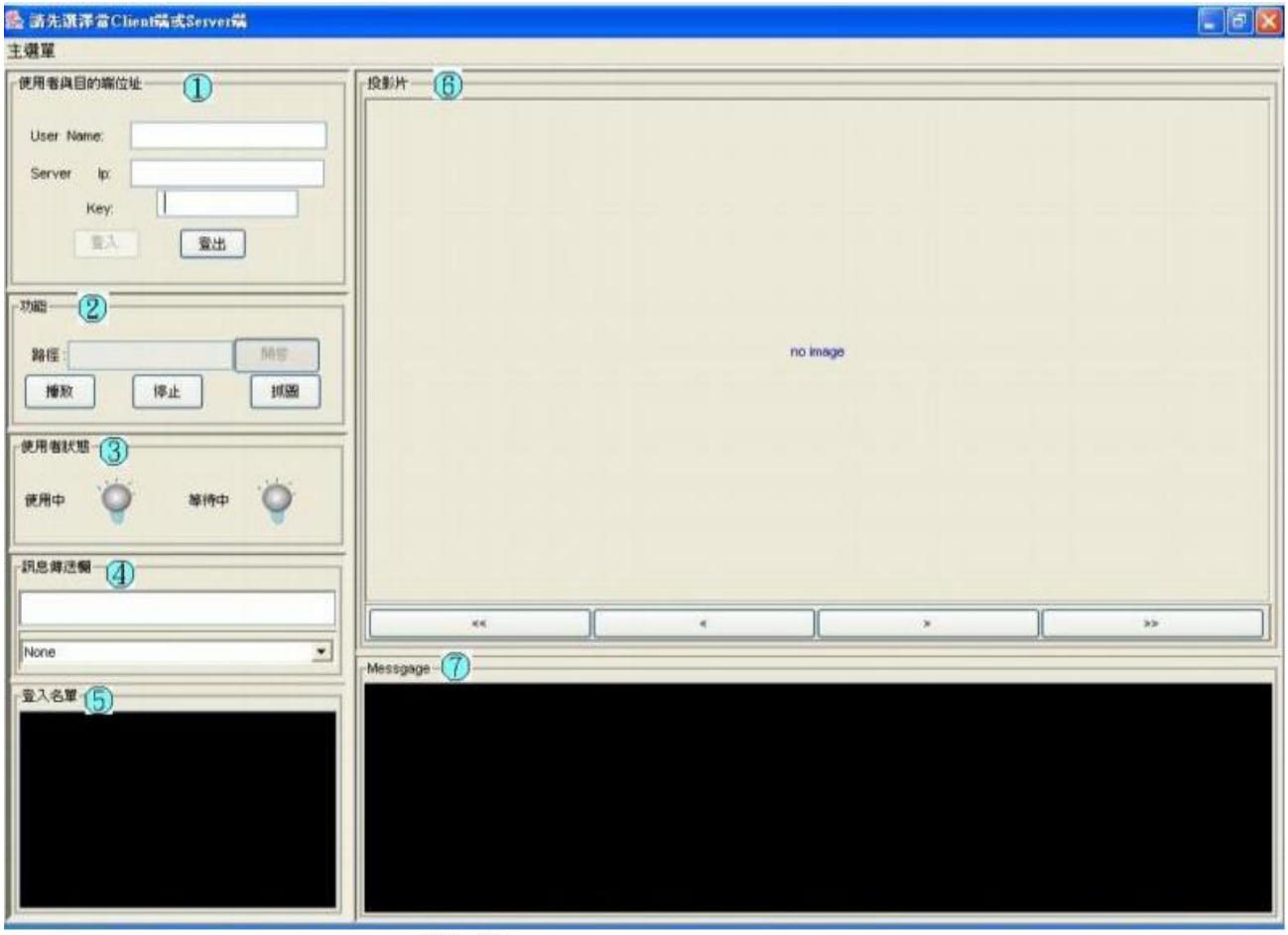


圖 2.7　專題中的 Swing 介面

2.4 系統實作功能介紹

■ 使用者與目的端位址

☐ 檢驗輸入的 user name、server ip、加密 key，的合法性

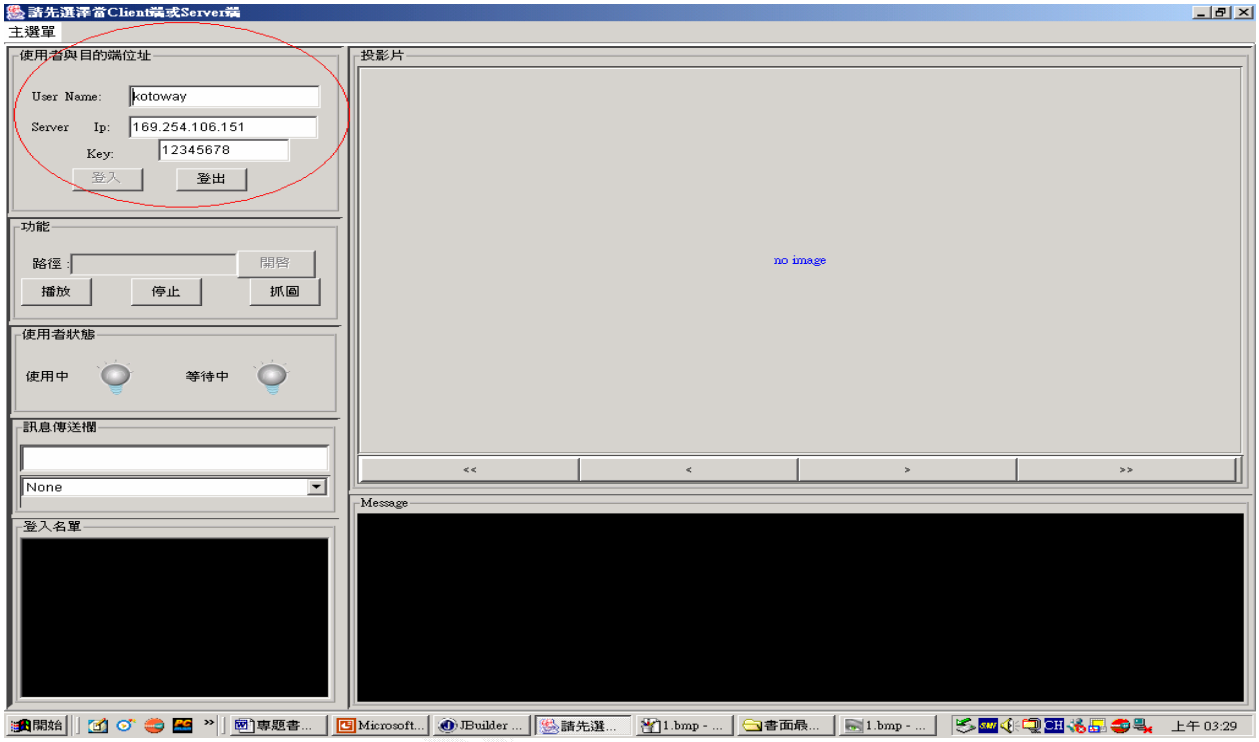


圖 2.8 使用者與目的端位址

■ 開啟舊檔

☐ 利用 filechooser 套件, 設定可開起的檔案為*. jpg 檔

☐ 對*. jpg 檔產生預覽效果

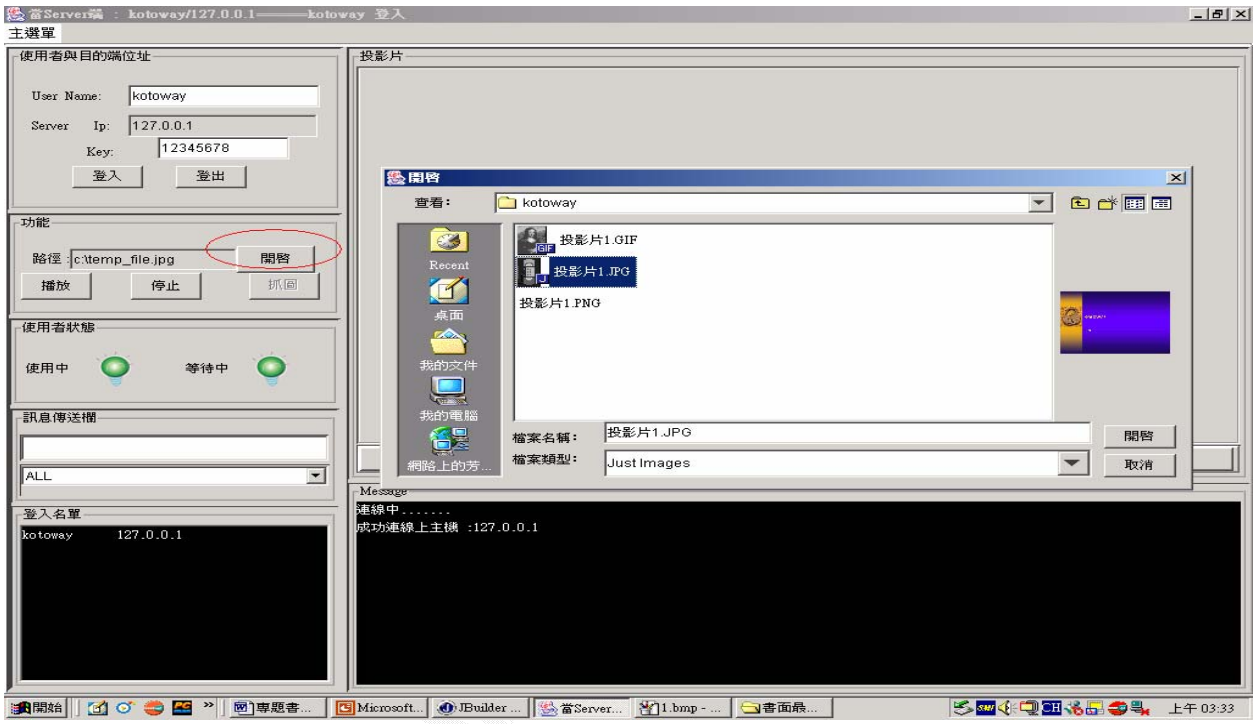


圖 2.9 開啟舊檔

■ 投影片

☐ 對所開啟的相似檔名檔案,做 arraylist 的儲存,例如:ta1. jpg、ta10. jpg、ta2. jpg、…

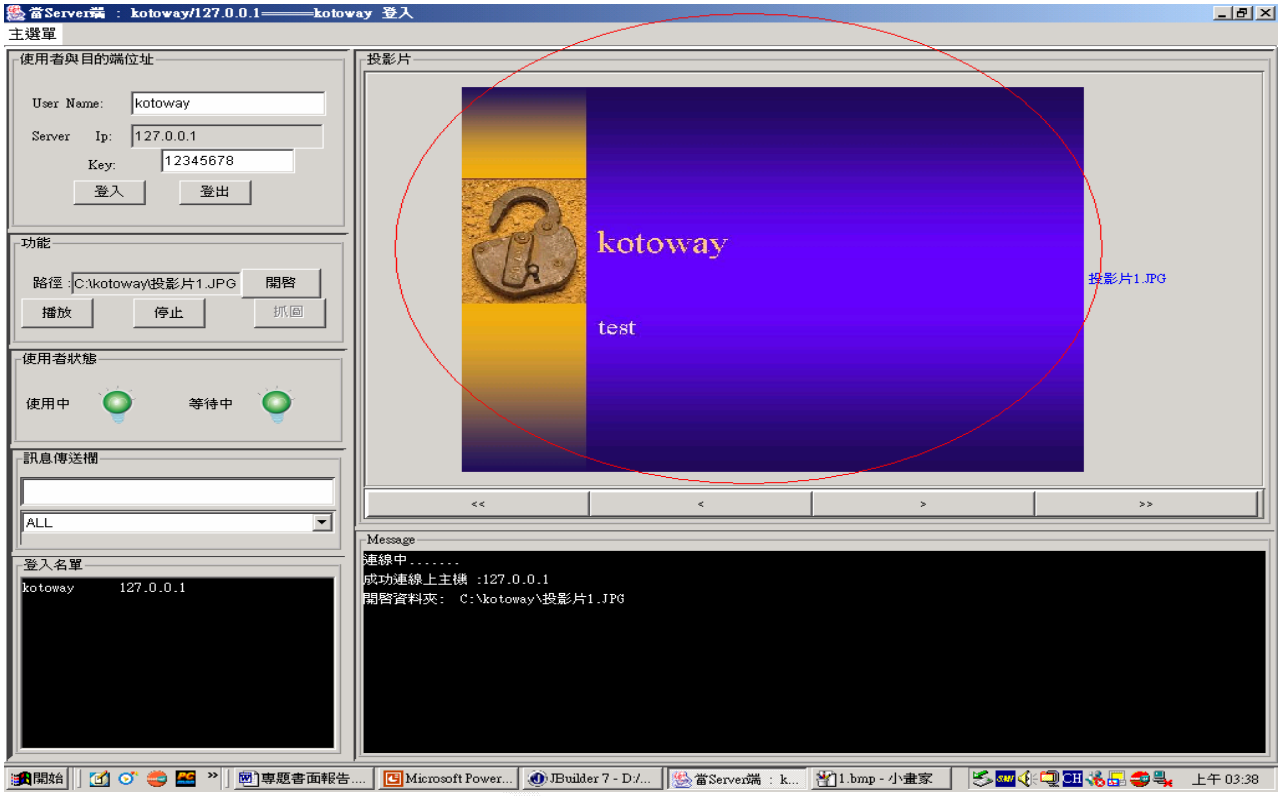


圖 2.10 投影片

■ 直接播放

☐ 即請求取得播放權

☐ 得到 Server 端允許後，開始傳送先前開啟舊檔時，所選取的檔案

☐ Client 端藉由“<<” “<” “>” “>>”來切換使用者要播放的投影片

圖 2.11 直接播放

■ 抓圖播放

☐ 即 Client 端採取截取自己電腦畫面的方法，取得播放權後，每一秒鐘自動抓取螢幕，然後傳送

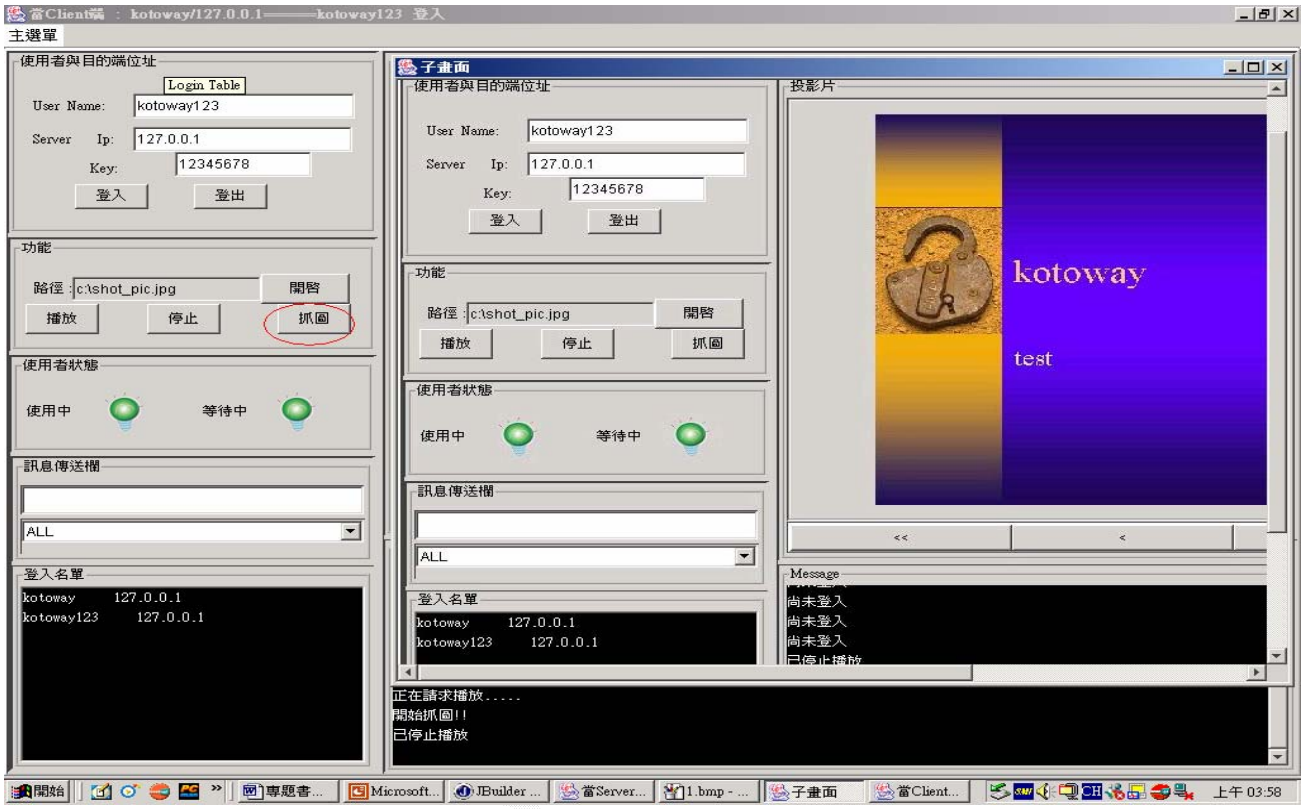


圖 2.12 抓圖播放

第三章　Server 與 Client 架構

3.1 JAVA 提供的網路功能

JAVA 所提供的網路功能主要分為三大類：

- URL(Uniform Resource Locater)：單一資源位置
- Socket：兩端資料傳輸，先連接後傳資料，為我們使用的方法
- Datagram：同為資料傳輸，但不可靠

3.1.1 Socket

使用此建構子 Socket()來產生 socket，並連結到指定的主機和通訊埠。此時可以使用 getInputStream()和 getOutputStream()回傳 inputstream 和 outputstream 物件，用他們來和遠端主機溝通。若是知道了目的主機的 port 和 ip 時，可使用 Socket(String host,int port)，例如：140.134.27.100:80

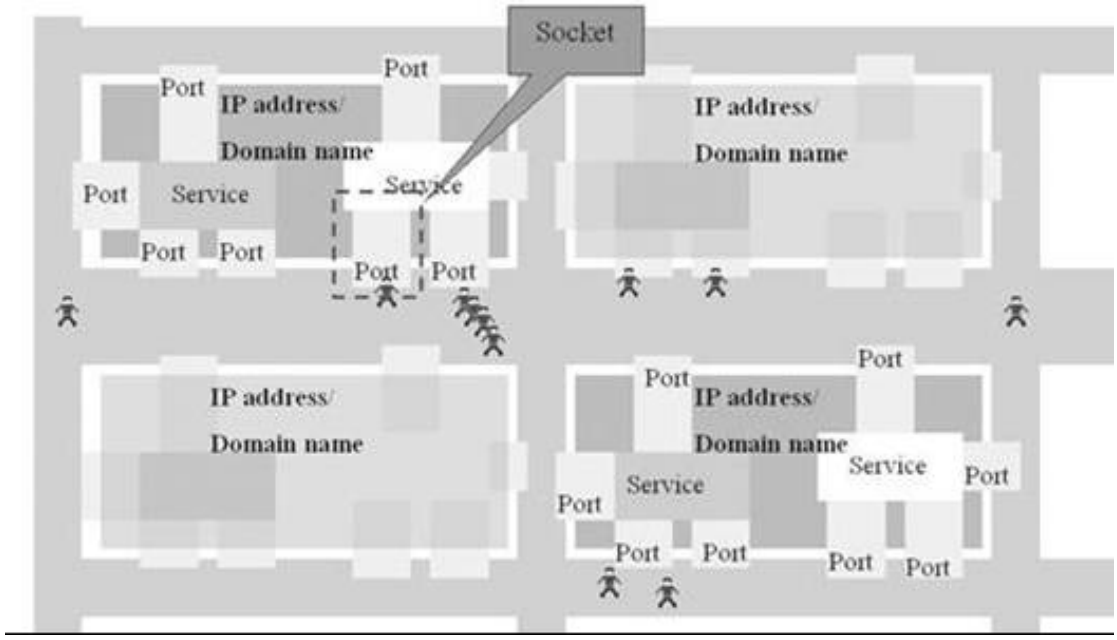


圖 3.1　Socket 概觀圖

3.1.2 ServerSocket

此類別為 Server 所使用，用來聆聽 Client 端的連結請求，產生一個 serversocket 時，便用 accept()方法來連結，當收到連結請求時，accept()會接受該連結，並傳回一個 socket，如此便可產生溝通。

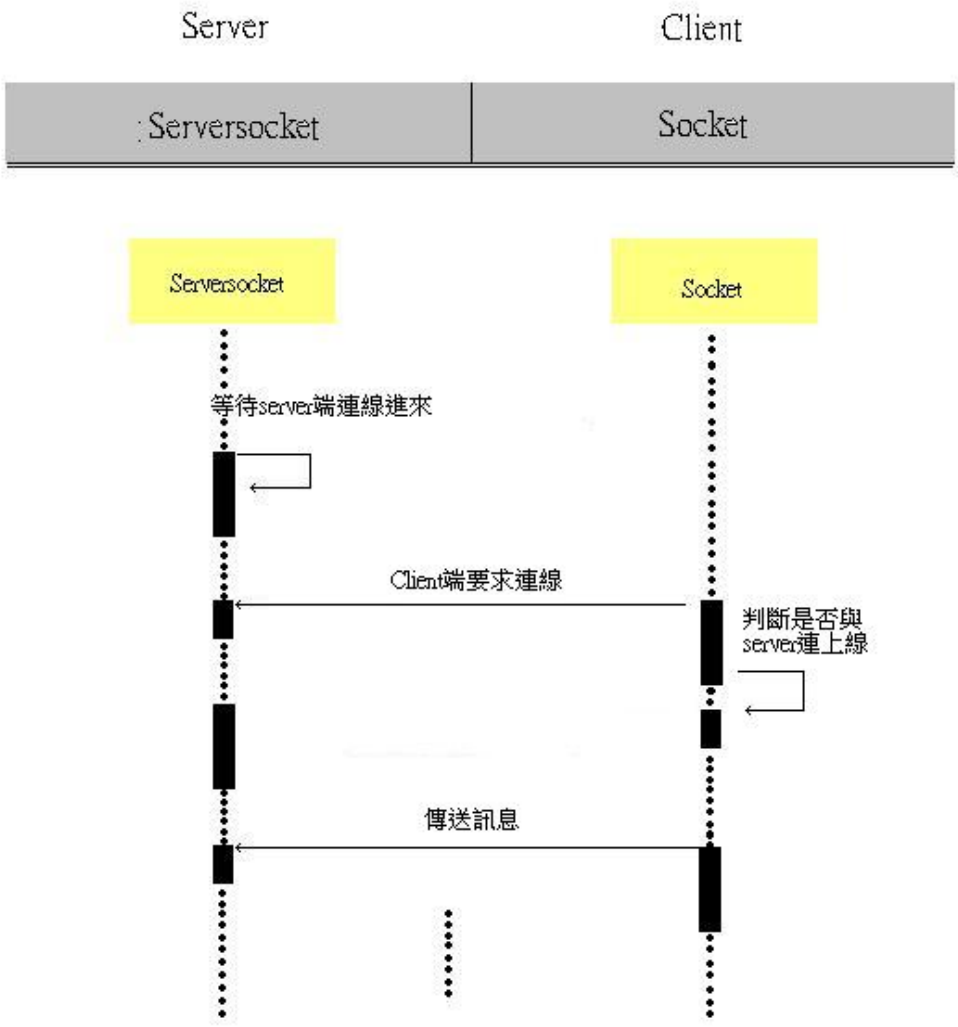


圖 3.2 Server 與 Client 的連線過程

3.2 設定環境架構

在無線網路環境下，各個 Client 端以及 Server 可自由溝通，Client 端也可透過無線網路傳輸投影片給 Server 端，再經由 Server 端傳送到單槍撥放，而 Server 與單槍之間是用線路連接，單槍不用無線傳輸的原因是因為，目前雖然也有出現無線網路機制的單槍，但是由於單價太高，因此站在消費者的角度，我們的系統可以節省開支。

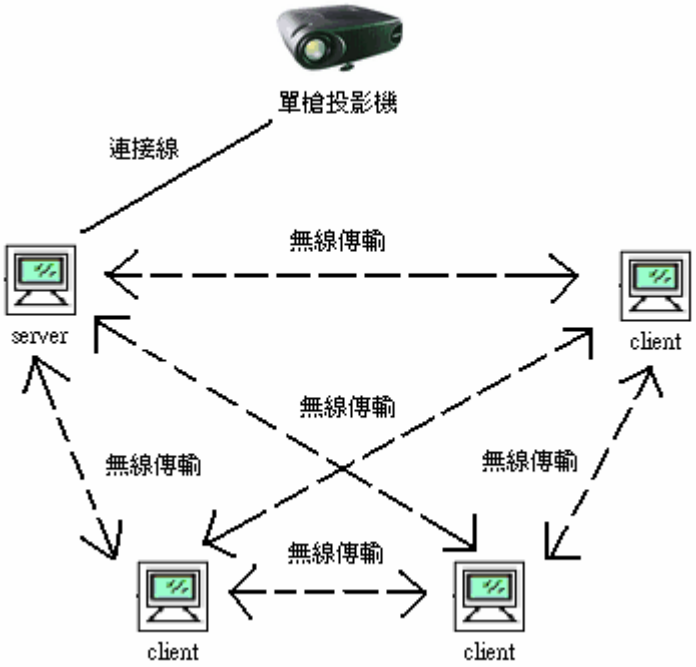


圖 3.3　環境示意圖

3.3 主從式架構

3.3.1 Client/Server 介紹

主從式架構解決了專用伺服器架構中存在的不足，Client 端既可以與 Server 端進行通信，同時用戶端之間也可以進行直接對話，而不需要伺服器的仲介和參與。

在主從式的架構之中，在 Client 端未發送訊號給 Server 端時，之間並不會有什麼連線狀態或是資訊的交流，當我們 Client 端傳訊息到 Server 時，Server 端就會建立一個連線的橋梁，連接兩個 Client 端，讓他們能相互通訊。此種架構的特色在於，只有當 Client 端送出要求的時候，Server 端才會傳送資訊給 Client 端，也就是說當沒有任何要求傳出去時，伺服器端和 Client 端之間完全沒有連線，Server 不會主動送資訊給你，所以可以大幅的減少網路的負荷量。下面的圖為基本的主從式構造圖：

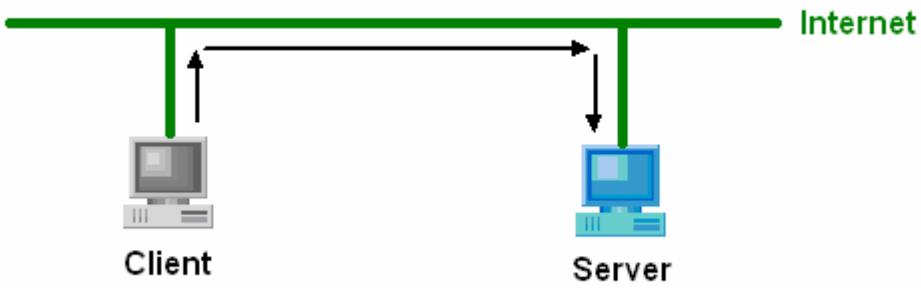


圖 3.4 client 端向 server 送出請求

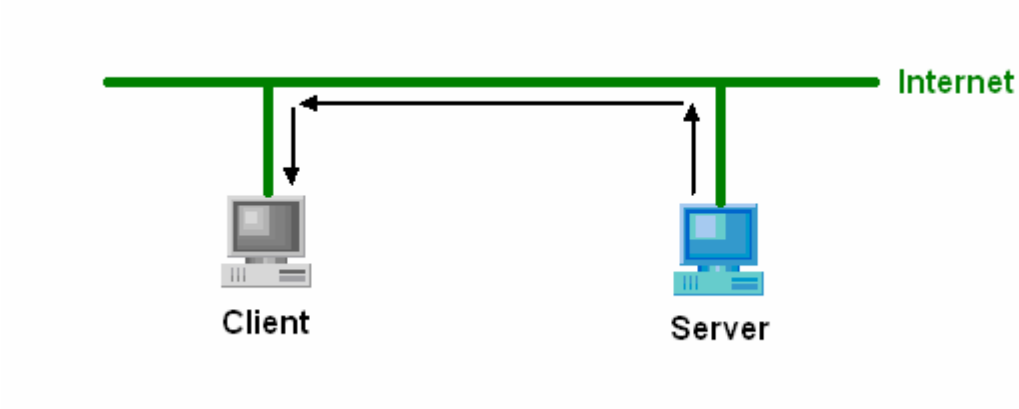


圖 3.5　server 回送結果給 client 端

3.3.2　Client/Server 特性

主從式架構的特性有以下幾點：

- 資源分享
- 開放性系統架構
- 擴充性高：系統可以依組織或環境的需求，不斷擴充其功能。
- 平行運算：平行運算能夠結合多台電腦主機功能(或個別單機處理)，處理複雜大量的資料，並加速完成每個案件，效率極高。
- 容錯性：其中一台損壞，其他電腦仍可支援運作。
- 透通性(Transparency)：對於 User 而言，整個系統使用起來，就像是只有一台電腦而已。
- 具親和力的使用者介面：透過適當的分工處理，Client 端的應用程式可以呈現更精緻的畫面給使用者，而後端的 Server 則專注於更高效率的執行處理，包括資料的存取、系統的管理以及安全性的防護等。

3.4 Client/Server 實際運用

在專題的製作中，我們所使用的主從式架構，為多(Client)對一(Server)的架構，在使用此系統時，需要由一台電腦當作伺服器(Server)端，可由視窗上的工具列來選擇作為 server，至於其餘的電腦，則選擇當作客戶(Client)端。在程式碼的撰寫時，由於考慮到投影片會議可能會因為 Server 端的電腦故障而中止，所以此程式的功能可以使任一台 PC 或 NB 由 Client 轉換成為 Server 端，如此一來在 Server 端故障時，即可用另一台電腦作替換，接上單槍後即可作使用。當電腦啟用 Server 端的功能時，電腦將自動的抓取所在位置的 ip，並可自行設定密碼，只讓知道密碼的使用者做登入。

實作多對一網路架構：

- ☐ Server 端會與每個 Client 端溝通
- ☐ 然後所有 Client 端之間也都彼此連線
- ☐ 實作小型聊天室

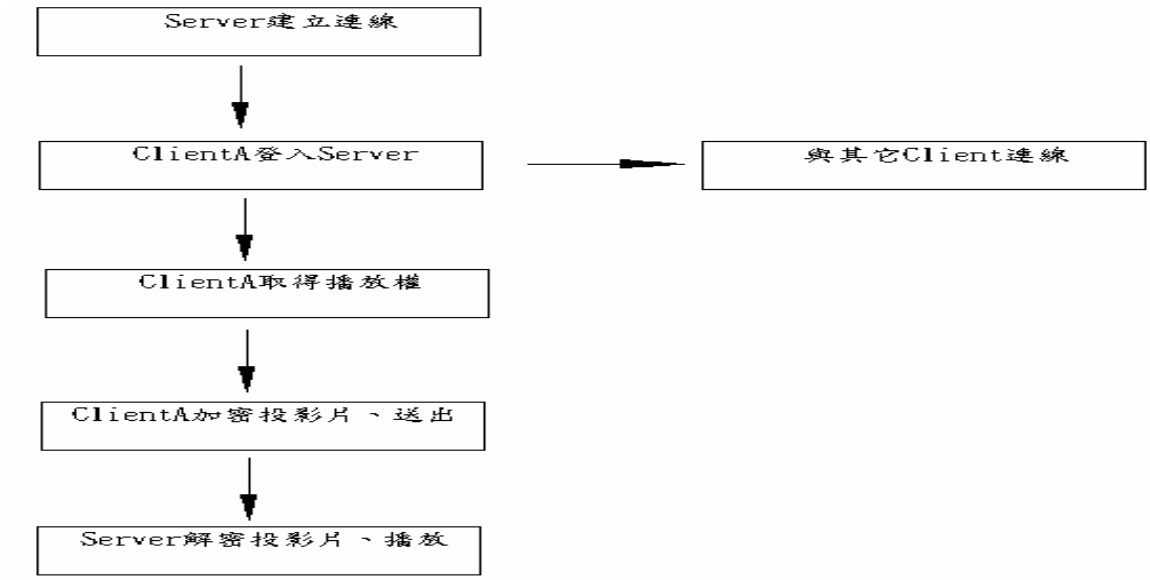


圖 3.6 server/client 實作流程圖

3.4.1 Server/Client 之間的傳訊

在此專題的 Server/Client 架構中，一開始 server 要先登入，開 port 4000 讓其他人登入，再來如果有人登入，server 會 new 1 個 thread 去服務他，然後 client 會送自己的"名字"跟"ip"給 server，之後 server 會把名字跟 ip 存起來。

如果又有一個人登入了，server 會 new 1 個 thread 去服務他，然後 client 會送自己的"名字"跟"ip"給 server，之後 server 會把名字跟 ip 存起來，然後 server 會把所有存起來的"ip"傳給所有的 client，然後當 client 收到 server 送來的 ip 會存起來，然後分別連線進去其他 client 且送"名字"跟"ip"給別人，然後別人也會把其他人的"名字"跟"ip"存起來，如此就可 1 對多連線，所以線上名單才會有其他人的"名字"跟"ip"。

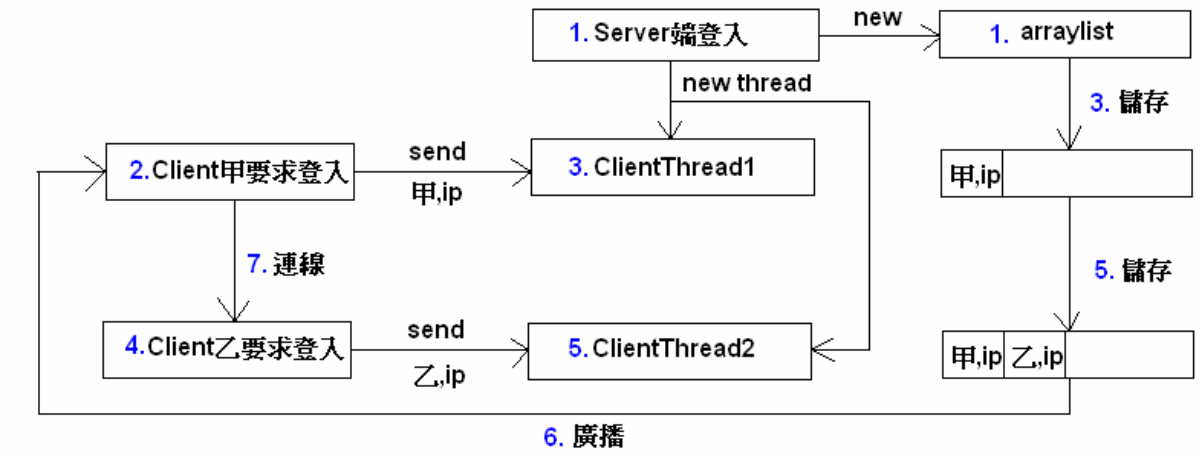


圖 3.7　server/client 傳訊步驟

3.4.2 client 和 server 之間的資訊傳遞功能

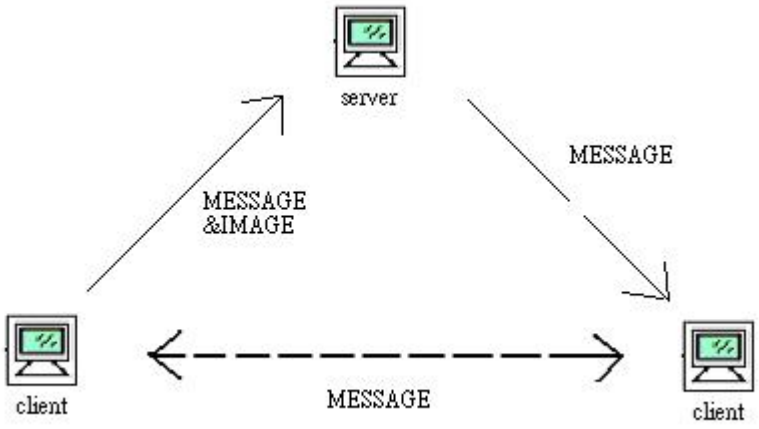


圖 3.8 client 與 server 之間的資訊傳遞圖示

●client對server可以傳message和image

●client對client只能傳message

●server對client只能傳message

第四章　加解密的原理與實作

4.1　密碼學(Cryptology)簡介

密碼學(Cryptology)一字源自希臘文"krypto's"及"logos"兩字，直譯即為"隱藏"及"訊息"之意。而其使用，可以追溯到大約四千年前。公元二千年，埃及人就將祭文刻在墓碑上。之後人們都是以書寫在紙張上的方式，用來傳秘密訊息。在二次大戰中，密碼更是扮演一個舉足輕重的角色，許多人認為同盟國之所以能打贏這場戰爭完全歸功於二次大戰時所發明的破譯密文數位式計算機破解德日密碼。西元 1949 年，Shannon 提出第一篇討論密碼系統通訊理論之論文，近代密碼學可說是濫觴於斯。直至西元 1975 年，Diffie 與 Hellman 提出公開金匙密碼系統之觀念，近代密碼學之研究方向，正式脫離秘密金匙密碼系統之窠臼，蓬勃發展，至今已近二十年。發展至今，已有二大類的密碼系統：一為對稱金鑰(Symmetric Key)密碼系統，二為非對稱金鑰(Asymmetric Key)密碼系統。

4.1.1　對稱金鑰密碼系統(Symmetric Key Cryptographic System)

對稱金鑰(Symmetric Key)密碼系統也就是傳統保密系統，使用的是對稱加密演算法(Symmetric Cryptographic Algorithm)，即加密端與解密端均要使用同一把金鑰(即 Secret Key)，其優點是加解密的速度快。在對稱金鑰密碼系統中最著名者為 DES(Data EncryptionStandard)，也是我們此系統所使用的演算法。

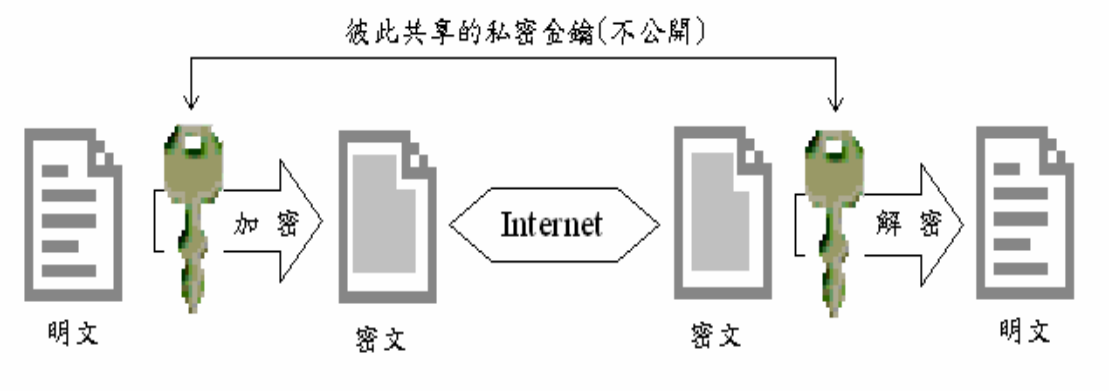


圖 4.1　對稱金鑰密碼系統

4.1.2　非對稱金鑰密碼系統 (Asymmetric Key Cryptographic System)

非對稱金鑰密碼系統是使用非對稱加密演算法(Asymmetric Cryptographic Algorithm)，加密端與解密端使用不同的金鑰。這兩個不同金鑰，一個為私密的解密金鑰(Private Key)由擁有人自行保存，另一個為可以公開的加密金鑰(Public Key)，兩個金鑰彼此配對使用，稱為「金鑰對」(Key Pair)。而非對稱金鑰密碼系統的金鑰對有兩種：

1. 數位簽章金鑰對(Authentication Key Pair)：

「私密金鑰」用於產生數位簽章。

「公開金鑰」用於驗證數位簽章。

2. 資料加密金鑰對(Confidentiality Key Pair)：

「公開金鑰」用於資料加密，資料加密與資料解密使用不同的金鑰，例 RSA、DSA。以公開金鑰(Public Key)加密，以私密金鑰(Private Key)。

「私密金鑰」用於資料解密，以私密金鑰(Private Key)產生簽章，以公開金鑰(Public Key)驗證簽章。

運算速度慢是非對稱金鑰密碼系統的缺點，所以不適合加密內容較大之訊息，與對稱金鑰密碼系統相比，加密部分大概慢了一千多倍。非對稱金鑰密碼系統例如 RSA(Rivest-Shamir-Adleman)演算法。

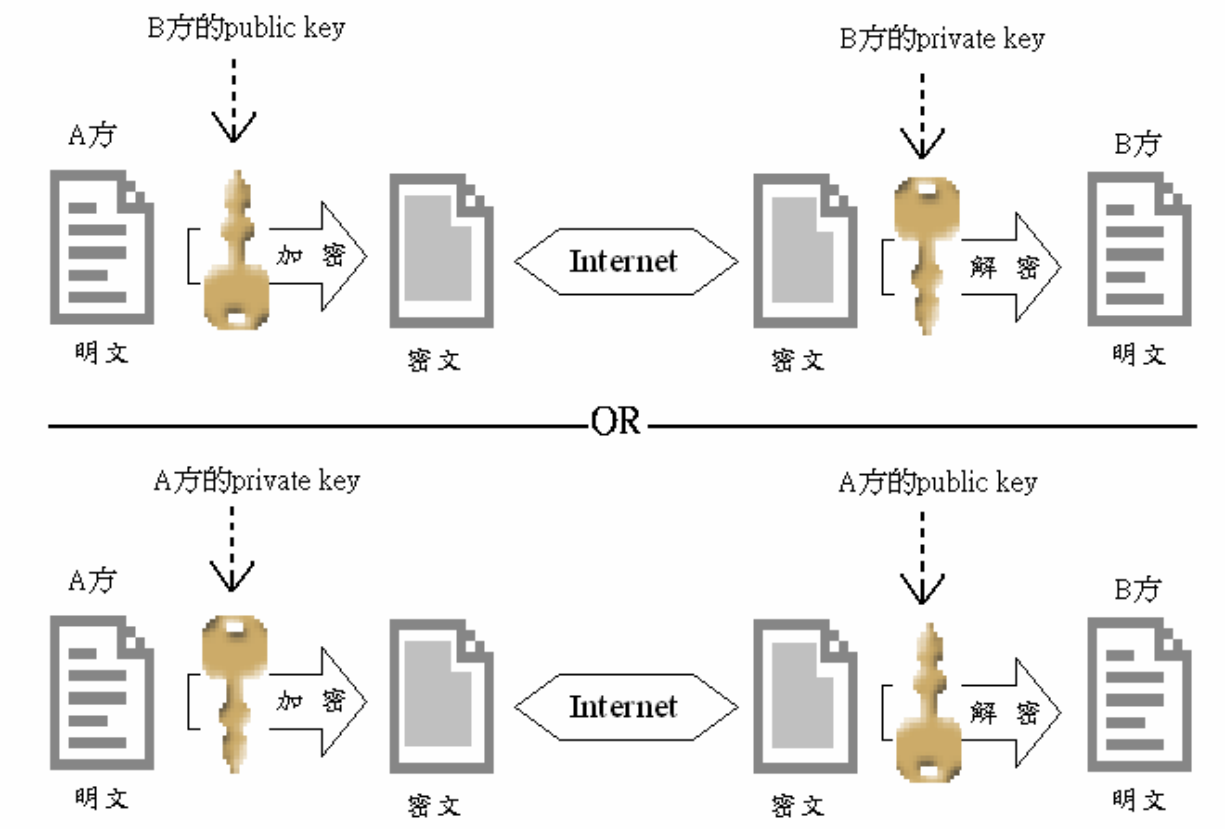


圖 4.2　非對稱金鑰密碼系統

4.2　使用技術介紹

我們加解密的工具為 JAVA 的 JCE(Java Cryptographic Extension)API，它可以實施多種類型的加密和其他涉及安全的任務。而我們專題中使用的加密演算法為 DES，比起其它的演算法，它擁有較快的處理速度，故在撥放投影片時不會產生嚴重的 delay，以達順利、流暢的目的。

4.2.1 DES 演算法

DES(Data Encryption Standard)，1970 年代中期由美國 IBM 公司發展出來的，且被美國標準局公佈為資料加密的標準。DES 屬於對稱金鑰密碼系統的區塊加密法，而區塊加密法就是對一定大小的明文或密文來做加密或解密動作，DES 所用的 KEY 長度是 64 位元大小，但因其中 8 位元用來做錯誤更正，所以真正加密的長度只有 56 位元大小。設計原理源起於 Shannon 的乘法保密系統(Product cipher)觀念，在運算推導過程中利用混淆(Confusion)與擴散(Diffusion)、切割分散的功能使得明文在運算的階段中一次又一次互換位置(查表)及增加(查表填位)、減少位元數(二進位轉十進位、查表)，經過 16 次的運算處理從事加、解密的工作。

4.2.2 加解密的過程

1. 產生 key

由於 DES 的缺點就是只有一把 Key，如何將 Key 安全的傳送到其他使用者身上，是很大的問題。因此我們不直接在程式中產生 Key，而是自己輸入 Key。

```
1. desKeySpec = new DESKeySpec(desKeyData);
2. keyFactory = SecretKeyFactory.getInstance("DES");
3. desKey = keyFactory.generateSecret(desKeySpec);
```

上段程式碼中 desKeyData 為使用者輸入的 Key(已轉為 byte)。desKeySpec 的唯一用途就是對 Key 進行分組(並為它們提供型態安全性)，在此將 Key 歸類為 DES 使用的型態。SecretKeyFactory 再將 desKeySpec 產生成真正 DES 加解密時的密鑰。下面是產生 DES Key 的流程圖:

圖 4.3　key 的產生流程

2. 產生 Cipher

Cipher(加解密器)就是用來將資料加解密的函式，首先必須設定它的參數:

```
des = Cipher.getInstance("DES/CBC/PKCS5Padding");
```

1　2　3

(1) **演算法型態**

提供 AES、DES、RSA 等演算法，因為我們使用的是 DES 演算法，所以在這裡參數設為 **DES**。

(2) **Mode**

提供 CBC(Cipher Block Chaining)、ECB(Electronic Codebook)、CFB(Cipher Feedback)…等模組，ECB 是 Cipher 中最簡單的模組，但缺點是若用同一把 key 加密相同的原始文字，所得出的加密文字區塊是相同的，因此如果區塊的重複性高，容易被解碼專家解讀；而 CFB 可以讓區塊式 Cipher 變得像是串流式 Cipher 一樣運作，但是效率不高；所以我們使用 **CBC** 區塊連鎖模組，每一個原始資料區塊都會用 XOR 運算和前一個區塊的加密資料合併，運算結果經過加密之後變成加密文字區塊，CBC 不但克服了 ECB 易被破解的缺點，效率也比 CFB 來的高。

(3) Padding

在加密的過程中，資料會被切成 64 位元區塊，加密後再輸出，但是資料尾端不一定能放滿 64 位元的區塊，因此用 Padding 將區塊補滿。在資料解密時，將 Padding 的部分移除，便可以還原成原來的資料。舉例來說，假如區塊大小為 8byte，而資料的區塊只有 4byte，則會補上 4byte 的資料變成 8byte。如下圖：

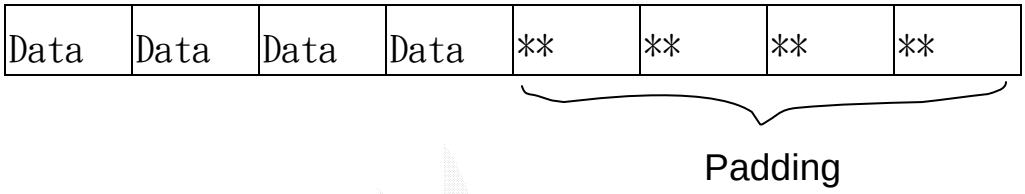


圖 4.4 Padding

設定完參數之後，就可以初始化 cipher，在這裡必須設定要做加密或是解密的動作，還有加密時所使用的 key(上一小節中產生的 key)，如下所示：

key

```
des.init(Cipher.ENCRYPT_MODE, desKey);      //加密
des.init(Cipher.DECRYPT_MODE, des_Key, ivps);      //解密
```

我們所設定的 IV(initialization vector)，用來和第一個區塊的原始資料做合併

3. 資料的加解密

```
fin_s=new    FileInputStream(path);
CipherOutputStream cout=new CipherOutputStream(fout_s,des);
```

上段程式碼在 Client 端中，CipherOutputStream 是一個加密器，fin_s 讀檔進來,透過加密器處理,輸出加密檔，然後以串流送出。

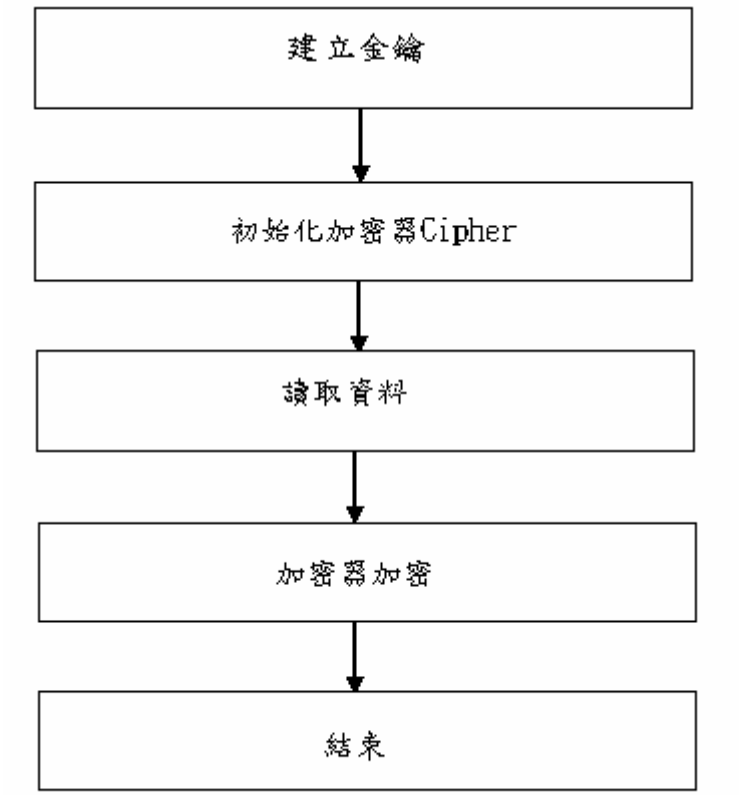


圖 4.5　加密流程圖

而在 Server 端，則是接收串流之後，讀入加密檔，被同樣的 IV 向量初始化，再透過 CipherInputStream 解密器解密，最後移除資料尾端的 Padding，輸出資料並 show 出圖片。

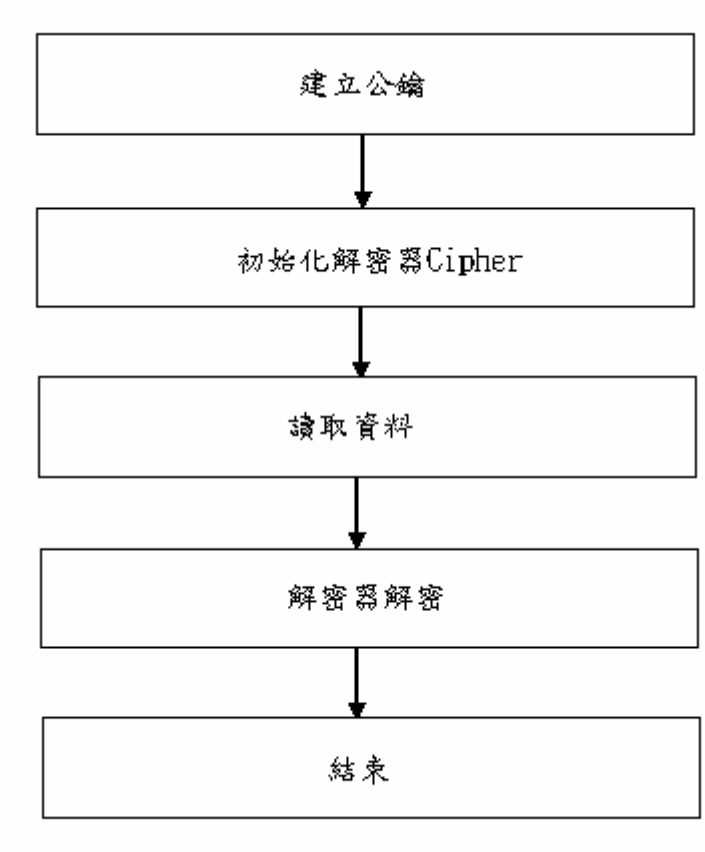


圖 4.6　解密流程圖

第五章　軟體未來發展的可行性與心得感想

5.1　軟體未來的發展

關於我們目前的這個軟體發展，我覺得未來的擴展性很大，因為就功能性來說的話，就可以擴充很多方面了，下面將列出並討論軟體的未來發展可能性：

1、 在傳送速度的部份：如何讓資料傳輸時，可以將資料作最有效的壓縮，好讓傳送的流程更加的快速，在軟體方面盡可能的作可能的改善

2、 在投影片的放映部份：因為在作簡報的報告前，必須先將每個投影片的檔名依數字作排序，在這個時候就必須人工的去作檔名的更改，也許未來作簡報播放時，能夠依放入資料夾的時間順序，或是有辦法先將簡報用程式先作檔名上的處理，這麼一來就可以更加輕鬆的完成播放前的動作了。

3、 資料安全的部份：在這次的專題之中，我們是選用 DES 來作加密的動作，但光只是 DES 的加密方法來說，對於防止資料被人解密的安全性來說是有限的，所以說若能找到更好的方法來作加密，這樣的話才能夠安心的作機密性的簡報報告，而不會有安全性不足的問題。

4、 關於簡報發表時的方便性：對我們這次的簡報系統來說，其中有個問題就是，當 client 的子畫面傳送到 server→單槍投影機後，投影的大螢幕上只會出現子畫面的畫面而已，就算當時滑鼠的軌跡在子畫面上移動，也不會抓到滑鼠的軌跡，所以在報告時想要說明重點的部份時，就必須要借助一

下其他的輔助工具，如紅外線筆等來作重點提醒，也就是因為如此，所以有想到開發軟體的功用來代替輔助工具，像是如畫筆的功能，可選擇合適的顏色來作重點的提醒，在畫上去的幾秒內，畫過的痕跡會自動消失，這只是其中一個想法，總之能作到完全只從電腦上報告完整個簡報，會是個不錯的目標。

5.2 心得感想

這次的專題的題目是老師給的，加上同組的組員對網路方面的題目都很有興趣，所以便開始著手於這個專題上面了。這次的專題是自己依照著興趣去實作，一開始完全沒有方向真的不知道要如何著手，該用什麼語言好？用到哪些套件？該了解哪些東西？在書上所獲取的相關資源有限，因此多半時間都是在網路上搜尋資料，開始的那段期間進展非常慢，曾經試著要利用其他的方法去達成我們的目標，畢竟許多套件都是我們沒有碰過的，究竟哪一種能夠完全符合我們的要求，做成我們想要的東西，實在無法肯定。感覺上好像走了很多冤枉路，其實並不然。也因為這個機會多認識了好多的東西，像是國外有個軟體跟我們要做的專題十分相似，只是他們是使用雙輸出的顯示卡，價錢頗高，因此放棄這個方法，不過卻也給了我們很大的信心，相信專題一定可以完成成品。後來上 JAVA 網站上尋找資料，也透過老師、助教的指導，才有一個方向遵循。

當初開始在作的時候，會覺得自己想的還蠻理想化的，認為很多想加進去作的事情應該不是很難作，但實際去做了之後，反而會覺得不知所措，因為有時腦子裡所認為的東西，寫進去電腦後，所帶來的作用跟想像的不太一樣，還好多虧了小組組員和其他善心人事的幫助下，才使得事情慢慢的有所斬獲，也看了許多的書籍後，才懂得一些小小的心得和原理，在找尋資料的過程當中，學習到了許多以往較少接觸到的東西，覺得學習到東西才是這次專題的重點，該如何去尋找資料，判斷資料是不是有用，這次專題都是很好的學習經驗。畢竟新的東西實在太多，當初在 JAVA 的網站尋找資料時，看到很多沒有碰過的套件，實在覺得滿震撼的，原來這麼多的東西我都不會，甚至不知道是用來做什麼的。指導老師-李維斌，也常告訴我們，市面上的書都

是舊的知識，你會別人也會，而新的、別人不會的東西都在網路上，要試著去學習它們提供的說明。當新的東西出來時，你才會具有競爭力，因為你已經嘗試過學習一個未知的東西，相對的你也有辦法去學習這次的新東西。這期間我們看了很多 Java 提供的 API Documentation、Programmer’s Guide，也在討論區中找尋相關的文章，甚至去問發表文章的人，進而學習他們的實作經驗。

總之當我們再去學習一樣新的東西時，我們已經有經驗知道該如何去尋找資料，該如何學習，怎麼分析規劃整個系統。也懂得如何互相討論，互相分工合作，來達成我們的目標，在整個過程之中，覺得最重要的還是分工相互合作，相互打氣加油和督促，分工合作使得得到的成果更加的美好。

參考資料

[1] 精通 Java Swing，林智揚、范明翔、陳錦輝 編著，金禾資訊，2002 年 12 月初版四刷

[2] JAVA I/O 與通訊介面，蕭明城、周岱琳 著，金禾資訊，2002 年 9 月初版一刷

[3] JAVA 程式設計，鄧永亥、楊錦文、謝金興 編著，金華出版

[4] 關於Client/Server主從式架構 http://master.mis.npust.edu.tw/~m8756004/mis-paper/distribute.htm

[5] JAVA 語言官方網站 http://java.sun.com./

[6] JSPtw.com http://www.jsptw.com/jute/

[7] The Java™ Tutorial，A practical guide for programmers http://java.sun.com/docs/books/tutorial/

[8] 網路與通訊-淺談主從式架構，作者：許憲忠 http://www.ascc.net/nl/84/1109/03.html

[9] Java Cryptography Extension1.2.2 http://java.sun.com/products/jce/doc/guide/API_users_guide.html

[10] JAVA 密碼學，作者：Jonathan Knudsen，O' Reilly 出版

[11]近代密碼學及其應用，作者:賴溪松、韓亮、張真誠，松崗出版

[12]Microsoft PowerPoint 簡報-密碼學重要觀念
http://www.sna.csie.ndhu.edu.tw/~cnyang/HA/sld014.htm
[13]Taica 台灣網路認證-教育園地
http://www.taica.com.tw/education/ca-1-1.htm

附錄 A

操作手冊

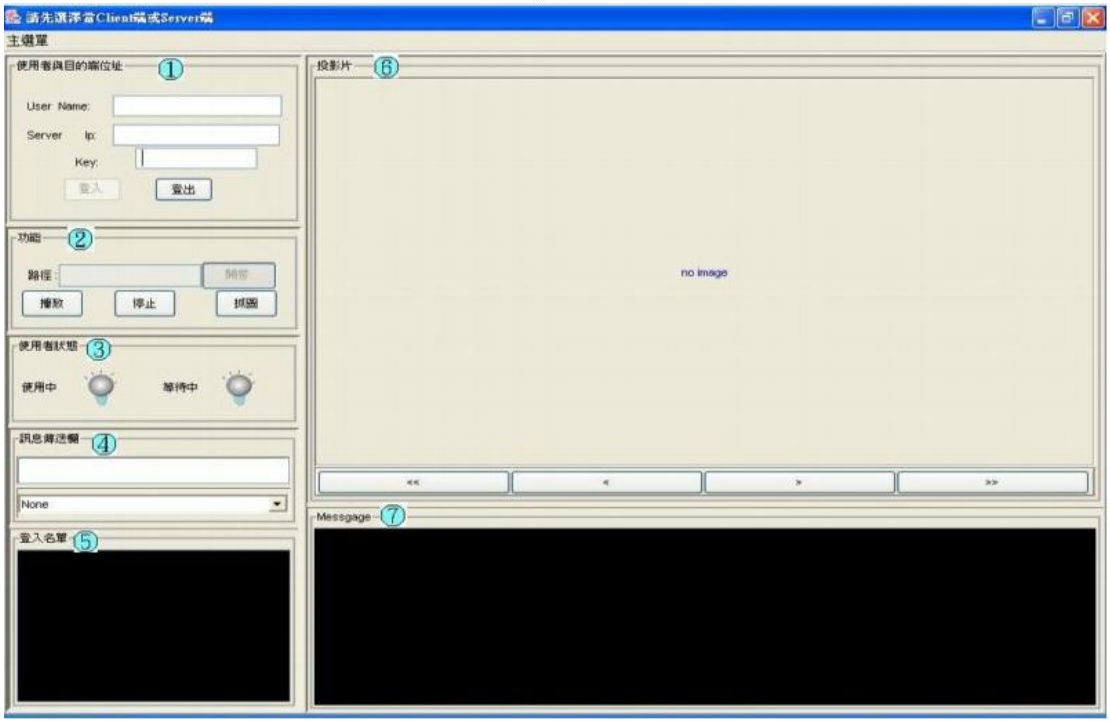
一、在 JavaBuilder 下開啟程式：

1.使用者需要安裝 JBuilder 工具及 JDk1.4.1(內含 JCE 套件)

2.一開始先到開一新專案(File→New Project)，然後再以開啟舊檔方式(File→Open Project)，開啟程式中的 project.jpx 檔。

3.開啟後在 Client4 上按右鍵→Run Using Client 即可將整個程式作開啟的動作，之後就可以進入系統介面了。

二、軟體操作需知：



上圖為介面標示號碼圖，除了主選單未標示號碼，其餘有 1~7 的數字作標示，在下面會作一一的介紹：

◎主選單：可選擇要當 client 或是 server 端，client 和 server 端的不同點在於，當你以 server 端進入時，(介面標示號碼上)ip 位址將自動抓取目前電腦已設定的 ip，而 client 端

則要輸入 server 端的 ip 才能作登入的動作。

①使用者與目的端位址：有 username，server ip 及 key。

●Username：可使用英文作個人的代號，如 yifung、kotoway。

●Server ip：在主畫面選擇 Server 的狀態下可不用處理，若選●擇 Client 狀態，則要輸入 server 端的 ip。

●Key：輸入 Server 端所設定的密碼用，輸入錯誤則會造成無法登入的情況

輸入上面三者即可作登入的動作，並開啟投影片和傳訊的功能。

②功能：有開啟、播放、停止、抓圖四個選項。

● 按開啟時，就如同一般 windows 的開啟功能，可在此選擇想要播放的圖片。

● 按播放時，會讓”使用中”的燈由綠轉紅，作圖片播放的動作，可由按鍵作向前向後的操作。

● 按停止時，可讓播放的動作停止。

● 按抓圖時，此時會開啟子畫面，並將子畫面的圖片傳到 server 端去。

③使用者狀態

有使用中及等待中兩種，未登入前為灰色，登入後為綠色，正在使用的播放者，使用中的燈會以紅色表示之。

④訊息傳送欄

可傳送文字訊息給其他電腦，作為聯絡溝通用途。下方有一下拉式工具列，可作與全部的人對話或是對特定人物的對話。

⑤登入名單

每當使用者登入後，會顯示出 username 以及其 ip 位址。可作線上人物查詢用。

⑥投影片

下方有四個鍵：”<<” 、”<” 、”>” 、”>>” ，由左到右的功能分別為：到第最前頁、上一頁、下一頁及到最後頁。

⑦ Message

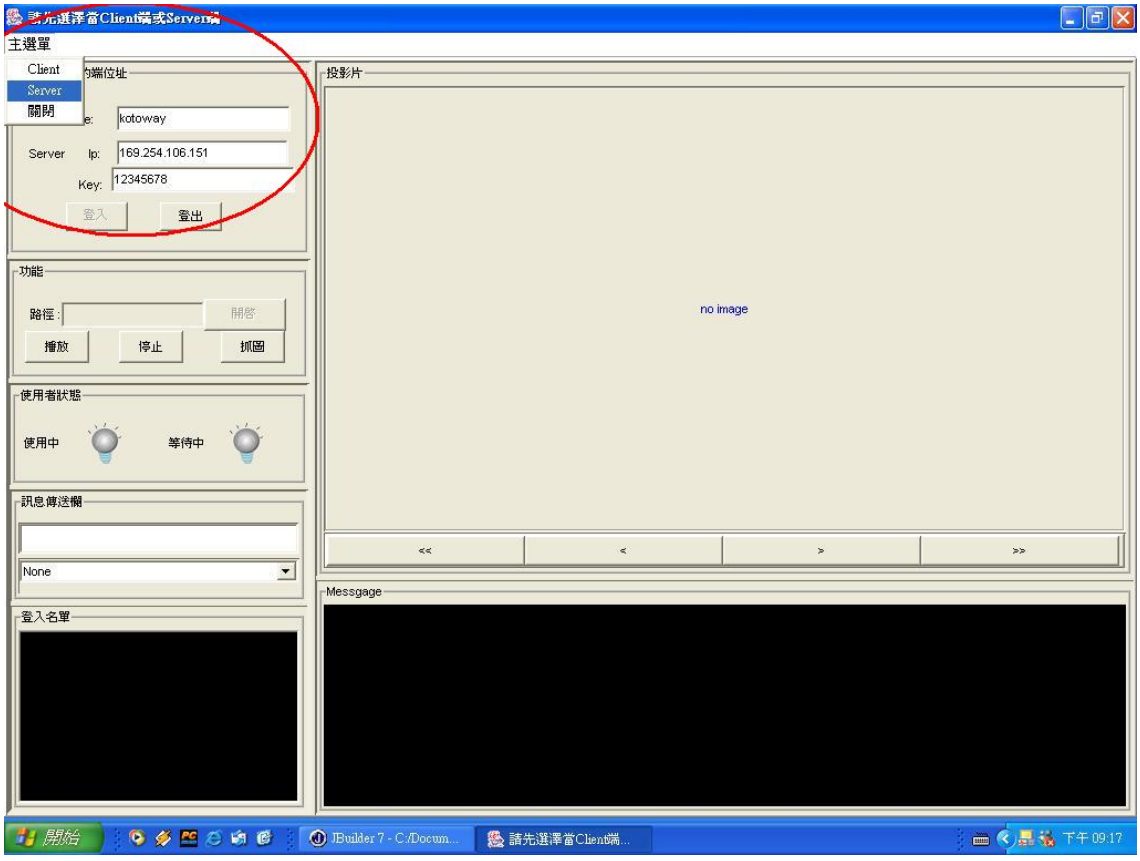
會顯示 user 的各種動作狀態，如登入、登出、傳送等訊息……。

附錄 B

專題實作過程實錄

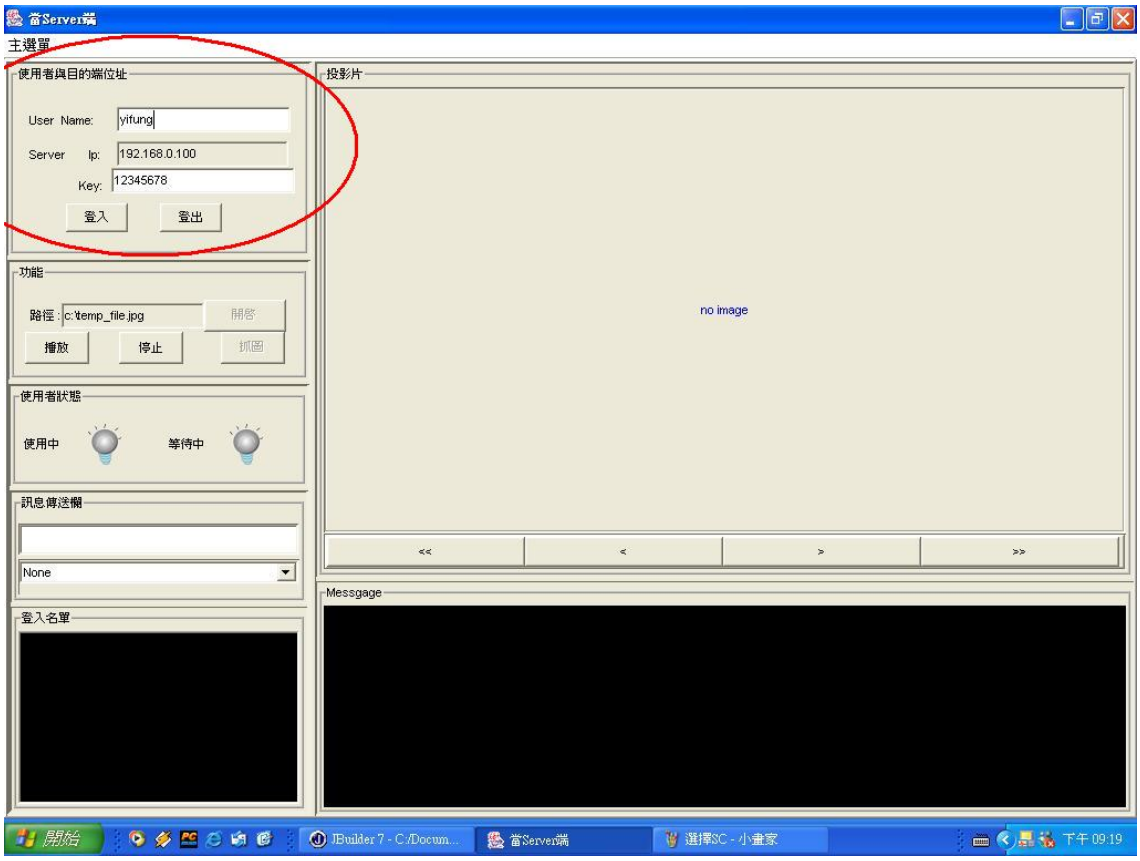
1. 決定 Server 端及 Client 端

在程式的一開始執行時，可在視窗上方的”主選單”中，選擇此台電腦在作簡報時所要擔任的角色，可選擇作為 Client 端或是 Server 端，亦可作視窗的關閉。



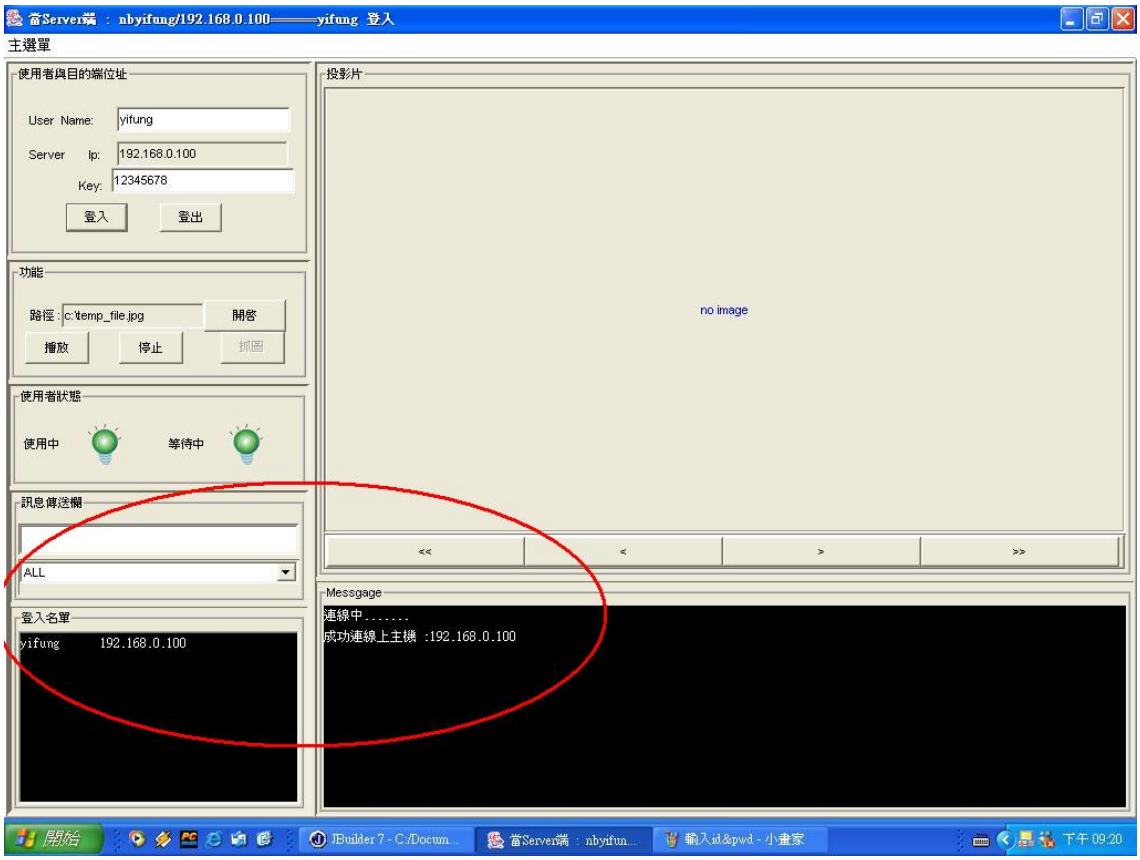
2. 使用者登入

在選擇作為 Client 或 Server 端後，即可開始在”使用者與目的端位址”輸入 username，目標位置 IP(設為 Server 端的電腦會自動的抓取自己位置的 IP)，以及所設定的 KEY，即可按”登入”作登入的動作。

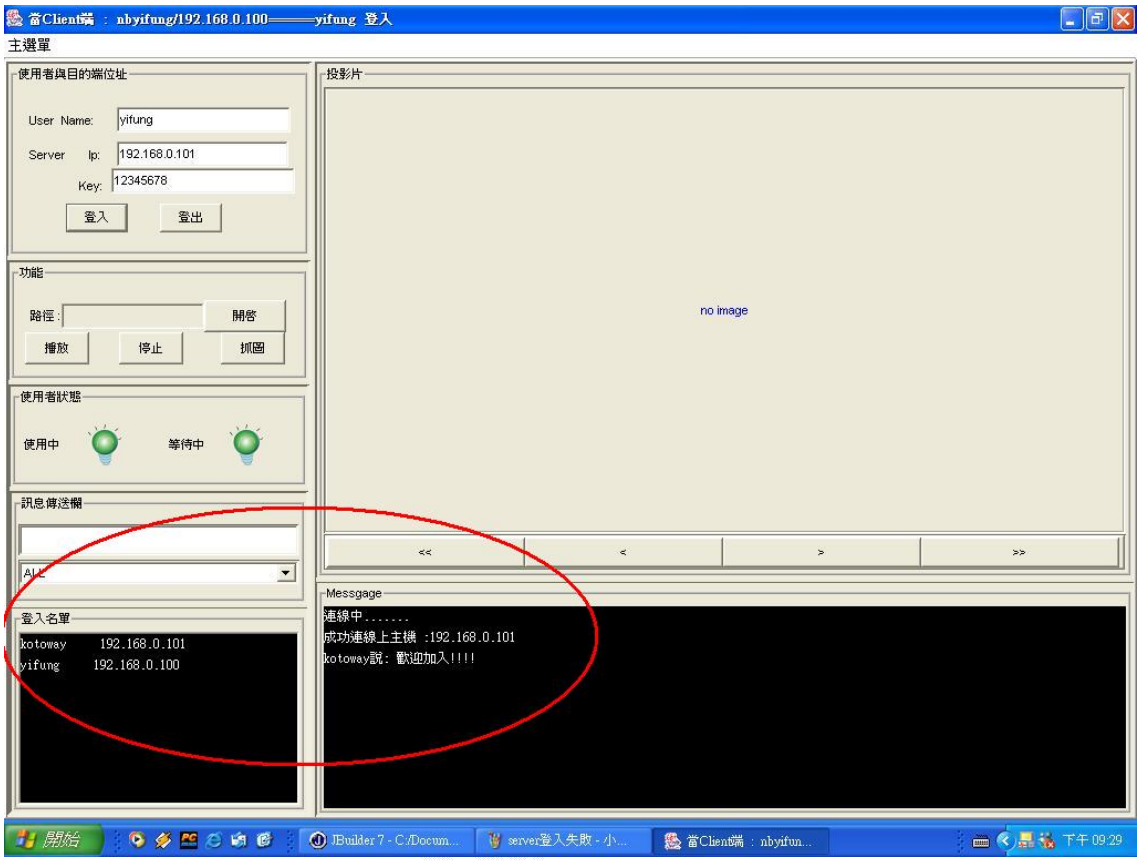


3. 登入成功

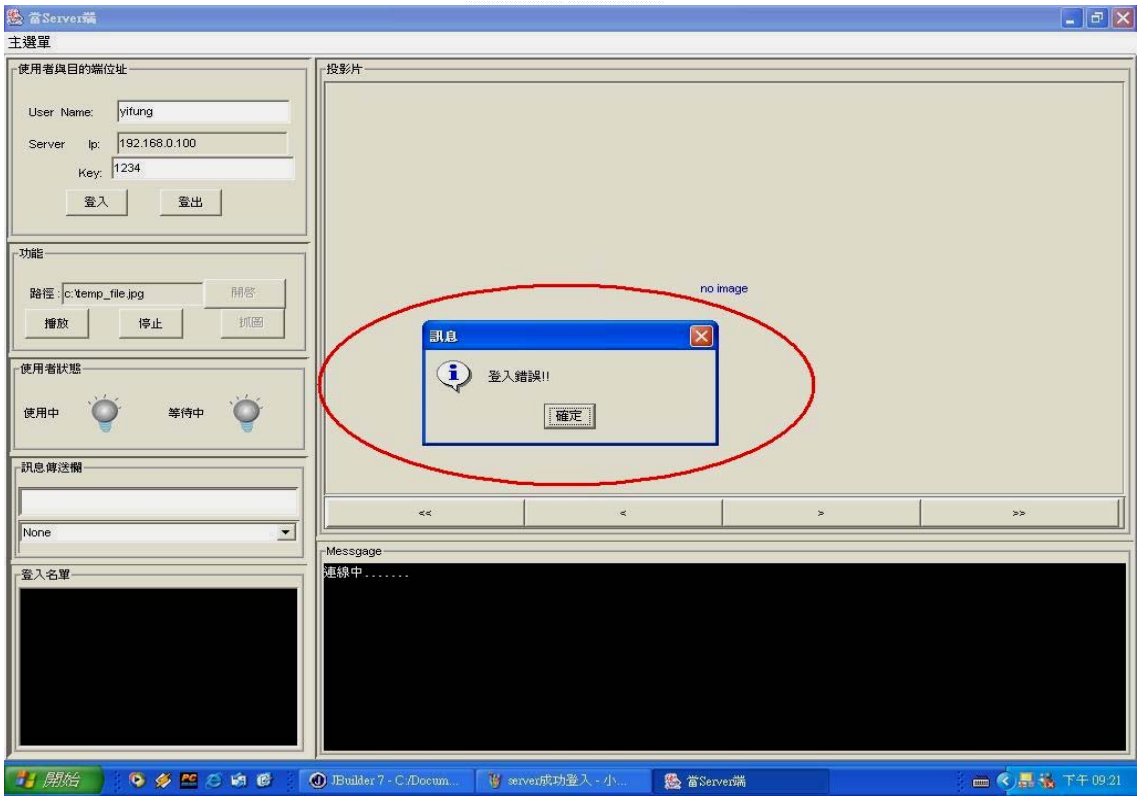
在”使用者與目的端位址”輸入 username 及 key 之後，便可按”登入”，此時”Message”欄便出現成功連上主機字樣，”登入名單”中也會顯示出登入的 username 以及其 ip 位址。下圖為 Server 端登入成功。



當程式作完登入的動作之後，在下方的”Message”欄將會顯示登入的訊息，在”登入名單”中，則會顯現出目前所登入的使用者名單，Server 端的使用者也包括在內。下圖為 Client 端登入成功。

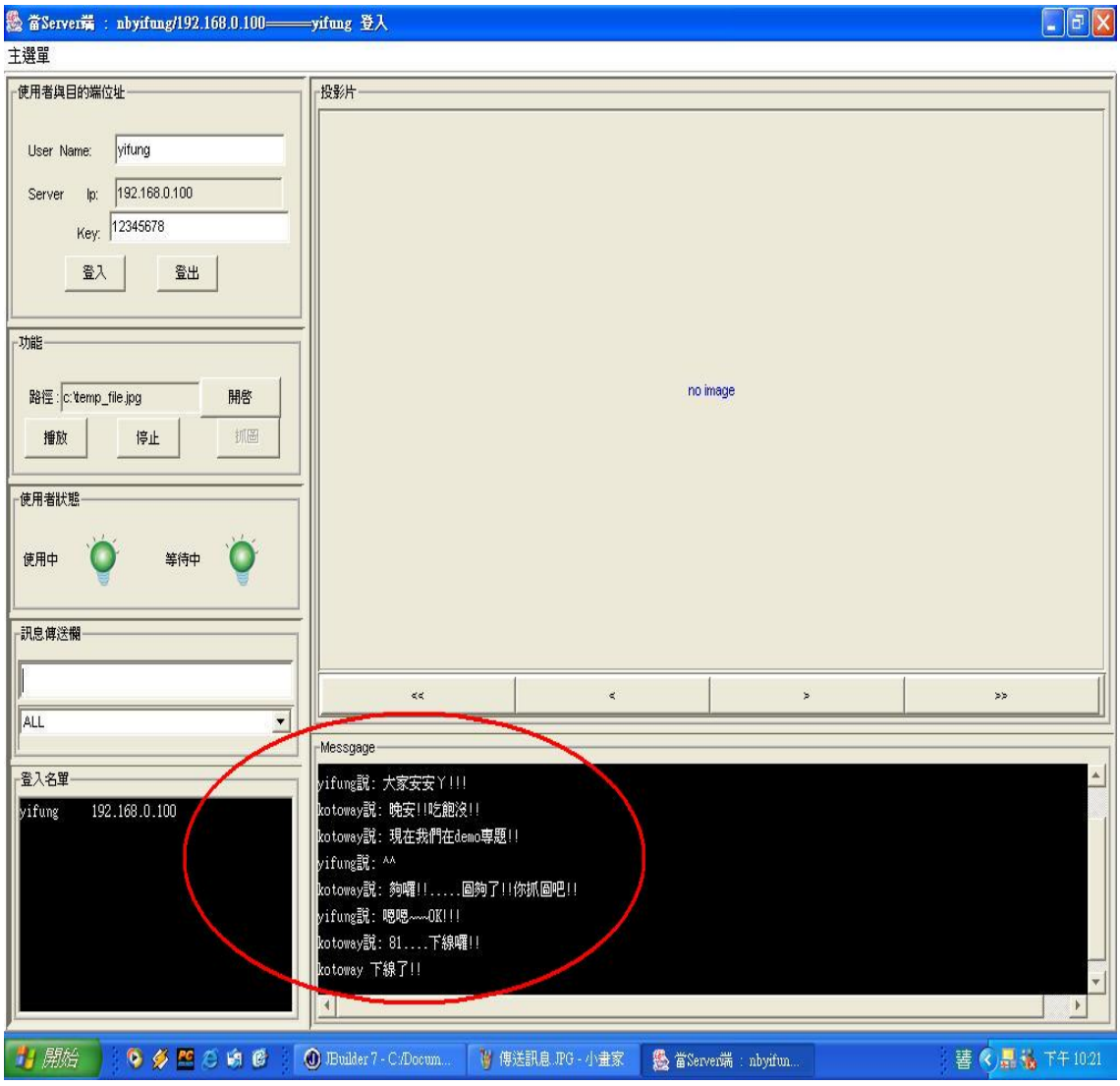

當Client端 : nbyifung/192.168.0.100——yifung 登入
主選單
使用者與目的端位址
User Name: yifung
Server Ip: 192.168.0.101
Key: 12345678
登入
登出
功能
路徑:
開啓
播放
停止
抓圖
使用者狀態
使用中
等待中
訊息傳送欄
ALL
登入名單
kotoway 192.168.0.101
yifung 192.168.0.100
投影片
no image
<<
<
>
>>
Messgage
連線中.....
成功連線上主機 :192.168.0.101
kotoway說: 歡迎加入!!!!
開始
JBuilder 7 - C:/Docum...
server登入失敗 - 小...
當Client端 : nbyifun...
下午 09:29

4. 登入失敗


當Server端
主選單
使用者與目的端位址
User Name: yifung
Server Ip: 192.168.0.100
Key: 1234
登入
登出
功能
路徑: c:\temp_file.jpg
開啓
播放
停止
抓圖
使用者狀態
使用中
等待中
訊息傳送欄
None
登入名單
投影片
no image
訊息
登入錯誤!!
確定
<<
<
>
>>
Messgage
連線中.....
開始
JBuilder 7 - C:/Docum...
server成功登入 - 小...
當Server端
下午 09:21

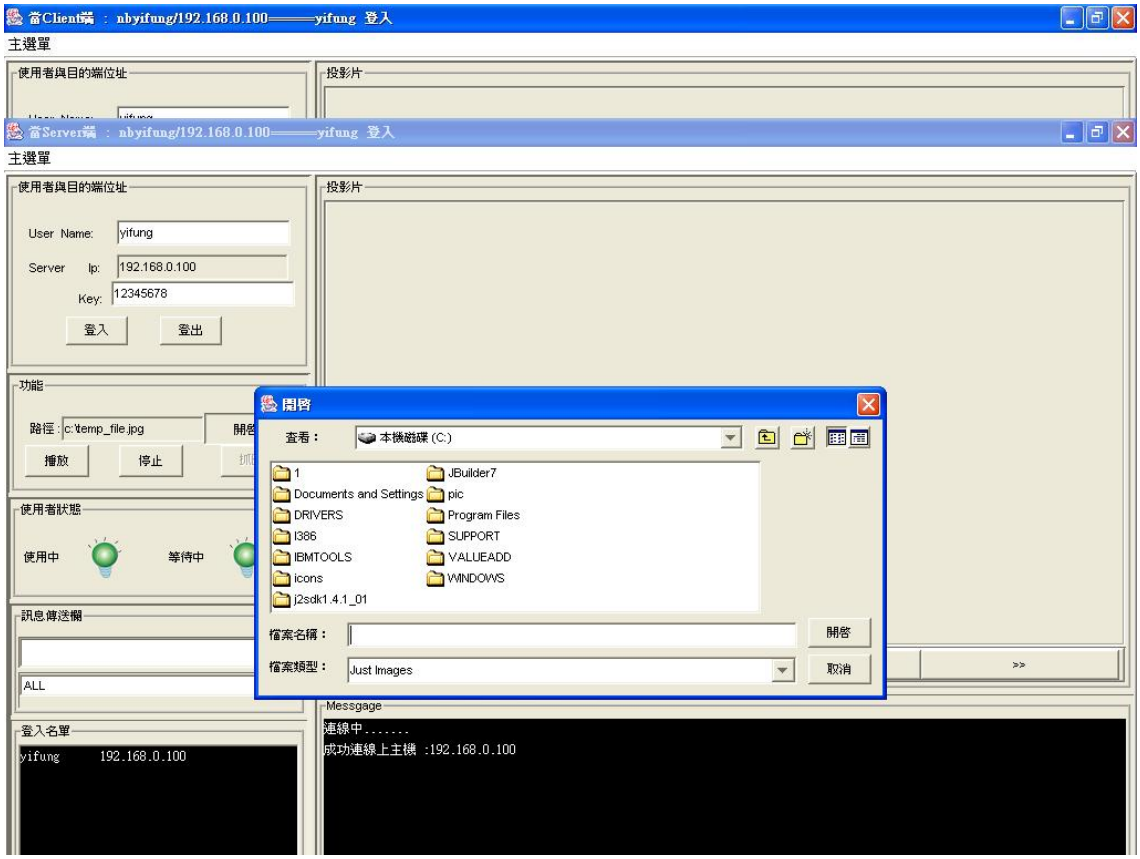
5. 線上訊息傳送

在”訊息傳送欄”中，可作傳送訊息的動作，下圖為一 Client 及一 Server 在作對話後的結果，其中也包括了 Client 的離線動作，在 user 離線後，”使用者名單”便只剩 Server 端的資訊。



6.撥放投影片(傳送圖片方式)

要作投影片的播放時，可由”功能”的”開啟”功能開啟，並開始選擇想要播放的投影片內容。



7. 投影片撥放中

當我們選擇好預備開啟的投影片時，便可在”功能”上按下”播放”來作投影片的播放，此時我們可以注意到，”使用者狀態”的燈炮由綠轉紅，表示正在播放中，Server 端將出現子畫面，子畫面便可經由單槍送到大型螢幕上。

8.撥放投影片(傳送螢幕方式)

此為 Client 端將圖片傳送到 Server 端後，所呈現的播放畫面，傳遞時間約 1~2 秒，此時單槍會擷取子畫面的內容作播放。