FINAL REPORT

SMART BICYCLE FLEET MANAGEMENT SYSTEM

FOR GREEN UNIVERSITY

ASST. PROF. DR. ISARA ANANTAVRASILP

ASST. PROF. DR. RONNACHAI TIYARATTANACHAI

FISCAL YEAR 2016

INTERNATIONAL COLLEGE

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

รายงานการวิจัยฉบับสมบูรณ์

ระบบจัดการจักรยานอัจฉริยะสำหรับมหาวิทยาลัยสีเขียว

Smart Bicycle Fleet Management System for Green University

ผศ.ดร.อิสระ อนันตวราศิลป์

ผศ.ดร.รณชัย ติยะรัตนาชัย

งานวิจัยนี้ได้รับทุนสนับสนุนงานวิจัย

จากงบประมาณเงินรายได้ประจำปีงบประมาณ พ.ศ. 2559

วิทยาลัยนานาชาติ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ชื่อโครงการ	ระบบจัดการจักรยานอัจฉริยะสำหรับมหาวิทยาลัยสีเขียว Smart Bicycle Fleet Management System for Green University
แหล่งเงิน	งบประมาณเงินรายได้ วิทยาลัยนานาชาติ
ประจำปีงบประมาณ	2559 จำนวนเงินที่ได้รับการสนับสนุน 400,000 บาท
ระยะเวลาทำการวิจัย	2 ปี 6 เดือน ตั้งแต่ 1 กันยายน 2559 ถึง 28 กุมภาพันธ์ 2562
หัวหน้าโครงการ	ผศ.ดร. อิสระ อนันตวราศิลป์
หน่วยงานต้นสังกัด	วิทยาลัยนานาชาติ

ABSTRACT

As transportation management is one of the six UI GreenMetric Criteria, many universities have provided bicycle fleets for their students and staff members for commuting within campus as a mean to reduce energy consumption and air pollution from motor vehicles. One of the common bicycle renting systems is to allow users to rent and return the bicycles at designated stations. This system would not be efficient and convenient if the users always have to return the bicycles at the origin or if each station is located too far away from the others. Additionally, overseeing a large number of bicycles could be problematic. Without sufficiently secure system, some bicycles might be lost and never return to the stations. This study attempts to design an advanced bicycle tracking system to help secure and maintain bicycle rental system on campus. This system would help universities in the UI GreenMetric World University Ranking to meet the criteria in transportation management more effectively.

Table of Contents

Page

List of Tables

Tables Page

List of Figures

Chapter 1
Introduction

1.1 Background

Security is increasingly becoming more prominent due to the result of economic inflation [1]. With regard to this, emerge varieties of means to implement security. One of the widely-used means of security is locking system. In this document, two usage types of locks are defined as: private and public.

Private locks are locks used with private properties, e.g., house, bicycle, and cabinet. This type of lock is used mostly by only a few trustful users (e.g. family members). Properties used with private locks are not focused on being shared and the owner is the main person who locks and unlocks it.

Public locks, on the other hand, are locks used with public properties, e.g., office, public bicycle, and public lockers. This type of lock is for public users to access it. Owner of the property are expected to have a lower degree of control on the usage of the property and user is not as trustworthy as in private; users might not have an incentive to secure the property after usage.

Even though locks have been created since the ancient Egypt, not much have changed [2]. People still have to own a physical key which must be carried at all times and could be easily lost or stolen. A combination lock allows user to use the lock without having to carry a key, but when sharing the combination once, the lock is forever shared. In a digital world, this problem can be solved by using a virtual key that can be kept, share, or revoke at any time.

1.2 Problem Statement

Securing or locking is arguably the most troublesome part of using a product especially when it is shared between multiple users. Conventional method requires users lending their keys or giving away their combinations in order to give access to the person. However, the method is insecure and, in the case of lending key, laborious.

One of the largest issues of using a physical key is the ability to share especially for public usage. Sharing physical keys could mean giving away the key which can be easily duplicated and ultimately compromising security. However, there is some business that requires public sharing of key such as a public bicycle rental service. A public bicycle should be made in such a way that is easy to access and return while being secure. In the present implementation, it is not that simple since users will have to go register at a physical booth for a key which is needed to be returned after each usage. This makes accessing the service troublesome and insecure.

Therefore, there is a need for the study to develop a lock system that can be easily shared for public use, while having suitable a security level. The system should also entail state-of-the-art design that can allow users to lock and unlock device via a mobile device.

1.3 Objectives of the Study

The objective of this study is to develop a lock system that can:

- Lock and unlock using user common owned device (e.g. mobile phone)
- Share lock to a specific person/group
- Revoke usage of the shared lock
- Track usage of each lock

1.4 Scope of the Study

The study focuses on implementing a smart bike sharing system using KMITL's campus as a study area for pilot-scale launch. Approximately 90 bicycles were deployed for the users with about 10 bicycles spared for replacement during maintenance.

Chapter 2
Literature Review

2.1 Existing Work

There are many kinds of lock systems designed to serve the stated purposes, each with varying strengths and weaknesses. Below is a summary of some of the exceptional work in relation to this project.

2.1.1 Mahidol's Bike Sharing

One of the most primitive bicycle-sharing system, "White Bike" is provided by Mahidol University (MU). It uses the concept of sharing physical keys to unlock the bike with no computerized system. Users are required to exchange their student ID card with a security guard nearby the station for the key to unlock the bike. After usage, the bike needs to be returned at the same station in order for an exchange back of key and ID card.

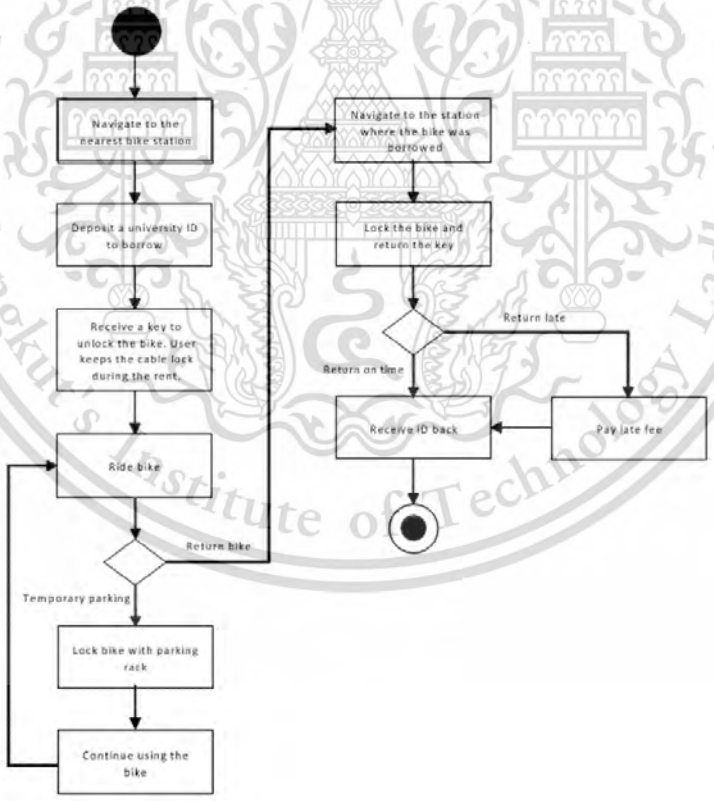


Figure 2.1 Workflow of MU's White Bike

2.1.2 CU Bike Sharing

CU Bike, provided by Chulalongkorn University (CU) is an implementation by Smoove, a French company which designs, manufacture, and install bicycle-sharing system solutions. An incremental step of MU's White Bike, instead of having a security guard to manage the keys, CU Bike uses a computerized locking station and bike. User will be required to have a membership card that uses RFID to tap and unlocks the bike with a combination of personal PIN code. After finish using users will be able to return the bike at any station as opposed to the same station from the MU's White Bike.

The system consists of combination of short-range and long-range wireless communication. Each bike communicates with a nearby station via ZigBee while each station communicates to the central server via GPRS.

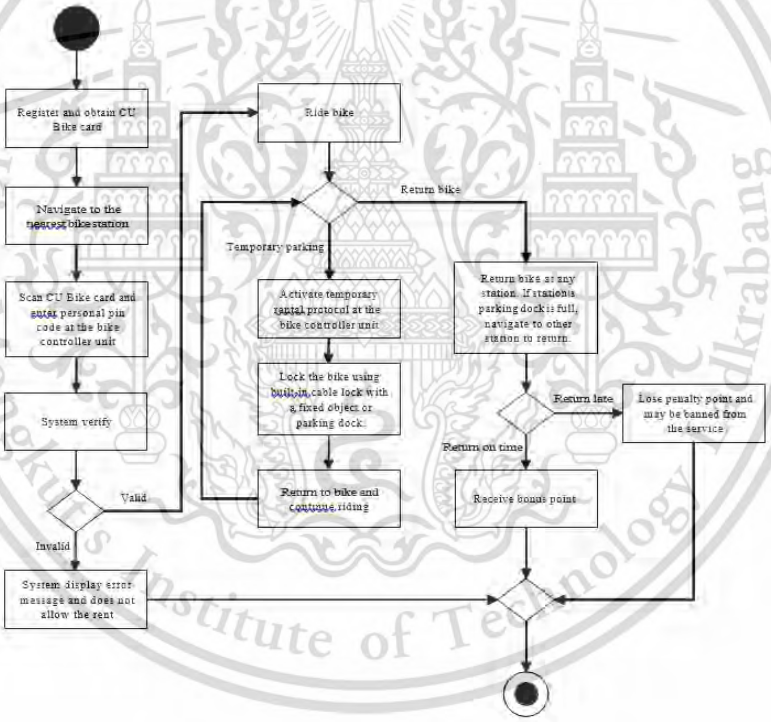


Figure 2.2 Workflow of CU Bike

2.1.3 WEBIKE

This application runs on a scope of campus level. It focuses on the security of lending a bike to a student in the campus. With a simple process of retrieving a passcode from the server and entering it onto a keypad, it accomplishes a certain level of security. However, with the current level of technology, this method is not sufficient as it lacks countermeasures against fake authorization as a student. Its simplicity reflects this flaw.

Additionally, the lock it uses, the U-Lock, requires a stationary bar or pole to be attached with. Looking ahead in case of rising numbers of bikes, there might not be enough pole or bar and would cost a lot to build more.

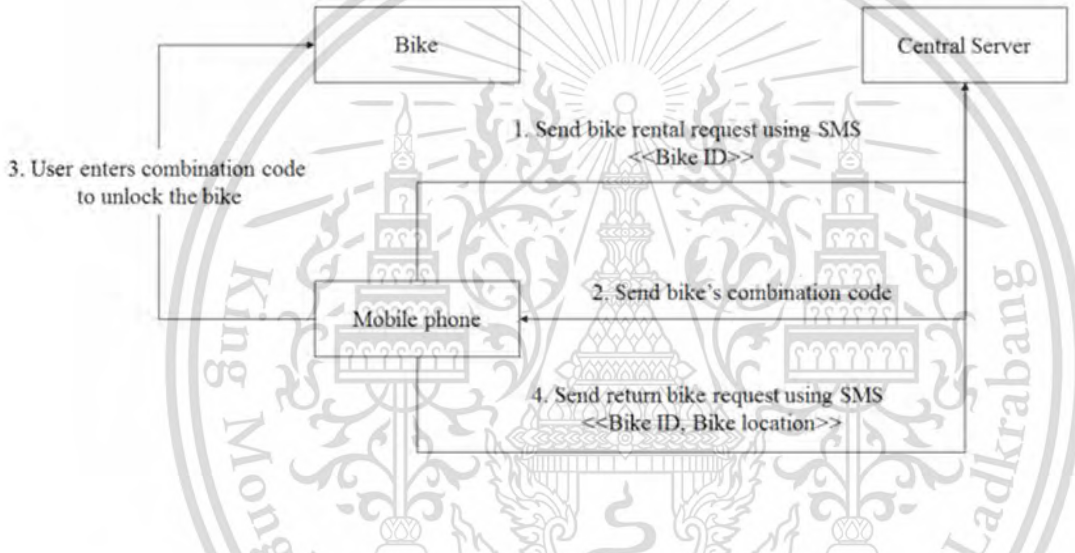


Figure 2.3 Workflow of WeBike

2.1.4 MuniBike

Interestingly, this application approaches security in several ways. This is not surprising with a city-wide scale it is running on. It provides different alternative means to retrieve a key to unlock the lock and use the bike such as SMS, VoiceCall, Mobile Application, or just simply keypad. Although the means are diverse, they all lead to one security scheme, authorization with the server and receive a key. As a result, it, unfortunately, shares the same flaw as the previously mentioned application, weBike.

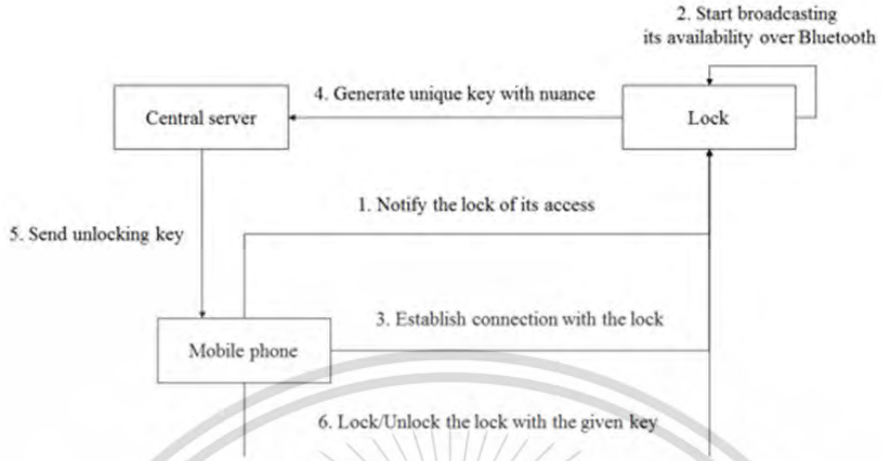


Figure 2.4 Workflow of MuniBike

2.1.5 Bit Lock

With a scope as wide as all end users is this application, BitLock. It similarly uses the U-Lock as its lock as the weBike application. However, comparing to the other two previously mentioned, Bitlock centers its focus differently. Unlike the two that have one owner of the system, a campus or a city as a whole, this application has many owners, each corresponds to the lock they bought. Therefore, only owner can use the lock, which leads to few questions on cases such that the owner wishes to share the lock or even sell out the lock. These matters are not answered with this application.

BitLock introduces a different security measure and communication technology approach than weBike and MuniBike by using Bluetooth. Bluetooth is one of the communication technology for short-range data transfers. It provides low power consumption and there are a lot of Bluetooth modules available on the market. Most devices such as smartphones or tablets support Bluetooth making it a popular choice for short-range communication standard. BitLock may be superior to others with its usage of Bluetooth. However, it does not support real-time GPS tracking, thus lacking a countermeasure against theft.

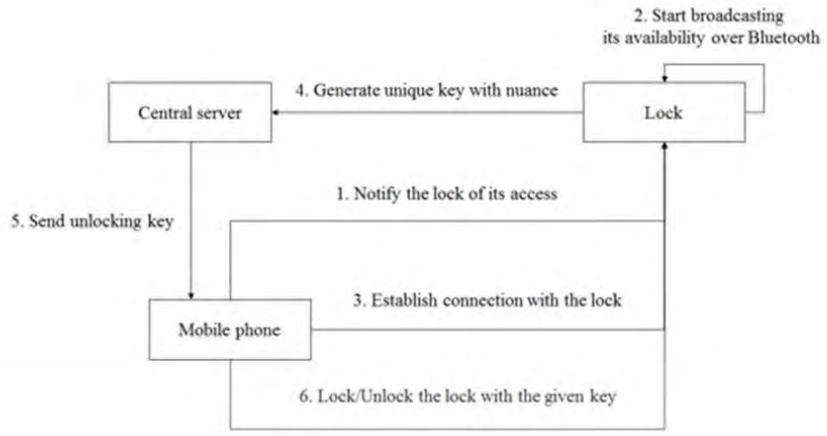


Figure 2.5 Workflow of BitLock

2.1.6 Noke (No-Key)

Noke runs in a similar manner to BitLock as it focuses on end users but with some twists. Noke answers the questions left by BitLock in a very satisfying way. It provides a way to share access to the lock and change of ownership. The shared access could be altered as pleased by the owner. Also, the lock does not limit to one specific usage. It could be used on many items such as door and bag. Regarding the security measures, Noke operates on the same design as BitLock, resulting in same strengths and weaknesses.

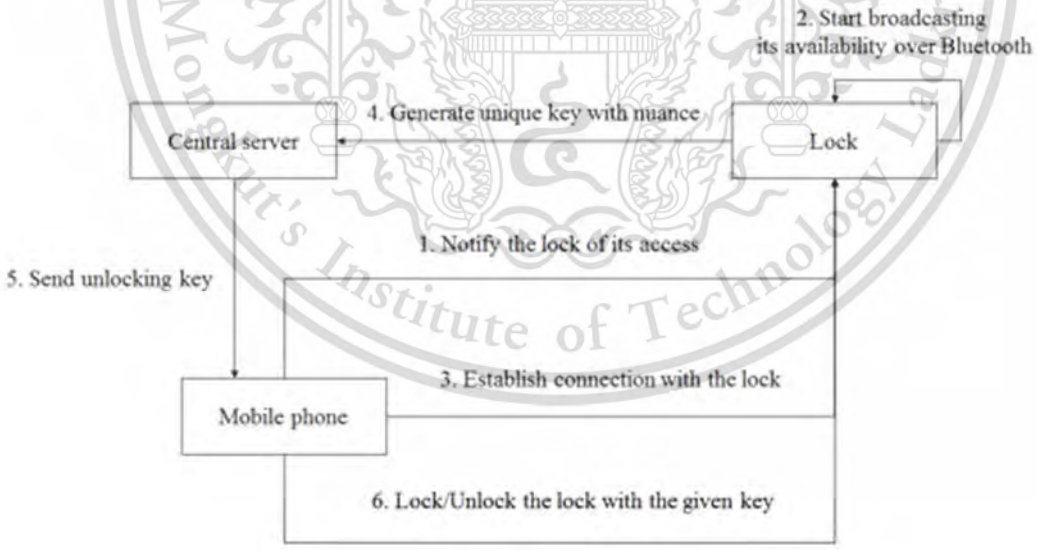


Figure 2.6 Workflow of Noke

Chapter 3
Requirements Analysis

This chapter provides detailed insights on the requirements resulting after the analysis of related existing works along with use cases of the system. Requirements are represented in a form of FURPS+ model (Table 3.1) which can aid in discovering potential needs that are both functional and non-functional.

3.1 Requirements

3.2 **Use Case Diagram**

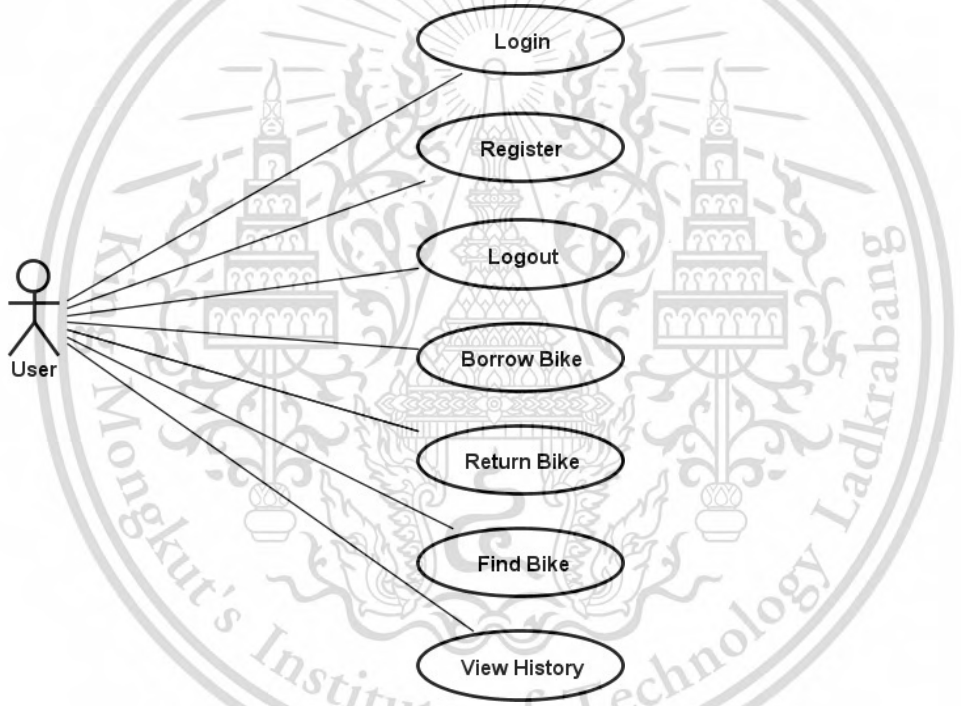


Figure 3.1 Use Case Diagram of KMITL Bike Application

3.3 Use Case Description

Table 3.2 Use Case Description - Login

Use Case	Login
Primary Actor	All users
Pre-condition	User has the application on their device. User is registered.
Post-condition	User is logged in to the system.
Flow of events	1) User opens the application
	2) User enters their company username and password (ex: KMITL NAC)
	3) Server recognizes that the user is already registered
	4) Server verifies user's information
	5) User is logged in to the system
Alternative Flow	Condition: Wrong username/password
	3a) System notify user that the username/password is wrong
	Condition: Unable to login
	4a) System notify the user and asks user to login again

Table 3.3: Use Case Description - Register

Use Case	Register
Primary Actor	All users
Pre-condition	User has the application on their device.
Post-condition	User is registered. User's information is recorded correctly into the server's database.
Flow of events	1) User opens the application
	2) User enters their company username and password (ex: KMITL NAC)
	3) Server recognizes user never register
	4) Application provide registration form
	5) User enters personal information into the form provided in the application
	6) Server verifies user's information
	7) User is registered
Alternative Flow	Condition: Invalid Information
	5a) Application asks user to re-enter the information into the application.
	Condition: Unable to register
	6a) Application notifies the user and asks user to apply the registration again

Table 3.4: Use Case Description - Logout

Use Case	Logout
Primary Actor	Authorized user

Pre-condition	User has the application on their device. User is registered. User is logged in.
Post-condition	User is logged out from the system.
Flow of events	1) User opens the application
	2) User presses to "Logout" button on the application
	3) Application performs logout for user
	4) User is logged out from the system
Alternative Flow	Condition: Unable to logout
	4a) System notify the user and asks user to logout again

Table 3.5: Use Case Description - Borrow Bike

Use Case	Borrow Bike
Primary Actor	Authorized user
Pre-condition	User is already logged in to the system through the application. The bike is in a locked state.
Post-condition	Bike is unlocked. Log is correctly saved into the system. Status of the bike is updated.
Flow of events	1) User arrives at the bike with the application on mobile phone
	2) User opens the application
	3) User presses the switch on the bicycle box
	4) User presses "Borrow Bike" button in the application
	5) Application shows a list of bike usage plans
	6) User selects a bike usage plan
	7) User scans QR code that attached on the bike
	8) Server verifies user's balance, status, and permission to borrow the bike

	9) Application sends unlock key to the bike
	10) Locking mechanism on the bike unlocks itself
Alternative Flow	Condition: The bike is already borrowed
	9a) System notify the user that the bike is already borrowed by someone
	Condition: Insufficient points to borrow
	9b) System notify the user that their points are insufficient to borrow

Table 3.6: Use Case Description - Return Bike

Use Case	Return Bike
Primary Actor	Authorized user
Pre-condition	User is already logged in to the system through the application. User is in a borrowing status. The bike is in an unlocked state.
Post-condition	Bike is lock. Log is correctly saved into the system. Status of the bike is updated.
Flow of events	1) User opens the application
	2) User presses "Return Bike" in the application
	3) User scans QR code that attached on the bike
	4) Application checks if the bike is locked
	5) Server verifies user's status
	6) User successfully returns the bike
Alternative Flow	Condition: The bike is not locked properly
	5a) System notify the user that the lock is not locked properly

Table 3.7: Use Case Description - Find Bike

Use Case	Find Bike
Primary Actor	Authorized user
Pre-condition	User is already logged in to the system through the application.
Post-condition	-
Flow of events	1) User opens the application
	2) User press on "Find Bike" in the application
	3) Application places bicycle "markers" on its map
	4) User walks to the desire bike

Table 3.8: Use Case Description - View History

Use Case	View History
Primary Actor	Authorized user
Pre-condition	User is already logged in to the system through the application.
Post-condition	-
Flow of events	1) User opens the application
	2) User presses on "View History" tab in the application
	3) Application lists all the borrowing sessions of user
	4) User finds interested session
	5) User presses on the interested session
	6) Application displays an in-detail view of the interested session

Chapter 4
Background Knowledge

This chapter will discuss background knowledge conducted in order to achieve the set objectives. Below are knowledge needed prior to fully understand the proposed solution.

4.1 Asymmetric Encryption

Asymmetric encryption is a form of cryptography and its sole purpose is to solve the age–the old problem of key sharing.

Prior to the asymmetric encryption, most encryptions were done symmetrically where both the sender and the reader need to know the key and that same key is used for both encryption and decryption of the message. The problem with symmetric encryption lies with the process of sharing the key between the sender and the reader. Since the key has to be kept secret, the key cannot be shared between the two parties securely without needing the two to be physically next to each other.

Asymmetric encryption was first thought as a form of "non-secret encryption" where the key does not need to be entirely secret [4]. Instead of having only one key to perform both the encryption and decryption of the message, asymmetric encryption has two different keys: a public key and a private key. The usage of two keys mentioned is called as public-key encryption [5]. Either of these key scan be used for encryption or decryption but they must be used as a pair and performs different tasks. The difference between the private and public keys are as the name suggested, private keys are meant to be kept secret while public keys can be viewed by the public. To further clarify, public keys can be stolen but it will be useless since decrypting a message requires both public and private keys. Communication will be done by only the exchange of public keys, making making asymmetric encryption or public-key encryption a good candidate for a secure communication regardless of attempts on eavesdropping or interception.

4.2 Cryptographic Nonce

A cryptographic nonce is an arbitrary number that is made to be used once. Nonce consists of series of randomized number and is used in an encrypted message in order to prevent an event of a replay attack. Without nonce, every message that has the same content will appear to be the same even with encryption, attackers could save the message and replay it anytime.

4.3 Bluetooth Low Energy Module and Properties

Bluetooth low energy or BLE is a wireless personal area network technology with low energy functionality. BLE device can be run for long periods on power sources, such as coin cell batteries or energy-harvesting devices. It also comes with small size, low cost, and high compatibility for mobile phones and tablets, which is suitable for the Internet of Things [6]. In BLE devices, there is an extension of the classic Bluetooth stack that implements a specific Bluetooth profile known as the Generic Attribute Profile or GATT in short. BLE devices will use GATT to communicate with each other. Data are organized into nested objects called Profiles, Services, and Characteristics, as illustrated in Figure 4-1 [7].

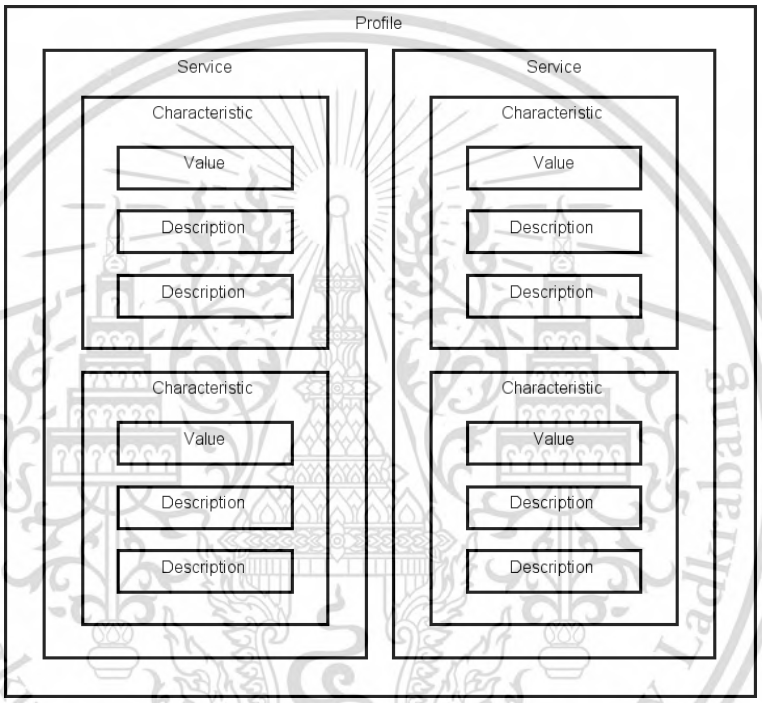


Figure 4.1: Overview of Bluetooth GATT

The GATT profile contains characteristics which are the data of BLE devices such as sensor data. Each characteristic is formed together into logical functions called service. Some characteristics are read-only, while others can be written for device configuration purposes. Inside each characteristic, there is a descriptor, which can be used to configure specific behaviors like notifications. Characteristic notifications allow configuration like pushing updates as depicted on schedule, or when the value of the characteristic changes. This is very efficient way to reduce the power usage since the host application is not required to connect to the remote peripheral all the time [7].

Chapter 5
System Design

5.1 System Architecture

The system consists of three main components: server, smartphone, and the lock unit. Since the lock unit does not contain a cellular network module, as shown in Figure 5-1, the smartphone primary serves as an interface between the lock unit and the server by communicating over Bluetooth low energy wireless connection. Users will also use the mobile application as the main controller in unlocking the bicycle.

Figure 5.1: Overview of the system design for KMITL Bike

5.1.1 Bike Server

In the server side there are few more important details kept compared to the overview shown earlier. Figure 5-2 illustrates the relationship of necessary data in the server. During the riding session, the server will keep track of the user, be it the borrow time, return time, and even the route the user took. All these information will be kept as user's histories which can be viewed at any time by them. Also, each session requires a deposit corresponding to the amount of time alloted. The model of the bike is recorded as well to each session. Finally, the server will keep track of application version, both on Android and iOS, to make sure user's application will always be up-to-date.

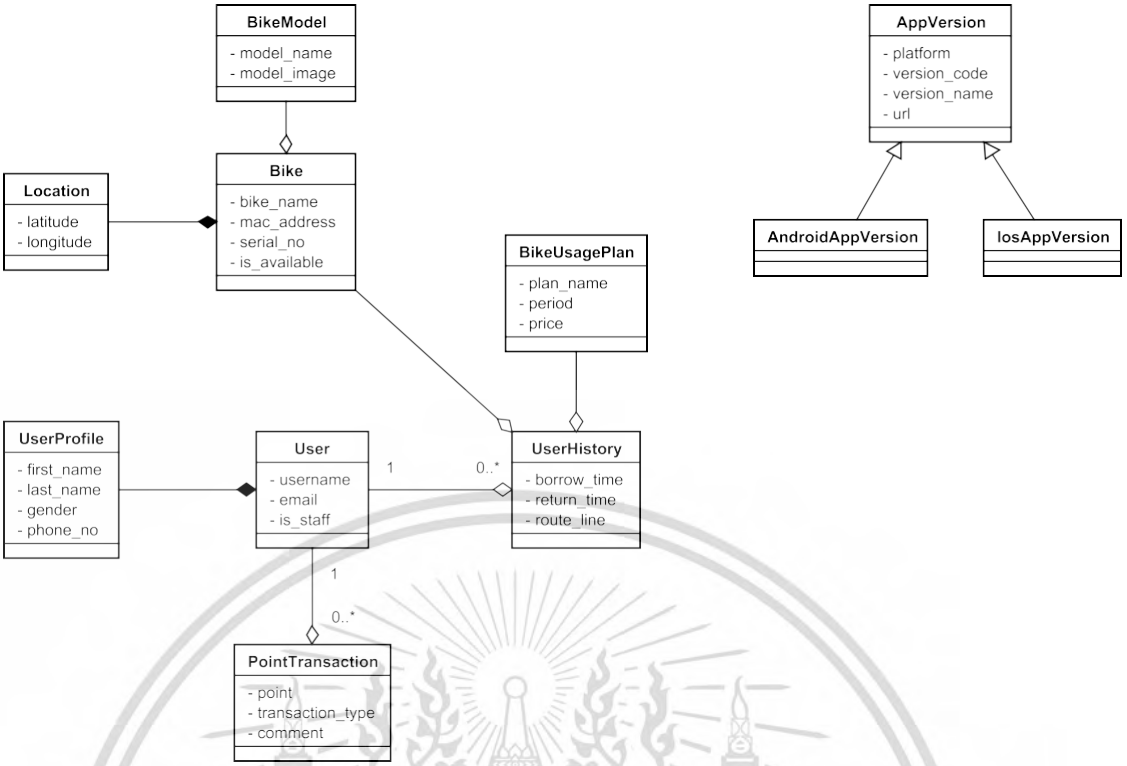


Figure 5.2: Simple class diagram of the server

5.1.2 Application Programming Interface

There are several services available on the server for the mobile application to use. The description of Application Programming Interface (API) are shown in Table 5.1.

5.1.3 KMITL Bike Mobile Application

For mobile application, it was developed with MVP (Model-View-Presenter) architecture as a design pattern. Here, each view came with their own presenter that will handle all presentation logic, acting as a middle-man in the process between model and view. Since model and view should not directly communicate with each other, having a presenter handling this task helps the system to achieve total independency. Additionally, in Figure 5-3, there are several services in the system. For communication, there are two services, Bluetooth and Location. Bluetooth service provides Bluetooth connection to the lock while Location service provides GPS location of the user. For any request from application to the server, API service is used. API service acts as a medium for server and mobile application to communicate. In the process, it gets response from server according to user's request.

Table 5.1: KMITL Bike REST API

Template	HTTP Verb	Description
api/v1/auth/access_token	GET	Return credentials for a login session and identifies the user
api/v1/auth/login	POST	Login into the server, this will result a call to I AM KMITL account validation
api/v1/auth/logout	GET	Logout from the server
api/v1/auth/register	POST	Register a new account
api/v1/services/available	GET	Return a list of bikes that are currently available
api/v1/services/update_bike_location	POST	Update the current location of bike to the server
api/v1/user/status	GET	Return user's status whether he/she is still in riding session or not
api/v1/user/borrow	POST	Borrow the bike by bike ID
api/v1/user/return	POST	Return the bike
api/v1/user/history	GET	Return user's riding history
api/v1/user/update_user_location	POST	Update the current location of user, this will be invoked while the user is riding

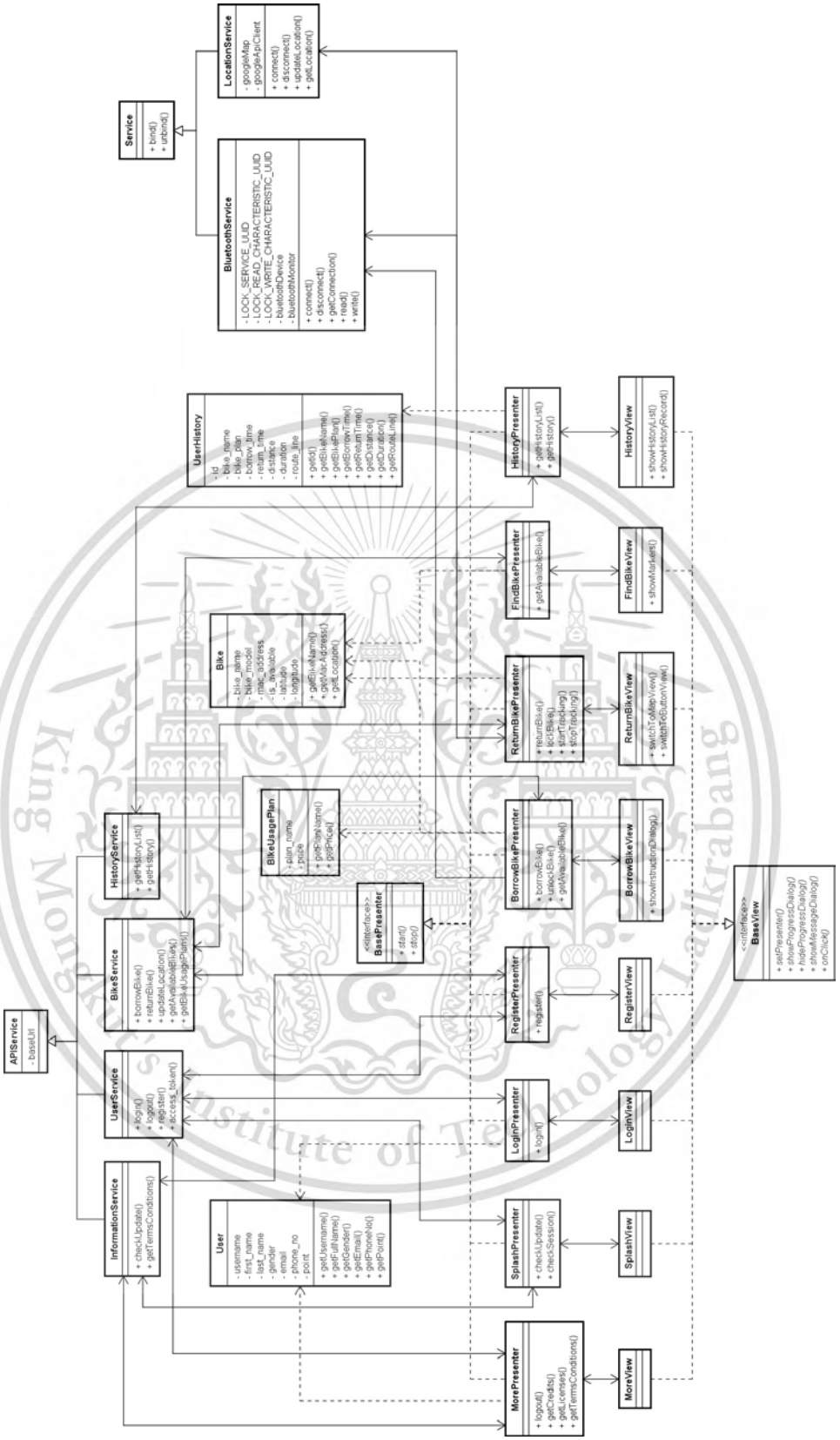


Figure 5.3: Class diagram of KMITL Bike mobile applicant

5.2 System Components

5.2.1 Server

Server serves as a bicycle management system. It consists mostly of two parts: database and service. The database collects information such as bikes locations, users' information, and usage sessions. The service checks for user's credentials, bike availability, and provide filtered information from the database to specific users.

5.2.2 Smartphone

Smartphone includes two types of operating system: Android and iOS. Since the lock unit does not contain any cellular network connection module (due to energy consumption), it cannot be directly connected with the server. Most smartphones are equipped with both Bluetooth LE and cellular network. This allows the lock to be able to communicate with the server via the smartphone. Smartphone also serves as the main interface for the user to interact with the system.

5.2.3 Arduino Pro Micro 5V/16MHz

Arduino is an open-source computer hardware which is widely adopted among hardware developers. It is usually served as a go-to hardware when starting out a project. Specifically, Arduino Pro Micro 5V/16MHz was chosen for the project due to its small footprint in terms of power consumption and physical size.

Figure 5.7: Arduino Pro Micro 5V/16MHz

5.2.4 HC-05 Bluetooth 4.0 Low Energy Module

HC-05 is a Bluetooth low energy (LE) module, primarily serves as a wireless communication between the Arduino and the smartphone. Bluetooth LE was chosen for its widely adopted standard for connecting with wireless peripheral devices as well as being energy efficient. A market study by IndustryARC Analysis reports that there could be over 8.4 billion units of Bluetooth LE shipped by 2020 [8].

Figure 5.8: HC-05 Bluetooth 4.0 Low Energy

5.2.5 TAU-0826 Solenoid

TAU-0826 is a Pull-Type Linear Solenoid with a maximum keeping force of 20N while consuming only 6V. It is one of the core actuator used in the unlocking mechanism of the lock unit. The uniqueness of TAU-0826 is its small footprint of only 26 × 25 × 22mm while being powerful enough to pull the latch used for locking the lock's shackle which makes it compatible with the designed lock unit.

Figure 5.9: TAU-0826 Solenoid

5.2.6 TL-W5MC1 Inductive Proximity Sensor

TL-W5MC1 is an inductive proximity sensor capable of running on 5–36V DC. It is used for detecting various types of metal. Its sensing capability depends on the type of metal. Ferrous metals, such as iron and steel, allow for a longer sensing range, while nonferrous

metals, such as aluminum and copper, can reduce the sensing range by up to 60 percent [9]. TL-W5MC1 has a detection range of 5mm according to the manufacturer specification. Its size of 30 × 18 × 10mm matches the size available in the lock unit.

Figure 5.10: TL-W5MC1 Proximity Sensor

Chapter 6
Development

This section elaborates the actual development processes of the project. The elab- oration is divided into two main parts: the development tools and the development iterations.

6.1 Development Tools

The development tools used in this project are:

- Operating Systems: Android 4.4 KitKat (API Level 19), Ubuntu 12.04.5 LTS
- Programming Languages: C, Java, Python 2.7
- Database: PostgreSQL 9.3.16
- Integrated Development Environments: ARDUINO 1.8.2, Android Studio 2.3.2, PyCharm Professional 2016.3
- Libraries & Frameworks: Crashlytics, Django, Django REST Framework, MVBarcodeReader, Neatle
- Utility Softwares: Adobe Photoshop CC 2017, Adobe Illustrator CC 2017, Autodesk Fusion 360, MakerBot Desktop 3.10, pgAdmin III 1.22.2

6.2 Development Techniques

6.2.1 Securing Data and Communication with RSA and Cryptographic Nonce

In order to ensure a secure locking system, crucial communications between each party should be encrypted. In the current system, there are three main communication parties of the system: the Lock, the App, and the Server. However, there are several problems that can occur with ordinary symmetric encryption scheme since it requires the key to be completely secret. This means that all the three parties will have to be able to keep its source code which includes the key to be hidden. This is almost impossible since the application can be reverse engineered through the usage of decompilers. Android application, for example, can be easily decompiled by tools such as Android APK Decompiler [10]. Access to the source code also gives the attacker the access to the key. This is why the system should be using the asymmetric encryption scheme.

Since the most crucial commands such as locking and unlocking the lock are from the Server, Server will encrypt those commands with a private key. The message will then be passed on to the Lock through communication with the App,

making the App to acts only a bridge connecting between the Server and the Lock. The lock will then decrypt the commands using a public key.

There is one more way an attacker could unlock the lock without the Server's authorization. That is after the attacker had legitimately unlocked the bike through Server's authorization, the attacker could record all communication that is being done between the App and the Lock and replays it later. This way, the Server will never know about the Lock being unlocked. Fortunately, the solution happens to be relatively easy, since the Server will just have to make sure that each message being sent will not be the same. The Lock and the Server could agree and add a nonce to the message which will change on every usage session.

To conclude, the usage of nonce will help prevent a replay attack and an asymmetric encryption scheme will prevent the attacker from having complete control of the system after obtaining the key through means like code decompilation.

6.2.2 Robust Encryption Method with Cipher Stream Chaining Process

As mentioned in the previous section, an ordinary symmetric encryption scheme has a severe disadvantage. It requires all the communication parties to keep their source codes (that may contain the shared key) secret. This is prone to decompilation attack.

To address such shortcoming, we have explored a novel symmetric encrypt method, called Cipher Stream Chaining Process (CSCP). By employing logistic map and a perceptron model, CSCP would allow all parties to communicate using shared keys that is very difficult to extract. Currently, our new method can encrypt only images. However, we believe we can extend our technique to real-time communication used in bike-sharing domain as well. This work has been published in [12].

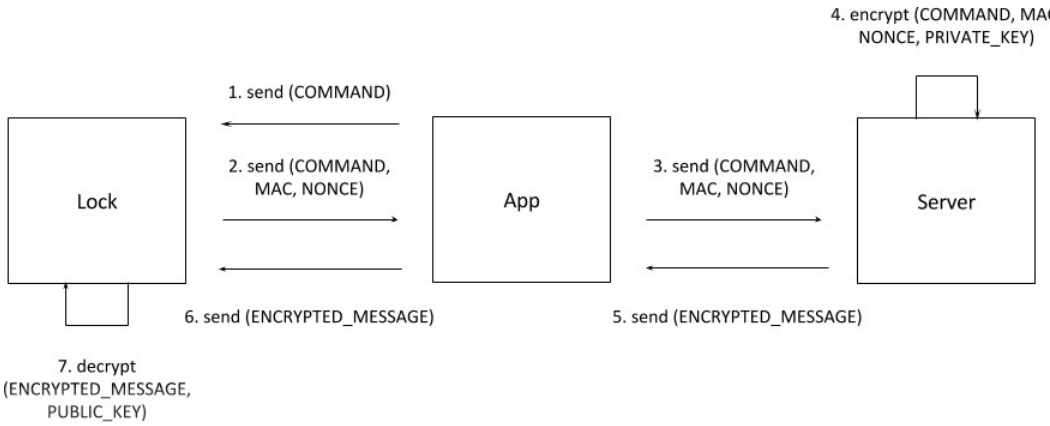


Figure 6-1: Overview of Unlocking Process

6.2.3 Underlying Communication in Unlocking Process

A flow of unlocking process can be described as shown in Figure 6-1. In order to initiate the connection between user's mobile phone and the lock, Bluetooth pairing procedure must be performed. To satisfy what was stated in the requirements, Bluetooth will broadcast itself at all time. During a broadcasting process, the bike will be visible to the user to unlock. When the user chooses the bike by scanning a barcode on it, the mobile application will request for unlock by sending a command to the lock. The lock will generate a message to be passed from the application to the server. After the server got the message, the message will be encrypted with a private key, that only known to the server, and pass back to the application. Once the application received the key from the server, user's mobile phone will connect to the lock and start discovering the services. After the process of discovery is completed, user's mobile can send a message to any characteristics available on the lock service as shown in Table 6.1. For the locking or unlocking process, the characteristic FFE0 is used as a destination for sending the unlock key that received from the server. If the key is valid then the bike will be unlocked and ready to ride. The procedure is also the same for locking the bike when the user wants to return. However, the key validation is not required anymore.

Table 6.1: Bluetooth Characteristics Available on the Lock

Characteristic	Operation	Usage
FFE0	Read/Write	Send the command to the lock or unlock, Read the result after the command is executed
180F	Read only	Read battery level of the lock

6.2.4 Near Real-Time Location Tracking

Since the cost of 3G and GPS module is considerably high, the alternative way to track the bike is to use location service of user's mobile phone. By using mobile phone's Location service, the location of the bike, which represented as latitude and longitude, is updated to the central server every 10 seconds during the ride. The origin of this interval is based on an idea that the update interval should not be too frequently nor infrequently. If the update is invoked in short interval, it will consume data usage too much and if the interval is too long, then an action might not be taken in time in case the bike got stolen. Even if ten-seconds interval location tracking might not be real-time, but it is still acceptable as near real-time.

Apart from high cost of GPS module, the GPS modules generally require high energy consumption. Also, it does not work very well during bad weather, indoors, or areas with many buildings, such as university campuses. To this end, other means of localization may be required.

6.2.5 A Pre-processing Technique for BLE-based Localization

Since the cost of 3G and GPS module is considerably high and GPS may not work well in some situations, the alternative way to track the bike locations is required. One of the candidate technologies is Bluetooth LTE. Bluetooth LTE is designed to consume low power and the hardware is relative cheap. However, it is not intended for localization purpose. Nevertheless, our research [13] shows that Bluetooth LTE can be used to find location of a Bluetooth beacon via trilateration method. We have also proposed channel separation pre-processing technique that can improve distance estimation based on the Received Signal Strength Indicator (RSSI) of the Bluetooth signal. Due to limitation of our devices, the research is focused on indoor localization. However, we believe that our method can also be employed in bike-sharing system.

6.2.6 Searching Nearby Bikes on Google Maps

As the smart bicycle fleet does not require any stations to park, the bikes do not have a fixed position where the user can go there and grab them. If the user needs to use the bikes, then he or she will likely have to go through looking around the places to find them. For the convenience of the user, the mobile application provides the Google Maps view with the markers, which indicate the bikes' location, on it. The bikes that are already in use will not be shown to the user. With the find bikes feature, the user can easily locate nearby bikes and go there to borrow the bikes whenever he or she wants.

6.2.7 Activity Timeline for Bicycle Rental

In the rental business, keeping a track of user rental history is required. Each riding session contains an information of bike ID, route that the user takes, distance in kilometer unit, duration, and time-stamps when the user borrowing/returning the bike. The user can view his or her history, which included the information described above, via the mobile application.

6.3 Development Iterations

6.3.1 Software Development

First Iteration: Bluetooth with Cable Lock (Hybrid)

To fulfill the requirements stated in Chapter 3, the first version application was released. The application was implemented using Ionic, an open-source hybrid application development framework which can develop the native-like application made out of HTML, JavaScript, and CSS. However, as Ionic didn't provide native components like Bluetooth or Location, another library, which is called Cordova, was used here to add up a lack of these components. The tools provided in the framework were simple to use so there was not much difficulty in developing.

The usage of the application was straightforward. User can borrow the bike by selecting the preferred bike from the list appeared on the mobile application. This list came from scanning the perimeter for the application registered Bluetooth's MAC Address and filtering out any unrelated Bluetooth devices. Figure 6-2 shows the screenshots of the first version of KMITL Bike application.

Features in this iteration:

- Borrow bike
- Return bike
- Find bike
- View riding history (without route line)

Frameworks & Libraries used in this iteration:

- Ionic 1
- Cordova Bluetooth Serial
- Cordova Geolocation

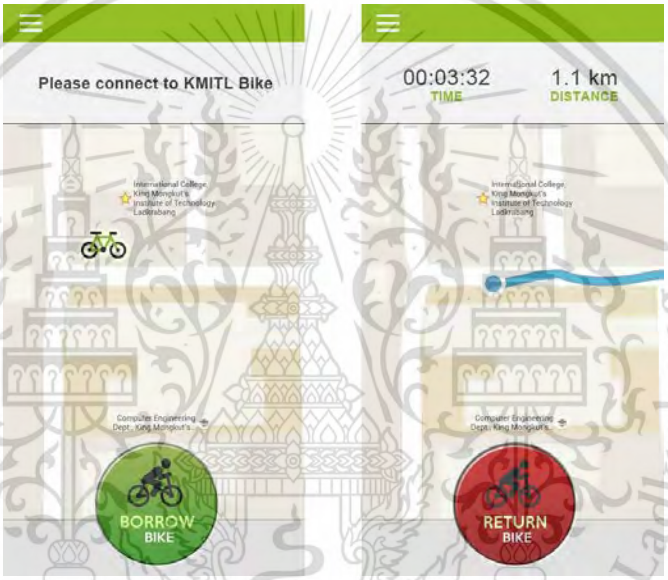


Figure 6-2: 1st Iteration - KMITL Bike Application

Second Iteration: Bluetooth with Cable Lock (Native)

After experiencing some unknown issues with Bluetooth connection in the first application, it appeared that a hybrid application was hard to track down the issues that related to hardware components of mobile phone like Bluetooth or Location. As a response, the development of the application was completely changed from a hybrid application into a native application.

In this iteration, there was also an improvement to the design of the user interface to make it more intuitive and open for new features as shown in Figure 6-3, Figure 6-4, and Figure 6-5. Crashlytics is embedded into the app in order to be able to keep track and assess crashes in real-time. Additionally, some new features

were added to make the application more suitable for real-world usage.

Features in this iteration:

- Borrow bike
- Return bike
- Find bike
- View riding history
- Near real-time tracking
- View user profile

Frameworks & Libraries used in this iteration:

- Android Native Libraries
- Crashlytics

Figure 6-3: KMITL Bike application - 2nd Iteration

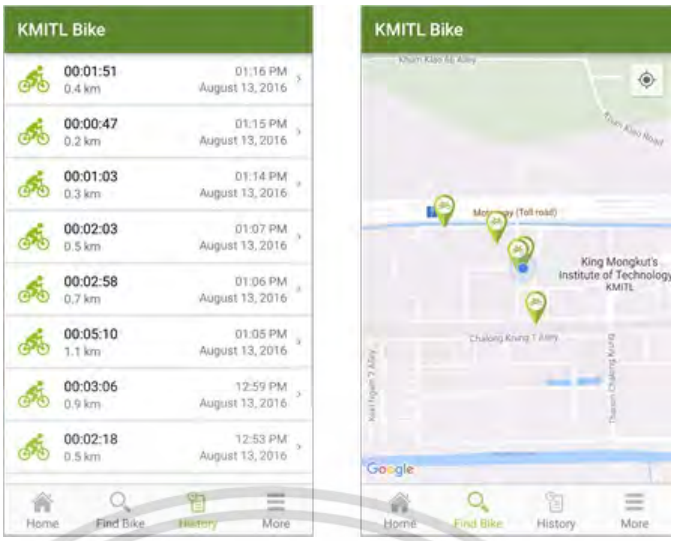


Figure 6-4: KMITL Bike application - 2nd Iteration (continued)

Figure 6-5: User can choose a bike from the list

Third Iteration: Barcode Scanner with Passcode Lock (Native)

As a durability of the cable lock design in Section 6.3.2 was not enough to withstand the real-world environment (e.g., not rain-proof, internal circuit components could not handle rough terrain), the locking mechanism needed to be revised before deploying to an actual use. However, it was also necessary to conduct a test flight for the purpose of collecting information. Therefore, a temporary solution was raised, and

it was to use manual passcode lock for a certain time along with barcode authentication. After the user scans the barcode on the bike, the corresponding passcode for the specific bike will show up and can then be used to unlock the lock. Not only that, using the barcode could indirectly prove the presence of the user near the bike as well.

Features in this iteration:

- Borrow bike
- Return bike
- Find bike
- View riding history
- Near real-time tracking
- View user profile

Frameworks & Libraries used in this iteration:

- Android Native Libraries
- Crashlytics
- MVBarcodeReader

Fourth Iteration: Bluetooth with Semi-automated Lock (Native)

After the run with cable lock and barcode scanning system, there were few observable good points. Barcode scanning successfully verify that the user was in the vicinity of the bike and prevent long distance borrowing. Since the Bluetooth module used in this project could receive connection as far as 10 meters, this system could cover this loophole [11]. However, the newly designed lock required Bluetooth connection, thus, barcode was combined with Bluetooth schema to perform without loophole. Furthermore, in this iteration, there were minor improvements on the stability issues found while testing as well as Point System implementation. The Point System served as the protection to bike abuse problems. If any user misused the system in any way listed in the term and conditions, their credits will be deducted accordingly. If their credits were to reach zero, they may not use the system anymore.

Features in this iteration:

- Borrow bike
- Return bike
- Find bike

- View riding history
- Near real-time tracking
- View user profile
- Point system

Frameworks & Libraries used in this iteration:

- Android Native Libraries
- Crashlytics
- MVBarcodeReader
- Neatle

6.3.2 Hardware Development

First Iteration: Cable Locking System

While the goal of this project is to deploy the locking system and software system at the same time, the resources and time for them are not equal. The locking system took a longer time to finalize the model design and create a final product whereas the software could be tested almost immediately after completion. As a result, it was better to create a mock locking system to support the finished software. In this first iteration, a metallic box and a cable were used as a lock. This lock will be placed on top on the back wheel of the bicycle and the cable is used to hold the wheel in place, restricting the ride. A test was conducted to prove the usability of the planned system. After the system went on two events: KMITL Science Exhibition Day 2016 (Figure 6-6) and Engineering Expo 2016: Engineering Innovation with Thailand 4.0 (Figure 6-7), the lock showed few issues. The lock could not detect if it was locked or not, which showed its vulnerability. Additionally, it was too fragile to external forces while riding and transporting. Fortunately, the software testing went well.

Figure 6-6: HRH Princess Sirindhorn at KMITL Science Exhibition Day 2016

Figure 6-7: Team at Engineering Expo 2016

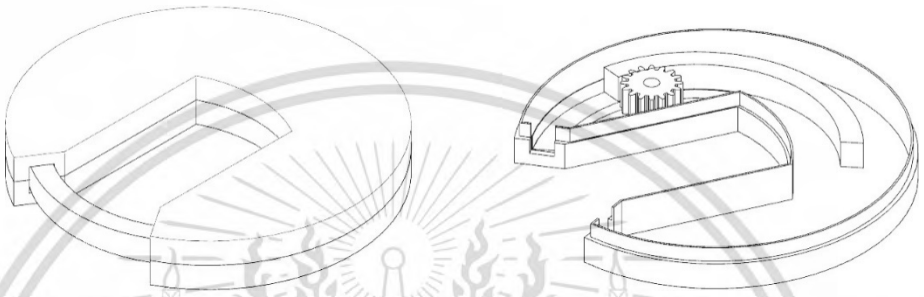
Second Iteration: Automated Lock

Improving on the previous iteration, a fully automated lock controlled by a mobile application via Bluetooth connection was designed. This lock had a button as a sensor for detecting locking state, which countered the issue with the first lock. As for the internal mechanism, the locking shaft was pushed and pulled by a horizontal gear driven by a motor, holding and freeing the back wheel of the bicycle respectively. Figure 6-8 below depict the design of this lock. This design was

presented to the committee and was, unfortunately, doubted. There were issues with a gear-driven mechanism, since it was prone to dust and could not handle forceful opening from users. In the end, this lock was found faulty before it was produced.

Figure 6-8: Locking Mechanism Design - 2nd Iteration

Third Iteration: Semi-Automated Lock with Teeth-Based Mechanism



To fix the previous issues with gear-driven mechanism, a new design using teeth-based mechanism was modelled. This model can be seen on Figure 6-9. The teeth on the locking shaft can only move one way through the teeth on the lock package, which is the act of pulling the locking shaft to hold the wheel in place. This is to ensure that at any moment, the lock can be locked without any need for battery. However, the unlocking process still require the battery to pull the teeth of the lock package away from the teeth of the locking shaft, creating a gap for the locking shaft to be pulled back by spring to its origin, freeing the back wheel of the bicycle. The teeth will be pulled by a servo's spinning motion to one side. Overall, it is a semi-automated process where user can unlock the bike automatically using mobile application while manually locking the bike to handle security issues if in any circumstances the battery is dead.

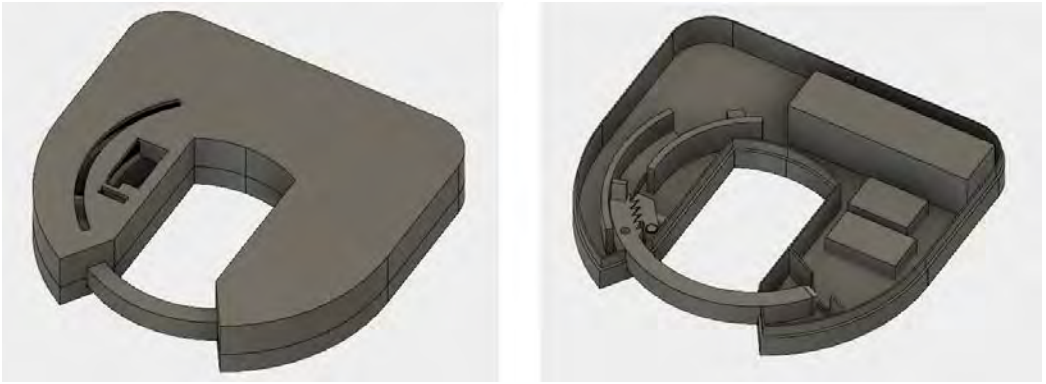


Figure 6-9: Locking Mechanism Design - 3rd Iteration

Fourth Iteration: Semi-Automated Lock with Sliding-Latch-Based Mechanism

Initially, the previous model appeared to be very promising. However, after the talk with Department of Mechanical Engineering at KMITL, there still were few stability issues with the lock. The choice of actuator for the locking system, the servo, was not suitable for harsh working environment such as constant shaking of the lock when riding on a rough surface. Moreover, the button that was used as a sensor to detect if the lock was successfully locked was unreliable. The right concept of designing a locking system was to involve as less mechanical parts as possible. The button required mechanical movement of the button surface to be contacted, which had high error rate depending on the amount of force and angle in contact. Not only that, the teeth-based mechanism could not hold on due to spring deformation and could be forcefully broken still. Therefore, a new model was designed and put through the prototype production. This model replaced the former mechanism with sliding-latch mechanism combined with solenoid to actuate it. It also used proximity sensor to remove the mechanical part of the button. Figure 6-10 represents the model of the lock.

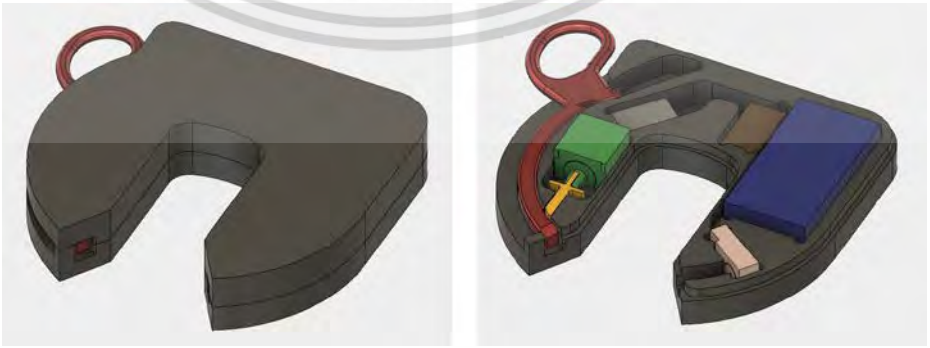


Figure 6-10: Locking Mechanism Design - 4th Iteration

Final Design: Semi-Automated Lock with Sliding-Latch-Based Mechanism V.2

The design presented in the fourth iteration is adequate for the basic functionality of the lock unit. However, throughout the development of second, third, and fourth iteration design, there are only testings on 3D printed plastics which are too fragile for real-world usage. In order to achieve full functionality testing, the lock unit needs to be made out of a stronger material such as aluminum. After discussions with several CNC machining factories, the design needs to be changed drastically to allow for the machining process possible at an appropriate cost and be more user-friendly while also concerning light raining conditions that might affect the inside electronics. Figure 6-11 represents the final design of the lock unit with its external casings made from aluminum 6061 (bottom piece which is shown on the right) and 6063 (top cover which is shown on the left). Aluminum 6061 and 6063 allows for high strength, good workability, weldability, and corrosion resistance of the lock unit package.

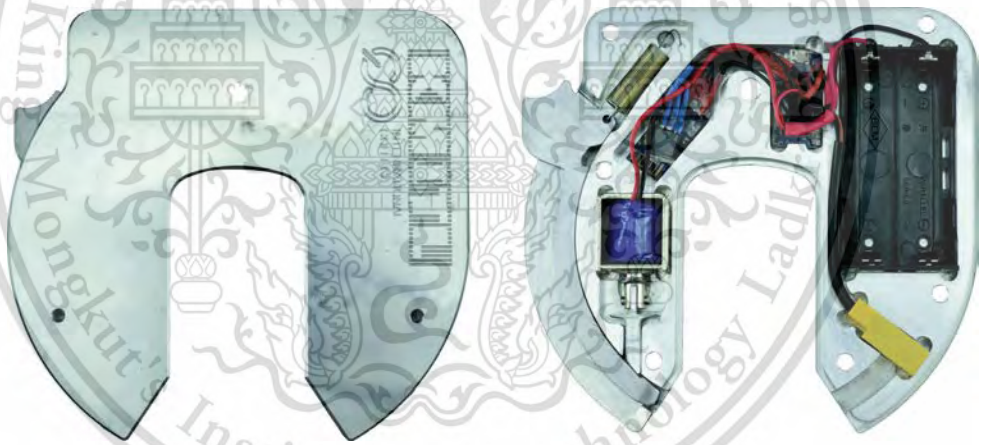


Figure 6-11: Locking Mechanism Design - Final Design

Chapter 7
Results and Evaluations

7.1 Experimental Method

The experiment for this system was initiated through a series of test flights. This test flight was conducted within a section of King Mongkut's Institute of Technology Ladkrabang campus. An application on both Android and iOS was implemented for the experiment under the name KMITL Bike. This application involved solely on the usage of bike as the focus of the test was on the bicycle aspect of the InfiniLock for the moment. The purpose of this is to gain feedback from users and use it to improve the system while promoting Green Campus campaign which is the underlying goal of the whole system.

7.2 Test Flight 1: The Beginning

In this test flight, the system was tested with actual users for its reliabilities, usabilities, and validity and lasted from January 18, 2017 to February 8, 2017 for a total of 21 days. However, due to the delay in hardware development, a substitute for the lock was necessary for this period of time. In the end, passcode lock was chosen for testing.

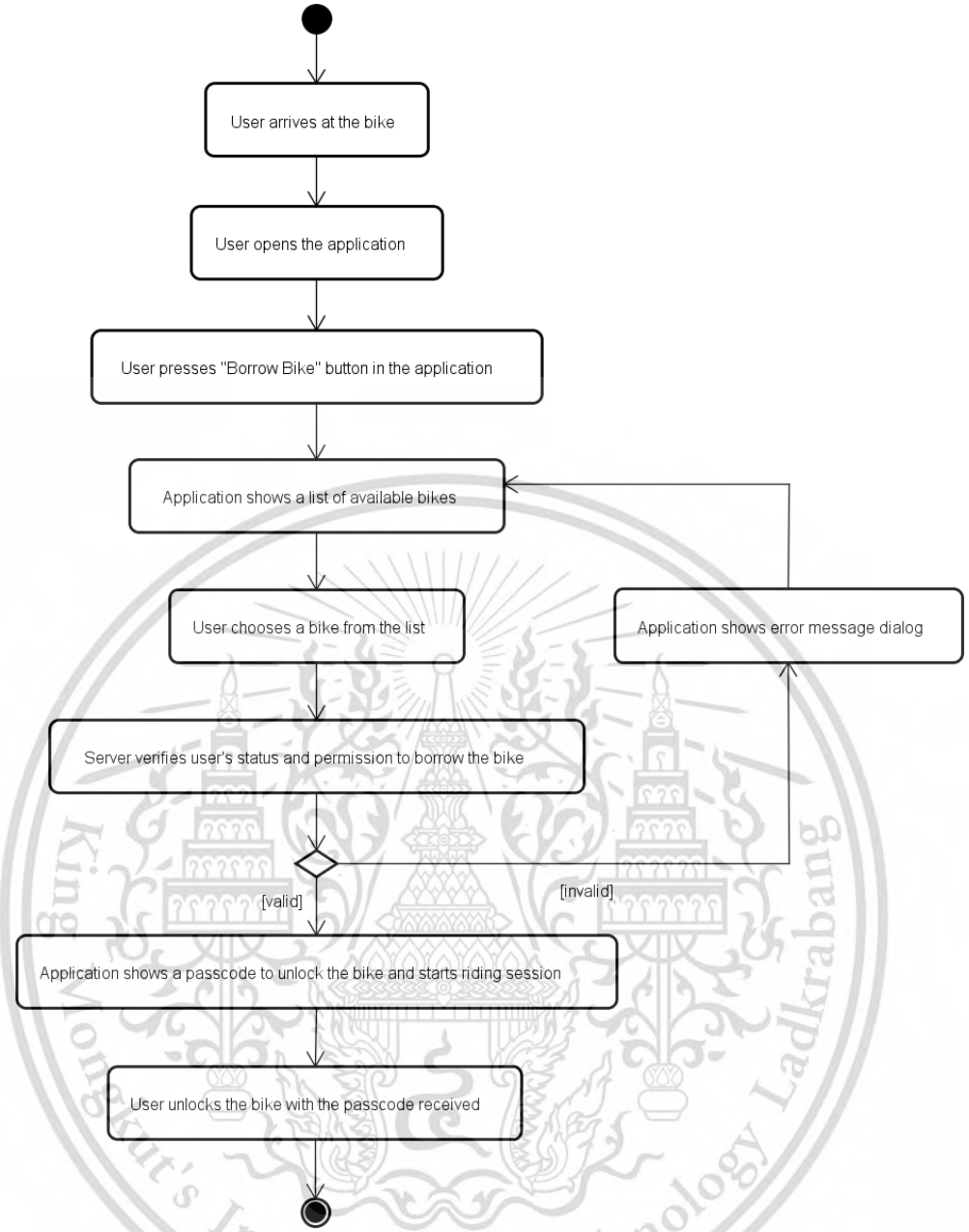


Figure 7-1: Borrowing a bike in TF1

The test flight was launched with two different types of bike: a city and commuting model. Table 7.1 lists the details of these models. The pictures of bikes can be seen in Figure 4-5 and Figure 4-6. The reason for the different types of bike is to accommodate both commuting and shopping for students and staff in KMITL. After the test ended, the number of usage in each type of bike will be counted and determine the ratio of future purchase for the bike.

Table 7.1: Bike Types

Model	LA City Green	GIANT Escape 3
Type	City Bike	Commuting Bike
Size (Seat Tube)	16"	XS/15" and M/19"
Number of seats	2	1
Price (THB)	3,500	8,800
Amount in service	3	5

Currently, KMITL students have two account used for access several institution facilities: generation 1 and 2 account. As for the authentication process of the system, users can use their KMITL account, both generation 1 and generation 2 account, to directly connect to the application. That way, users could be verified if they are actually students or staff in the university or not.

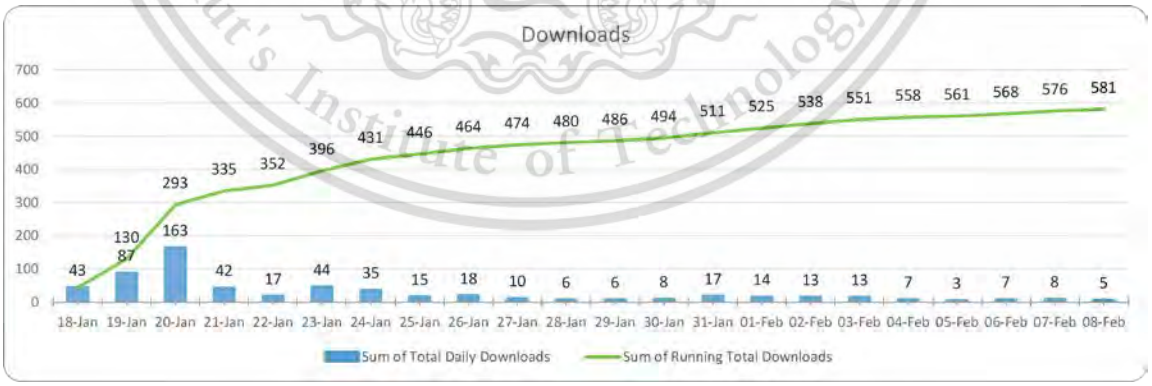
Figure 7-2: Picture of LA City Green bicycle

Figure 7-3: Picture of GIANT Escape 3 Bicycle

7.2.1 Results

The graph in Figure 7-4 represents the number of application downloads from January 18, 2017 to February 8, 2017. On the first day, the application starts off with 43 downloads. The day after, the application was promoted in the "KMITL Green Campus" page on Facebook, causing the number of downloads to slightly increase until it reaches the peak at 163 downloads in January 20. After that, the number sharply drops and fluctuates moderately throughout the rest of this Test Flight. Overall, the total amount of downloads grows linearly.

Figure 7-4: Number of downloads during TF1



Similar to the previous graph, the graph in Figure 7-5, which indicated the number of users, portrays the same growth. However, the actual numbers are different. The number of Figure 7-5 is less than that of Figure 7-4 due to some users who downloaded the application out of curiosity might not belong to KMITL community.

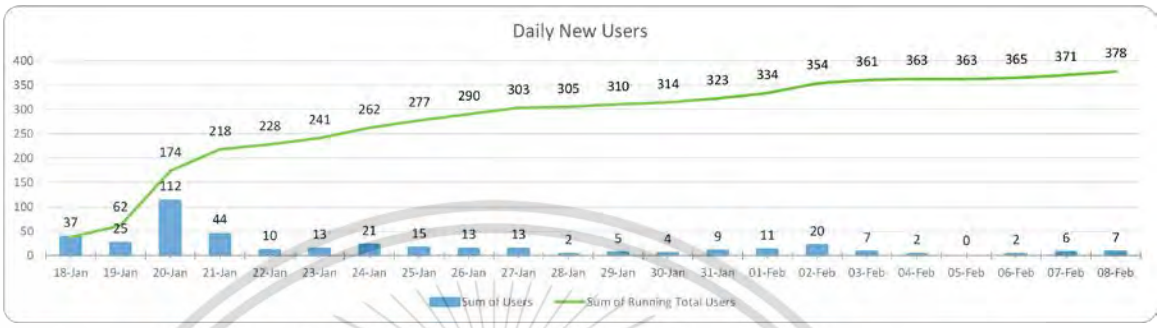


Figure 7-5: Number of users during TF1

As for the session, Figure 7-6 represents the usage of the application in each day during this Test Flight. The information between January 18 and January 24 is not available due to technical issues in the server that caused the loss of information in the database. The number of sessions during those time is approximately around 150 sessions. Nevertheless, the information in hand is still sufficient to arrive at an appropriate conclusion. It is possible to deduce from this graph that the day of week hold an impact on number of sessions as they are especially low on weekend. There are even a day on weekend with number of sessions as low as 5 on Feb 5.

Figure 7-6: Number of sessions during TF1

7.3 Test Flight 2: Barcode

After gathering feedback and improving system upon the last test flight, the system was relaunched on February 17, 2017 until May 11, 2017. Few changes were made for this test flight and all in regard to difficulties and incidents in the previous test.

With generation 1 accounts fading out, users registered with those will not be able to log into the system in the future. As a result, they were required to register again with the system using generation 2 account. Correspondingly, the system now limit new registration to only generation 2 accounts. However, since there still were unfamiliar users with generation 2 account, they will be prompted with texts and link to guide them through the steps to create a generation 2 account before creating an account for the system. Figure 7-7 compares the difference between previous test login screen and this test login screen.

Figure 7-7: Comparison between the login screen in TF1 and TF2

Figure 7-8: Sample of bike barcode

For location accuracy problem, barcodes were implemented in replacement to selection from bike list. Figure 7-8 shows a picture of the barcode that was on one of the bike. Prior to this, user could potentially borrow the bike without actually being near the bike, causing the bikes' locations to be misplaced. Figure 7-9 illustrates the new flow of user borrowing the bike with barcode schema implemented.

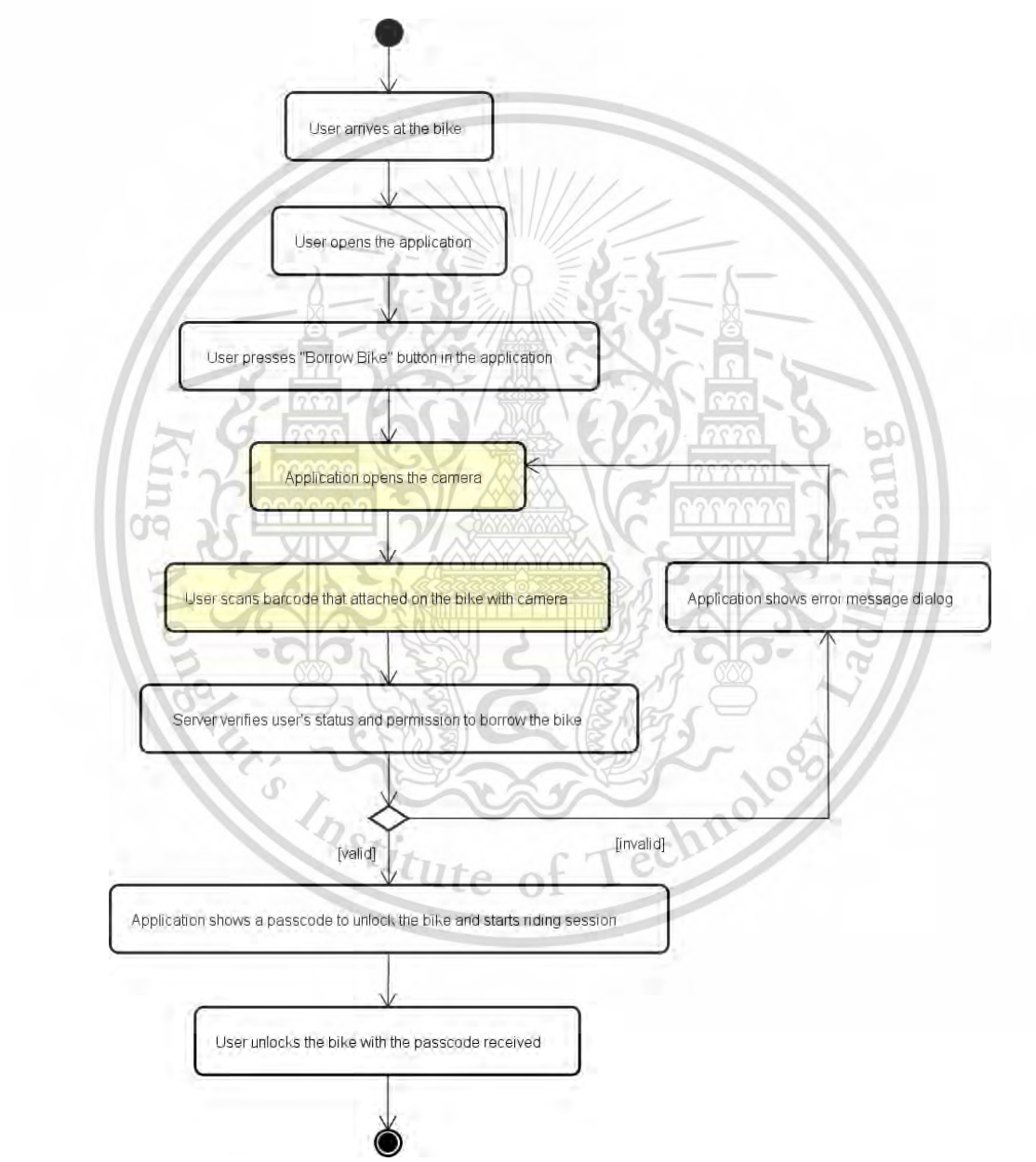


Figure 7-9: Borrowing a bike in TF2 (yellow indicates new changes)

At first, the solution for this problem was to filter users' location to those within a limited area around the bike. Unfortunately, due to inaccuracy of mobilephones' GPS, it may cause unexpected event where users may not be able to borrow the bike that is in front of them. Thus, having barcode will prevent such an event from happening as well as verifying that user is in vicinity of the bike in order to borrow it. Figure 7-10 display an instruction dialog from the application, which is a change from bike selection screen in Figure 6-5.

Figure 7-10: Instruction dialog in TF2

As for incidents where users rode the bike outside the specified area, terms and conditions and warnings were given in the application to restrict those kind of act. This will allow bike maintenance teams to easily take care and retrieve the bikes.

Figure 7-11: Test Flight Area

7.3.1 Results

The graph below in Figure 7-12 describes the number of downloads during Test Flight 2 which were held from February 17, 2017 to May 11, 2017. Continuing from the first Test Flight, the number of downloads stays low with a little oscillation of ups and downs. The highest amount of downloads are on February 20 with 10 downloads, which are considerably scarce compared to the initial launch of the first Test Flight. The reason behind this could be that daily downloads had reached its saturation point.

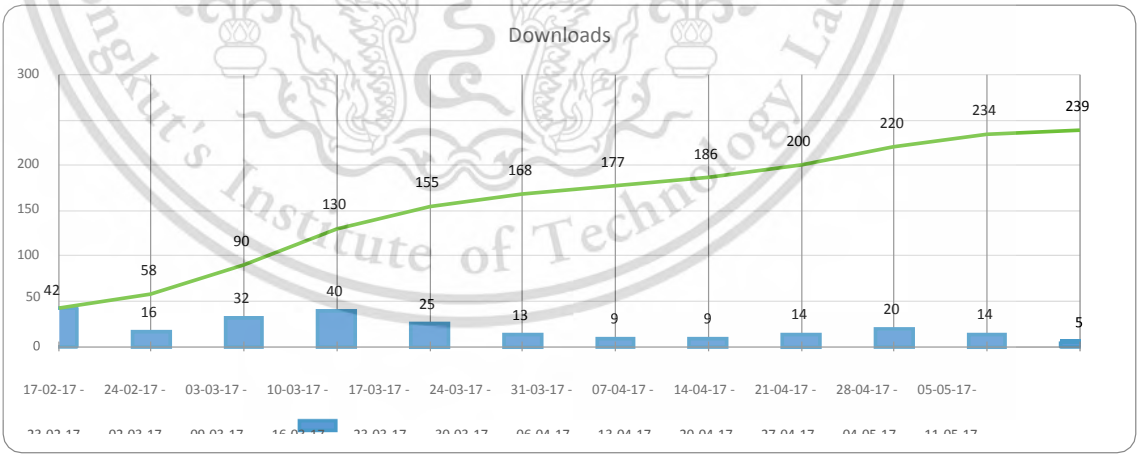


Figure 7-12: Number of downloads during TF2

Coincidentally, the graph in Figure 7-13 shows resemblance to Figure 7-12. The growth of both graphs are linear with identical slope. The actual numbers are unexpectedly similar as well. Still, there are few users with multiple accounts with different ID from both Generation 1 and Generation 2 KMITL account mixed in the count, so the numbers could probably be lower. Overall, there is no significant change from the first Test Flight.

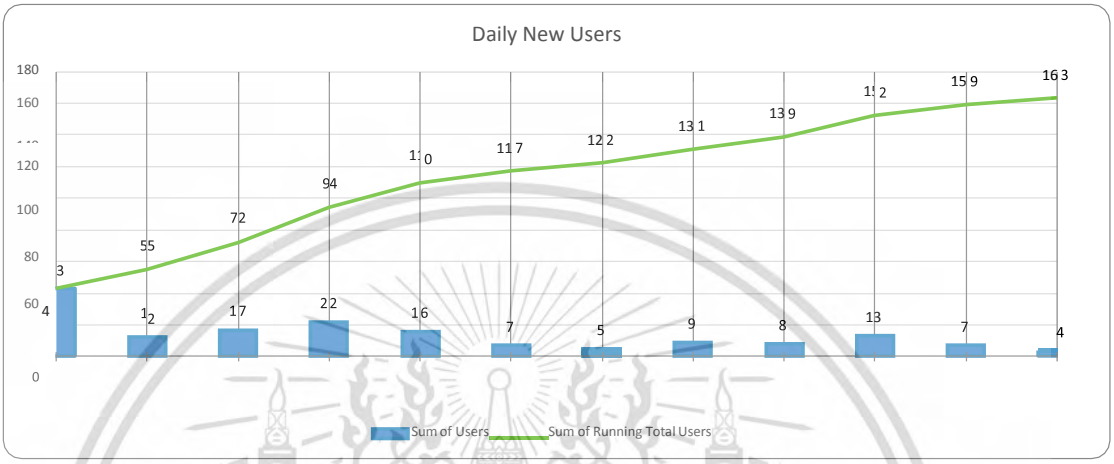


Figure 7-13: Number of users during TF2

Regarding the daily usage of the application during Test Flight 2, the graph in Figure 7-14 provides similar information to Figure 7-6 of first Test Flight except that the number is lesser. Nonetheless, the number of sessions appears to be higher than the number of downloads and the number of users, since there are regular users who use the service from time to time.

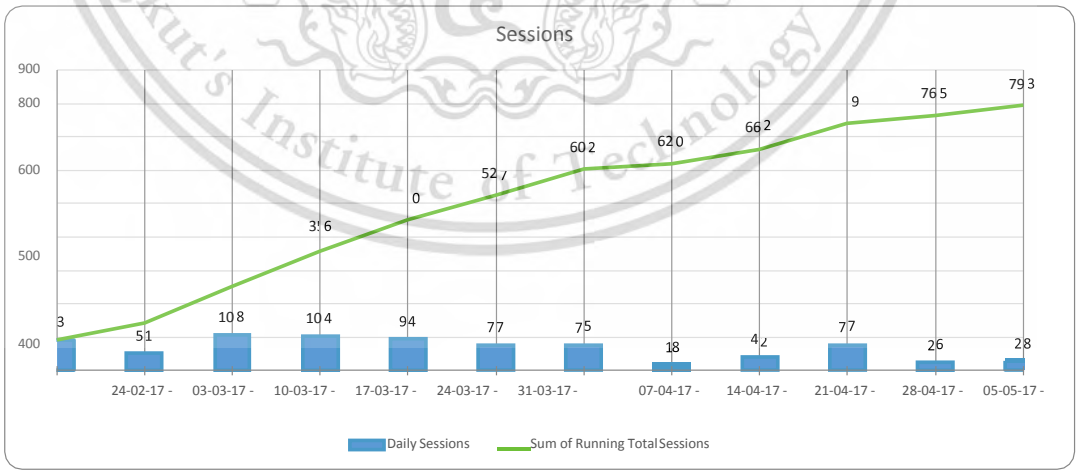


Figure 7-14: Number of sessions during TF2

7.4 Overall Discussion

Lots of data have been gathered during the two Test Flights. This section summarized the data since the beginning of the project until the end of Test Flight 2 (January 18, 2017 – May 11, 2017).

7.4.1 Downloads, New Users, Sessions

In the first week, the system received a tremendous amount of interest from the several announcements on social media and posters throughout the testing site. However, from Figure 7-15, it seems that the system have reached its saturated point in the first week making the downloads in the later weeks to be relatively low when compared to the first week. As for the amount in Figure 7-16, most of the new users appeared during the first week then leveled off in the following weeks for the same reason. Figure 7-17 shows the usage sessions of the application per week. It can be deduced that a lot of people were hype about the system in the beginning then began to loose interest later. Additionally, problems of inaccurate location of the bicycle also leads to frustration and unsatisfied users. It is also important to note that prior to the barcode schema implemented in Test Flight 2 it is very likely that users press borrow and return bike without actually using it as well. This is the underlying reason behind misleading high amount of usage before Test Flight 2.

Please note that the system was closed for maintenance during February 9, 2017 – February 16, 2017.

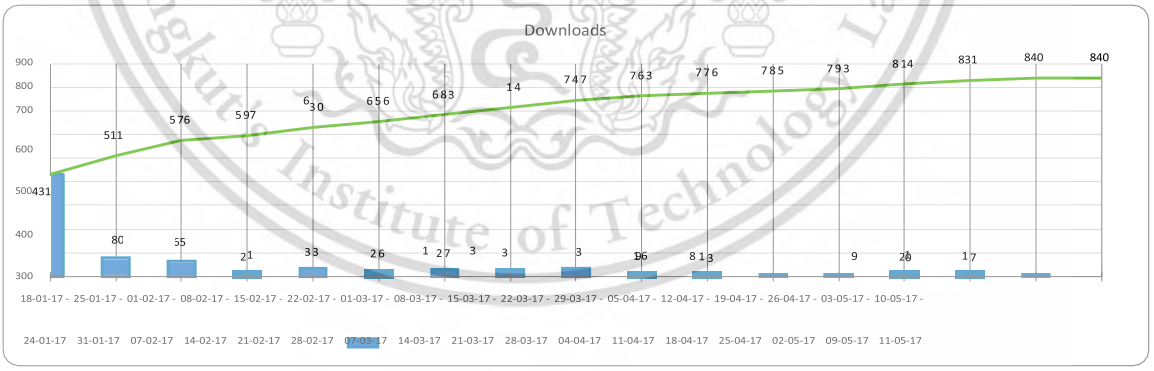


Figure 7-15: Summary of Downloads

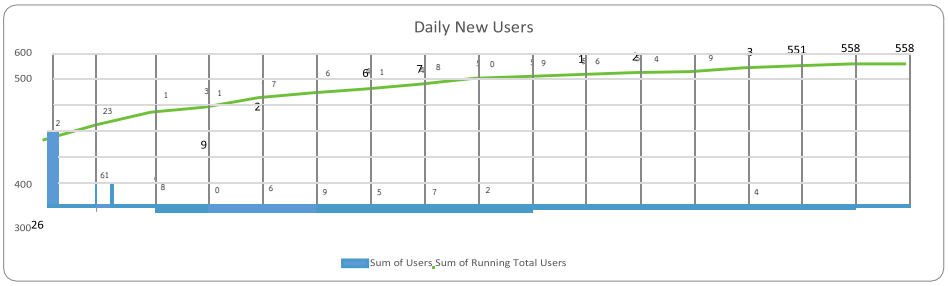


Figure 7-16: Summary of New Users

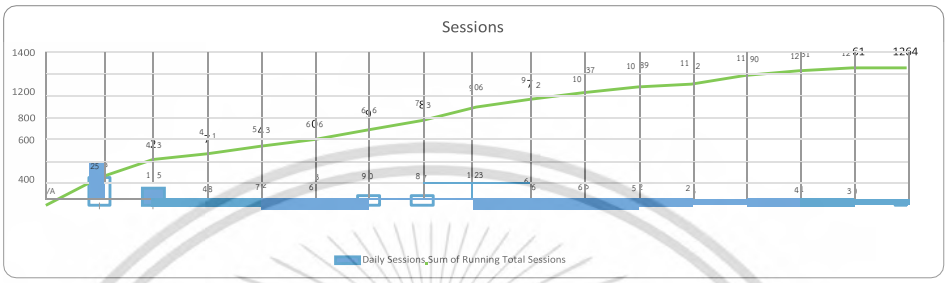


Figure 7-17: Summary of Usage Sessions

7.4.2 Users' Preferences

Since the launch of KMITL Bike, there are over 1200 sessions of borrowing bicycles. It is vital for the team to understand users' preferences in order to further improve the system towards users' demands.

Figure 7-18 and 7-19 visualizes the usage of each type of bike categorized by their gender. Figure 7-18 shows that over 78 percent of male users use the Escape 3 bikes while only 60 percent of female users use them. Two possible explanations are:

1. The design of Escape 3 bikes as seen on Figure 7-3 contains a top tube which make them difficult for female users wearing skirts to get on the bike.

2. Female users prefers a two seats model. From the team's observation, LA City Green bikes were usually rode by two passengers.

The reason why female users use more Escape 3 might be because of the lower availability of LA City Green bikes.

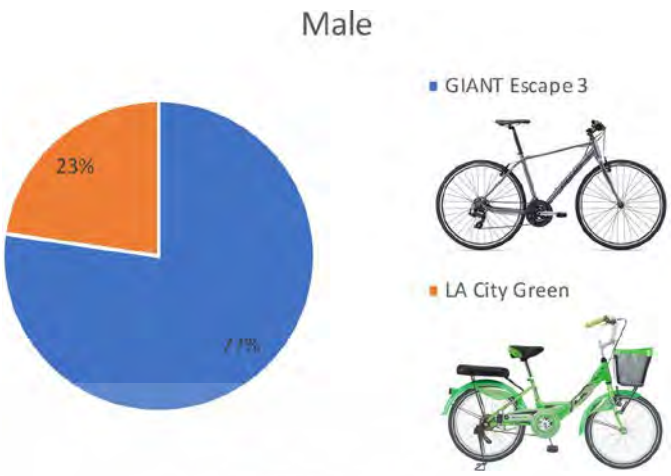


Figure 7-18: Male usage of different bike

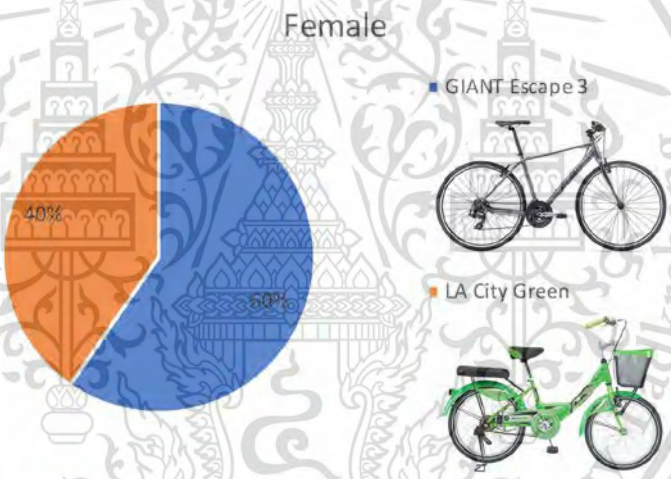


Figure 7-19: Female usage of different bike

Observing from Figure 7-20, the top three users were from the Faculty of Engineering, International College, and Faculty of Science, respectively. It could be inferred that the high usage came from the short distance between the main deployment area of the system. Still the distance is not the only factor for the difference in usage. With College of Data Storage Innovation and College of KMITL Nanotechnology being considerably near the testing site, it still had comparatively low usage to International College of the same distance. There seemed to be other influences on the usage. It was probably due to the size of each department as well, since those two departments had lowest amount of students among all other departments.

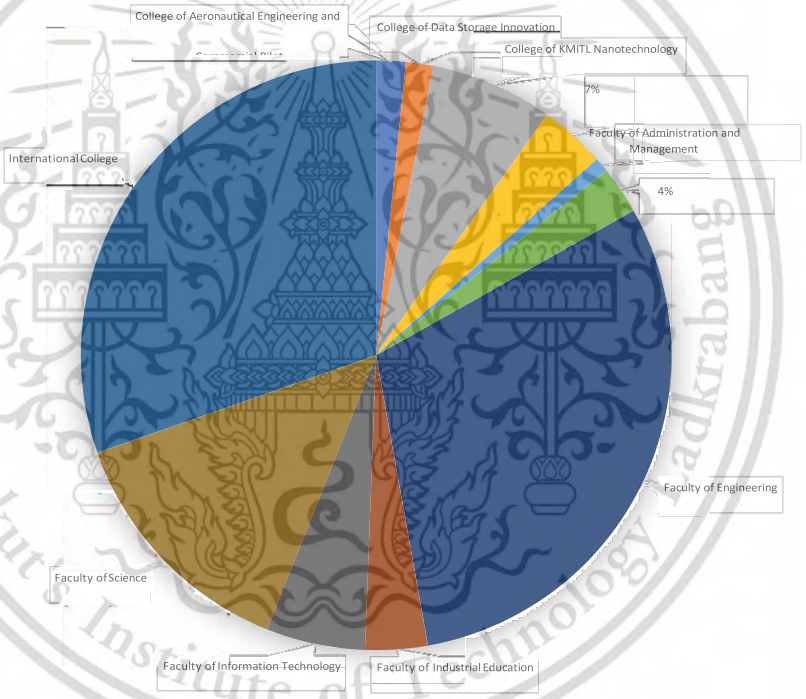


Figure 7-20: Usage by College and Faculty

Chapter 8
Conclusion

8.1 Summary

KMITL Bike was proven to be a difficult task when introduced into real-world testing. Several bugs and glitches were quickly found in the system since the first week of testing as there were over 150 sessions estimated usage sessions in just 6 days. Many students and faculty members from different faculties all over the institution showed their interest in the service. Several students post on social media and blogs review and feedback of the system. As of May 11, 2017 there are a total of 840 downloads, 1264 sessions, and 558 accounts from Test Flight 1 and 2 proved that KMITL students and faculty members are interested in the KMITL Bike service. However, due to technical difficulties the next test flight with the new lock unit will not be able to happen within the time of the submission of this document. This project can be considered a successful run.

8.2 Problems and Lesson Learned

Throughout the development of the project, there are several issues along the way that cause the project to take too much time than what was expected. In the process of solving them, there were lessons taught along the way.

8.2.1 Inexperience

Most of the problem are caused by the low experience in many new fields. For example, modeling 3D models poses a challenge for a team that are all Software Engineering students. However, trying to follow standard coding conventions and design patterns for better future code maintainability and scalability also requires going through several books and examples. Overall, time management must be done well to cope with the inexperience in this field.

8.2.2 Design for Real-World Use

Designing the app for using by the public with different platforms proves to be a challenge. Each platform has a different design language (i.e., Android uses Google's Material Design and iOS uses Apple's iOS Human Interface Guidelines). It is

essential to make the app intuitive for the users of each platform to follow the design language and guidelines set for their platform. Aside from following the guideline, users' feedbacks are also important and fixes are made accordingly.

8.2.3 3D Prototyping

In the hardware development process, over fifty prototypes were produced. This could not be achieved without a 3D printer. However, that does not mean it is nontrivial. 3D printing technology is not as matured as traditional 2D-based printing. It is not possible to select all the models and print them all at once. Each model must be exported to a printable file separately. The 3D printer's speed and temperature of both the nozzle and printing bed must be manually set and tweak occasionally in order to print some specific models. It takes several attempts of trial and error in the beginning and ever so often tweak for a specific model. Printing speed is also not that fast to ensure minimum error. It took at least 8 hours to print one prototype package which takes up time.

8.2.4 Moving to Metal

3D printing is a technology that was taken for granted. It is capable of printing complex shapes and sharp edges, something that traditional milling could not. This raises a problem when changing from plastic model to metal model. To lower the cost of CNC milling, the design needed to be drastically changed to have no sharp or narrow corners and take as much infill as possible.

8.2.5 Finding & Ordering Parts

Due to the limited space available to put the lock on the bike, the lock size must also be considerably small. This cause components in the lock unit to be hard to find due to the small size. In a case of the solenoid used in the latest prototype, the part was shipped from China which took several weeks to arrive.

8.3 Achievements

During the research, we have achieved several accomplishments as follows:

- Two research papers which are published in SCOPUS [12][13]. Both papers are shown in Appendix A1 and B1, respectively.
- Several key app and lock designs and related know-how in bike-sharing operation and development
- Real-world users feedbacks and riding statistics

8.4 Future Work

Regarding the aspect of the lock unit in KMITL Bike, here are some of the things that can be improved:

- Display status on the lock unit for diagnostic
- Increase battery life
- Integrate alarm buzzer to alert user and surrounding in case of theft
- Integrate real-time GPS tracking
- Optimize rainproof sealing and design
- Optimize design for mass production (e.g. reduce size, weight, and cost)
- Use dynamo to recharge the unit

Regarding the aspect of the application service in KMITL Bike, here are some of the things that can be improved:

- Add user feedback report
- Add user summary usage dashboard (e.g. social media related features, user's fitness level)
- Add ride history statistics (e.g. show graph of usage per month, show usage heat map)
- Add system near real-time statistics report generator in the backend system for system administrator
- Enable user to use the bike outside of the campus while ensuring that the user will always secure the bike and return the bike within the service area
- Increase service area
- Refactor code to Model-View-Presenter based design

References

[1] C. Tang and H. Lean, "Will Inflation Increase Crime Rate? New Evidence from Bounds and Modified Wald Tests", Global Crime, vol. 8, no. 4, pp. 311–323, 2007.

[2] M. Ceccarelli, International Symposium on History of Machines and Mechanisms. Dordrecht: Kluwer Academic, 2004.

[3] Medani, A., Gani, A., Zakaria, O., Zaidan, A. A., Zaidan, B. B., "Review of mobile short message service security issues and techniques towards the solution", Scientific Research and Essays, 6(6), 19. doi: 10.5897/SRE11.107, 2011.

[4] P. Sawer, "The unsung genius who secured Britain's computer defenses and paved the way for safe online shopping", Telegraph.co.uk, 2016. [Online]. Available: hwho-secured-Britains-computer-defences-and-paved-the-way-for-safe-online-shopping.html. [Accessed: 03-Dec-2016].

[5] W. Stallings, Cryptography and Network Security: Principle and Practice, 5th ed. Boston: Prentice Hall, 2011, p. 267.

[6] "Bluetooth Low Energy | Bluetooth Technology Website", Bluetooth.com, 2016. [Online]. Available: https://www.bluetooth.com/what-is-bluetooth-technology/how-it-works/low-energy [Accessed: 03-Dec-2016].

[7] "Bluetooth Smart For Android", Possiblemobile.com, 2016. [Online]. Available: https://possiblemobile.com/2013/12/bluetooth-smart-for-android/ [Accessed: 03-Dec-2016].

[8] Industry ARC Analysis, "Bluetooth Smart/Bluetooth Low Energy Market: Applications (Consumer Electronics, Healthcare, Sports & Fitness, Retail, Automotive, Security); By Technology [Discrete Modules, Integrated Modules (Single & Dual Mode)]-Forecast (2017–2022)", 2017.

[9] F. Lamb, Industrial Automation: Hands On, 1st ed. McGraw-Hill Education, 2013, pp. 74–75.

[10] "APK Decompiler - Decompile Android .apk", Javadecompilers.com. [On-line]. Available: http://www.javadecompilers.com/apk. [Accessed: 03-Dec-2016].

[11] "Arduino-info - Bluetooth-HC05-HC06-Modules-How-To", Arduino- info.wikispaces.com, 2016. [Online]. Available: https://arduino-info.wikispaces.com/Bluetooth-HC05-HC06-Modules-How-To. [Accessed: 10-May-2017].

[12] Tep S., Anantavrasilp I., "Robust Image Encryption Method with Cipher Stream Chaining Process", *Proc. of IEEE 4th International Conference on Computer and Communication Systems*, Singapore, 2019.

[13] Choosaksakunwiboon S., Terawong C., Suttisirikul S., Anantavrasilp I., Thiemjarus S., Wisadsud S., Kaemarungsi K., "A Pre-processing Technique for BLE-based Indoor Localization", In: *Proc. 12th International Convention on Rehabilitation Engineering and Assistive Technology (i-CREATe 2018)*, Shanghai, 2018.

Appendix

A1

A Pre-processing Technique for BLE-based Indoor Localization

A Pre-processing Technique for BLE-based Indoor Localization

Shanatip Choosaksakunwiboon, Chawin Terawong, Suppakorn Suttisirikul, Isara Anantavrasilp
King Mongkut's Institute of Technology Ladkrabang
Bangkok, Thailand

Surapa Thiemjarus*, Sodsai Wisadsud, Kamol Kaemarungsi
National Electronics and Computer Technology Center
Thailand

ABSTRACT
Indoor localization has long been an active area of research, in order to overcome the problems of locating people or objects in an indoor environment. In this paper, we propose a pre-processing technique that aims to improve the accuracy of indoor localization in healthcare application using Bluetooth Low Energy (BLE). This paper analyzes the effect of BLE communication channels and device orientation on the accuracy of distance estimation. The proposed channel separation preprocessing technique can improve distance estimation based on the Received Signal Strength Indicator (RSSI) of the Bluetooth signal by achieving a Root Mean Squared Error of 1.194 and standard deviation of 0.713.

Categories and Subject Descriptors
C.4 [**Performance of Systems**]: Modeling Techniques.
J.3 [**Life and Medical Sciences**]: Medical Information Systems.

Keywords
localization, indoor positioning system, RSSI, BLE, log-distance path loss model, channel separation

1. INTRODUCTION
In hospitals, the safety of patients is one of the most important factors that needs to be concerned. Indoor localization can be of use in many ways in order to aid patients and improve the patients' safety. For instance, an elder patient can accidentally fell on the ground somewhere in the hospital building. The system can immediately alert the nurses and doctors where the patient is located. Several studies proposed an indoor positioning system (IPS) for healthcare applications. For instance, [1] and [2] introduce systems that rely on Radio Frequency Identification (RFID) technology to track humans in the hospital.

BLE-based indoor localization is also widely used in many hospitals. BLE is one of the most commonly used wireless signal today for indoor localization because the Bluetooth module is equipped in almost every mobile device due to its power-saving nature. Although BLE is a prominent wireless solution for IPS, BLE-based systems tend to suffer from low accuracy detection due to their ultra-low power consumption. The effective range of BLE transmitter is usually set to 2 meters in order to save battery power and cost [3]. Several studies proposed indoor localization technique based on Apple iBeacons. Li et al. [4] used iBeacon to establish an in-room newborns localization system in a hospital. Yang et al. [5] provided navigation guidance for patients who had trouble finding the department or ward. Several studies on BLE-based indoor localization [6-8] reported very low accuracy, with up to 5 meters estimation errors.

Our goal is to improve the accuracy of tracking service of elderly people and patients using BLE. This paper presents a detailed analysis of the effect of BLE communication channels and the device orientation on the distance estimation accuracy. Several pre-processing techniques have been investigated and a pre-processing technique for improving the distance estimation accuracy through advertising channel separation by K-means clustering has been proposed.

2. RELATED WORKS
Existing works related to the development of indoor localization can be classified according to the media used to estimate the location, namely, infrared (IR) signal, sound, geomagnetic field and radio signal. Related works on these media will be briefly discussed in this section.

IR is one of the earliest commonly used media in IPS. Active Badge [9] is one of the examples for IR-based IPS. The badge worn by the target object continuously transmits a signal providing an information about its location. IR wave is fairly accurate for short range detection within a single room, since it cannot penetrate opaque objects such as walls.

Active Bat [10] and Cricket [11] are two examples of IPS that use ultrasound signals. The Active Bat system was equipped with a matrix of fixed reference nodes that act as ultrasound receivers on the ceiling. The tag worn by a person emitted ultrasound signals which were captured by the receivers on the ceiling and further reported to the central server. Cricket system enhanced Active Bat by using ultrasound with radio frequency signal to increase the coverage area of the positioning system. Beep [12] used audible sound as a medium to locate the target object indoor, resulting in an estimation accuracy of 0.6 m.

Easyshopping [13] is an example of application that use earth's geomagnetic-field for indoor navigation in a shopping mall. The shopping carts contain a touch screen monitor that users can use to search for the location of a particular product and navigate the users to the shelf containing that product.

Radio frequency technologies are becoming more commonly used for indoor localization since the signals have better penetration through solid obstacles such as walls and human bodies, allowing the system to have a larger coverage area. RADAR [14], by Microsoft Research, is the first RF-based IPS that provides a 2D position of the object and achieves an accuracy of about 4 m. In a RFID system, the tag gets activated by the RFID reader and returns a signal carrying the stored information about the target object [15]. In [16], based on Ultra-Wideband (UWB), Time

Difference of Arrival (TDoA) is used to compute the distance between the reference node (UWB receiver) and the target node (UWB transmitter). Yang and Shao [17] presented a WiFi-based indoor localization technique that improves the localization performance from the traditional trilateration technique, and achieved an average error of 1 meter. In [18] and [19], a comparison of the fingerprint-based and the trilateration techniques of WiFi-based localization in a rectangular room have been presented.

In the past five years, a few studies have been performed on BLE-based indoor localization, e.g., using trilateration or range-based localization [6-7] and fingerprint [8]. Topaz [20] used Bluetooth signal to estimate 2D position of objects in indoor environments. The system combined Bluetooth-based and IR-based positioning to obtain a higher accuracy. Ozer and John [21] used Kalman Filter to produce smooth RSSI readings while maintaining quick response time.

3. EXPERIMENTAL SETUP

3.1 Devices

This experiment consists of two main devices: tracker and receiver. The tracker is a BLE device which transmits Bluetooth signal and the receiver is used to record the RSSI associated to the tracker. Fig. 1 shows the devices used in this study. The AiR (Autonomous Intelligent Recognition) node is a custom-made miniaturized wearable sensor, developed based on the nRF51822 module by Imperial College London and NECTEC, for activity and behavior monitoring sensor. Raspberry Pi 3 is used as the receiver. The device comprises Quad Core 1.2 GHz Broadcom BCM2837 64bit CPU, 1 GB RAM, BCM43438 chipset for WLAN and BLE on board.

Fig. 1 Data Collection Devices: AiR Node (left) and Raspberry Pi 3 (right)

3.2 Data Collection

In this study, all the RSSI datasets are collected in an open area inside the 6th floor of the International College building in King Mongkut's Institute of Technology Ladkrabang (KMITL) with no obstacles between trackers and receivers. Fig. 2 illustrates how the devices are set up in the data collection process.

Fig. 2 Data Collection Setup

The receiver and the tracker are placed on the stands with a height of 1.15 m. The receiver is placed at a fixed location. A set of RSSI values are collected at each distance and orientation at a 10 Hz sampling rate. The BLE tracker is placed at varying distances of 0.5 to 7 m at 0.5 m incrementing interval from the receiver. At each distance, the tracker is placed in 4 different orientations, i.e., 0, 90, 180 and 270 degrees (rotated toward the receiver), as shown in Fig. 3. For each setting, a total of 200 samples was used. The train and test datasets were collected on two different days.

Fig. 3 Device Rotation (receiver is on the left)

4. DATA ANALYSIS

4.1 Path Loss Model

The distance between the tracker and the receiver can be obtained using the path loss model. The equation of the model is as follows:

$$RSSI_d = RSSI_{d_0} - 10n\log_{10}\left(\frac{d}{d_0}\right) + X_\sigma \qquad (1)$$

where $RSSI_d$ represents RSSI in dB measured at a target distance d, $RSSI_{d_0}$ is RSSI measured at the reference distance d_0. X_σ is a zero mean Gaussian random variable with a standard deviation of σ (the value of which is context-specific). n is the path loss exponent that describes the obstructions in the environment where the RSSI data is collected. Given the collected RSSI data, n can be calculated empirically, in prior, for each area through curve fitting. Given the coordinates of the reference receivers, the estimated distances can be further used to determine the coordinate of the tracker through a method called trilateration or range-based localization [19].

4.2 Data Pre-processing

In this paper, we explore the effect of different pre-processing techniques on distance estimation performance. Two different measures of central tendency are applied for data preprocessing, namely, moving average (M1) and moving median (M2). The filtering techniques are used to filter out the outliers of the collected RSSI data, by calculating the mean and median of the RSSI data over a specific window size.

BLE has 40 physical channels, three of which are used for broadcasting its advertising packets. Due to this nature of BLE, a channel separation pre-processing technique is used. The collected data is separated into three clusters prior to the computation of the path loss model for each advertising channel. For each channel, the mean of the set of RSSI of each distance is calculated then curve fitting is applied to obtain the path loss model. For distance estimation, K-means clustering is performed to distinguish which of the three channels the data belongs to. The top cluster represents channel 1 (M3.1) containing a set of highest RSSI values, the middle cluster for channel 2 (M3.2) and the bottom cluster for channel 3 (M3.3).

5. EXPERIMENTAL RESULTS

We first investigate the effect of device orientation on the model performance. Fig. 4 illustrates the path loss models obtained by fitting a curve through the distance-specific means of the training dataset for each device orientation. The result implies that vertical rotation of the BLE tracker can systematically affect the RSSI values. Angle 0 has lowest signal strength, followed by angles 180, 90 and 270, respectively. After 2.5 meters, the curve for Angle 0 starts to overlap with the curves of angle 90 and angle 180. This could be due to the degradation of signal strength as the distance increases, thus the signal is less stable. Incorporating the device orientation information into the path loss model, therefore, are likely to improve the distance estimation accuracy.

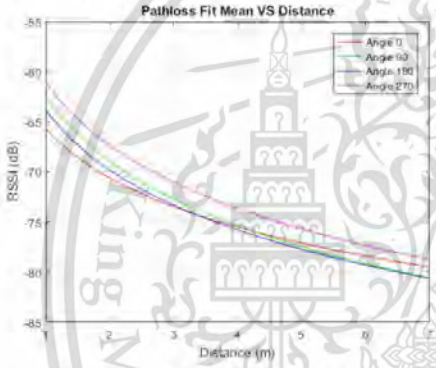


Fig. 4 Mean Curve Fitting of All Angles

The next step is to demonstrate the performance of different pre-processing techniques on distance estimation. The path loss models are created based on the training dataset collected during angle 0. Different pre-processing techniques are performed on the training set including moving average, moving median and the channel separation technique. The test dataset is used for distance estimation. Since device orientation can affect the accuracy, experiments are performed to compare the estimation results based on the data extracted from a known device orientation (Angle 270) and unknown device orientation (all angles). The test dataset is pre-processed by the aforementioned technique before substituting into the corresponding path loss model to obtain the distance. For pre-processing with channel separation, the test data is first separated into three clusters by K-means clustering and each cluster is further filtered by moving average prior to distance estimation. In this study, a fixed window size of 20 samples and a shifted window of size 1 are used.

Table 1 shows a performance comparison among different pre-processing techniques based on Root Mean Squared Error (RMSE), minimum absolute error, maximum absolute error and the standard deviation (SD) of the absolute errors. The RMSE of distance estimation with M1 (moving average) is 1.599 for unknown device orientation, and slightly reduces to 1.477 for known device orientation (Angle 270). Pre-processing by M2 for known device orientation yields a higher RMSE of 1.94. Since M1 outperforms M2, we apply M1 to the data of each channel obtained from channel separation. As a result, estimation by M3.1, M3.2 and M3.3 with known device orientation yields RMSE of 1.401, 1.194 and 1.67, respectively. The channel separation pre-processing technique indeed improves the accuracy of the distance estimation except for M3.3, where M3.2 has the lowest RMSE, maximum error and SD of absolute errors among all channels in this experiment.

Fig. 5 shows the bar graph of RMSE resulted from the distance estimation based on M3.2 pre-processing technique versus different distances. The error bar indicates the resulting minimum and maximum absolute errors. Notice that apart from 2.5 meters and from 5 to 6 meters, the RMSE from the distance estimation with known angle (shown in red) are lower than the RMSE from unknown angle (shown in green). Distance estimation with unknown angle tends to produce error bars with larger range and higher maximum absolute errors. This implies that distance estimation with unknown device orientation produce a more scattered and less reliable output.

According to the results, M3.2 pre-processing technique with known device orientation achieves an RMSE of 1.194 and SD of 0.713. This illustrates that choosing the correct channels for distance estimation and device orientation information can effectively improve the performance of the system.

Table 1. Distance Estimation Performance for Different Pre-processing Techniques

Pre-processing Techniques	Angle 270				Unknown Angle			
	RMSE	Minimum absolute error	Maximum absolute error	SD	RMSE	Minimum absolute error	Maximum absolute error	SD
M1	1.477	0.011	5.562	1.069	1.599	0.003	7.633	1.165
M2	1.940	0	9.106	1.488	2.660	0	20.08	2.144
M3.1	1.401	0.012	2.544	0.783	1.626	0.010	7.166	1.082
M3.2	1.194	0.025	2.372	0.713	1.400	0.011	3.634	0.835
M3.3	1.670	0.001	4.805	1.168	1.821	0.001	6.284	1.265

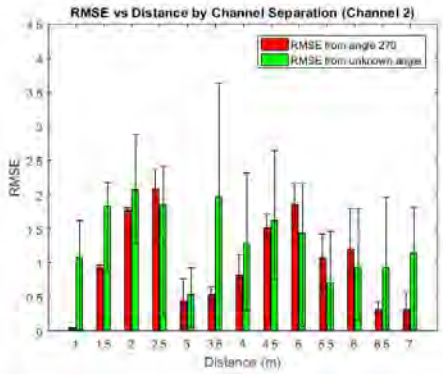


Fig. 5 RMSE of Distance Estimation by Channel Separation Pre-processing (Channel 2)

6. CONCLUSION

In this paper, we studied the effect of tracker orientation and the different BLE advertising channels on the signal strength. A BLE channel separation pre-processing technique is proposed. By comparing the path loss models from the means of RSSI collected through 4 different angles of rotations for different distances, we see a systematic change in the RSSI values. Using the channel separation technique, we obtain a lower RMSE and SD of the estimation errors compared to the conventional method that uses moving average and moving median filtering. Furthermore, using channel separation with known angle of BLE tracker produces better results than unknown angle. From the results, we conclude that a combined use of channel separation with device orientation information can improve the performance of BLE-based indoor localization by achieving an RMSE of 1.194 and SD of 0.713.

7. ACKNOWLEDGMENTS

This work is supported by a Newton Fund Institutional Links grant ID:330760239, under the Newton-Thailand Research Fund (TRF) partnership. The grant is funded by the UK Department of Business, Energy and Industrial Strategy (BEIS) and TRF and delivered by the British Council. This work is supported in part by the Anandamahidol Foundation.

8. REFERENCES

[1] Chen, W.-H., et al., *Dynamic Indoor Localization Based on Active RFID for Healthcare Applications: A Shape Constraint Approach*, in *2009 2nd International Conference on Biomedical Engineering and Informatics*. 2009, IEEE: Tianjin, China.

[2] Calderoni, L., et al., *Indoor localization in a hospital environment using Random Forest classifiers*. Expert Systems with Applications: An International Journal, 2015. **42**(1): p. 125-134.

[3] Leddy, P. *10 Things About Bluetooth Beacons You Need to Know*. 2016; Available from: http://academy.pulsatehq.com/bluetooth-beacons.

[4] Li, Z., Y. Yang, and K. Pahlavan, *Using iBeacon for Newborns Localization in Hospitals*, in *2016 10th International Symposium on Medical Information and Communication Technology*. 2016, IEEE: Worcester, MA, USA.

[5] Yang, J., Z. Wang, and X. Zhang, *An iBeacon-based Indoor Positioning Systems for Hospitals*. International Journal of Smart Home, 2015. **9**: p. 161-168.

[6] Contreras, D., M. Castro, and D.S.d.l. Torre, *Performance evaluation of bluetooth low energy in indoor positioning systems*. Trans. Emerging Telecommunications Technologies, 2014. **25**(8): p. 1-10.

[7] Jianyong, Z., et al., *RSSI based Bluetooth low energy indoor positioning*, in *2014 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*. 2014, IEEE: Busan, South Korea. p. 526-533.

[8] Faragher, R. and R. Harle, *Location Fingerprinting With Bluetooth Low Energy Beacons*. IEEE Journal on Selected Areas in Communications, 2015. **33**.

[9] Want, R., et al., *The Active Badge Location System*. ACM Transactions on Information Systems (TOIS), 1992. **10**(1): p. 91-102.

[10] Harter, A., et al., *The Anatomy of a Context-Aware Application*. The Journal of Mobile Communication, Computation and Information, 2002. **8**(2-3): p. 187-197.

[11] Priyantha, N.B., A. Chakraborty, and H. Balakrishnan, *The Cricket Location-Support System*, in *In Proceedings of the 6th ACM International Conference on Mobile Computing and Networking (ACM MOBICOM)*. 2000: Boston, MA.

[12] Mandal, A., et al., Beep: 3D indoor positioning using audible sound, in Second IEEE Consumer Communications and Networking Conference, 2005. 2005, IEEE: Las Vegas, NV, USA. p. 348-353.

[13] Kolehmainenn, V. *Easyshopping - revolutionary personalized shopping experience*. 2013; Available from: https://www.youtube.com/watch?v=ZOdJ57V32hU.

[14] Bahl, P. and V.N. Padmanabhan, RADAR: an in-building RF-based user location and tracking system, in In Proceedings of the Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM 2000. 2000: Tel Aviv, Israel. p. 775-784.

[15] Want, R., *An Introduction to RFID Technology*. IEEE Pervasive Computing, 2006. **5**(1): p. 25-33.

[16] Alarifi, A., et al., *Ultra Wideband Indoor Positioning Technologies: Analysis and Recent Advances*. Sensors (Basel), 2016.

[17] Yang, C. and H.-r. Shao, *WiFi-based indoor positioning*. IEEE Communications Magazine, 2015. **53**(3): p. 150-157.

[18] Emery, M. and M.K. Denko, *IEEE 802.11 WLAN Based Real-Time Location Tracking in Indoor and Outdoor Environments*, in *2007 Canadian Conference on Electrical and Computer Engineering*. 2007, IEEE: Vancouver, BC, Canada.

[19] Chermanomwong, P. and D.J. Suroso, Indoor localization system using wireless sensor networks for stationary and moving target, in 2011 8th International Conference on Information, Communications and Signal Processing. 2011, IEEE: Singapore.

[20] *Topaz Location System*. 2004; Available from: http://www.tadlys.co.il/pages/Product_content.asp?iGlobalId=2.

[21] Ozer, A. and E. John, *Improving the Accuracy of Bluetooth Low Energy Indoor Positioning System Using Kalman Filtering*, in *2016 International Conference on Computational Science and Computational Intelligence (CSCI)*. 2016, IEEE: Las Vegas, NV, USA

B1

Robust Image Encryption Method with Cipher Stream Chaining Process

The 4th International Conference on Computer and Communication Systems

ICCCS 2019

Singapore ❄ February 23-25, 2019

Submission Deadline: November 20, 2018

★ Proceedings

Accepted papers will be published in the conference proceedings, which will be submitted for inclusion into IEEE Xplore, submitted for indexing in Ei Compendex and Scopus.

★ Topics

- Algorithms
- Big Data
- Computer Architecture
- Data Compression
- Image Processing
- Mobile Computing
- High-Performance Computing
- Autonomic and Trusted Computing
- Parallel and Distributing Computing
- Biomedical Informatics and Computation
- Software Engineering and Knowledge Engineering
- Wireless Communications
- Network Communication
- Communications Transmission
- Network Security and Cryptography
- Wireless and Sensor Devices
- Remote Sensing and GPS
- RF and Microwave Communication
- Information and Its Technical Education
- Speech and Audio Processing
- Signal, Image and Video Processing
- Signal Detection and Parameter
- Artificial Intelligence and Machine Learning
- RF, Microwave and millimeter circuit
- Techniques of Laser
- Antenna and Propagation
- RF and Microwave devices
- Electromagnetic and Photonics
- Microwave Theory and Techniques
- Virtual Reality and Visualization
- Modulation, Coding, and Channel Analysis
- Integrated Optics and Electro-optics Devices

★ Keynote Speakers

Prof. Perry Shum
OSA Fellow, SPIE Fellow
Nanyang Technological University, Singapore

Prof. Guu-Chang Yang (IEEE Fellow)
National Chung Hsing University, Taiwan

Prof. Yang Xiao, (IET Fellow)
The University of Alabama, USA

★ History

ICCCS 2015
Kanyakumari, India | November 2-3, 2015
Publisher: IEEE Press (ISBN:978-1-4673-9756-8)
Papers of ICCCS 2015 have been indexed by Ei Compendex, and Scopus.

ICCCS 2017
Kracow, Poland | July 11-14, 2017
Publisher: IEEE Press (ISBN:978-1-5386-0539-4)
Papers of ICCCS 2017 have been indexed by Ei Compendex, and Scopus.

ICCCS 2018
Nagoya Institute of Technology, Nagoya, Japan | April 27-30, 2018
Publisher: IEEE Press (ISBN:978-1-5386-6348-6)
The conference proceedings of ICCCS 2018 is included in IEEE Xplore.

★ Committee

Conference Chairs
Prof. Yang Xiao, The University of Alabama, USA
Prof. Guu-Chang Yang, National Chung Hsing University, Taiwan

Program Chairs
Prof. Bo Yang, University of Electronic Science and Technology of China, China
Prof. Nobuo Funabiki, Okayama University, Japan

Publicity Chair
Assoc. Prof. Krzysztof Koszela, Poznan University of Life Sciences, Poland

★ Submission

1. Log in the Electronic Submission System and submit your paper;
2. Any questions about submission, please contact icccs@academic.net.

Nicole Hu icccs@academic.net www.icccs.org

Robust Image Encryption Method with Cipher Stream Chaining Process

Sovan Tep
International College
King Mongkut's Institute of Technology Ladkrabang
Bangkok 10520, Thailand
Email: 60610023@kmitl.ac.th

Isara Anantavrasilp
International College
King Mongkut's Institute of Technology Ladkrabang
Bangkok 10520, Thailand
Email: isara.an@kmitl.ac.th

Abstract— **A new image encryption algorithm that uses one dimensional logistic map combined with perceptron model is proposed. The algorithm uses logistic map to produce pseudo random sequences, which is used as sequence of keys to specify the weights of the perceptron. The, perceptron is used to encrypt the pixels of the image. The approach is also equipped with the novel Cipher Stream Chaining Process (CSCP), making it highly sensitive to given image. Our work is evaluated against histogram analysis, information entropy, key sensitivity analysis. Experiment results show that, the cipher image does not give out any information on the plain image and the algorithm is highly sensitive to plain image and key.**

Keywords: chaos; logistic map; perceptron model; encryption; security.

I. INTRODUCTION

Today, the internet is used, not only for legacy services such as email, chat or file transfer, but also social interaction, multimedia, games and other entertainment. Countless amount of non-textual data such as images, video and audio are being shared and transferred every day. This raises privacy and security concerns, especially for personal multimedia data. Several data encryption standards such as DES, triple DES, AES [1] have been introduced. However, such algorithms may only be suitable to encrypt textual data [2], but not multimedia ones. The reason is that multimedia data especially images and videos may be highly redundant (adjacent pixels may contain the same color). Thus, human may still be able to perceive the original image from the cipher image [3]. Multimedia data are also much larger than textual ones.

Recently, the encryption scheme base on the chaotic map is also considered as a good technique in cryptography [4] due to its nonlinear behavior. It also produces unpredictable condition where a slightly change in the initial point can lead to two different divergence outcomes which is the most desirable to the property of the key in cryptography.

In the last decade, many algorithms using chaos-based application have been proposed. Hanchinamani and Kulkarn [9] proposed the image encryption based on the Peter de Jong chaotic map [15] and a RC4 stream cipher [16]. The algorithms involve with three steps: 1) Permutation: Scramble the position of the row and column along with the circular rotations in the alternative orientation. This is to decorrelate the adjacent pixels of the image based on the value obtained from chaotic map. 2) Pixel value circular rotation: Changing the value of the pixels. 3) Diffusion: Spreading the effectiveness of each pixel over the entire image. Thanks to their two rounds of encryption, the scheme is very sensitive the plain image. Hence, the algorithm is robust against differential attack. Long and Tan [10] proposed multiple chaotic map for the digital image encryption. The algorithm consists of three chaotic maps: Chebyhev map, Nonlinear Chaotic Algorithm (NCA) and Logistic map. The algorithm produces the keys of the encryption and decryption which are generated by the plaintext values and Chebyshev map. The keys are then fed into Logistic map and NCA for confusing and shuffling the plain image respectively. Rohith et al. [5] proposed image encryption using 1-D logistic map because it is simple to implement but very efficient. The algorithm uses map function to generate pseudo-random sequence as the key streams. Then it applies XOR operation with a new sequence, generated from linear feedback shift register to produce another set of key streams. Finally, they use the last output key steams to confuse the image pixel by using XOR operation. Wang et al. [6] proposed encryption algorithm based on Lorenz chaotic map without XOR operation, instead they introduce a new way to scramble the image pixel value using a perceptron model. Due to the complex structure of the perceptron, it is a good approach for confusing and changing the pixel values of the image. However, [5] and [6] encrypt each pixel separately. Thus, they are not sensitive to plain text. That is, if some parts of the plain text are changed, only some parts of cipher text change accordingly. Thus, the algorithms are vulnerable to the differential analysis attack.

To be resistance to differential analysis attack, a good cryptosystem should be sensitive with respect to the given key and plain image. Even just one bit of the key is flipped, it should yield two completely different cipher images when applied to an identical plain image. Also, using the same key, even just one bit in plain image is flipped, it should produce completely different cipher images [7]. In our work, the combination logistic map and perceptron-model approach is used to encrypt pixel values. More importantly, linear feedback shift register, which improves the encryption statistic, is deployed into the cipher stream chaining process. Such approach allows for image-wide pixel-dependent encryption. As a result, when the value in even one pixel is changed, the entire cipher image is changed.

The rest of the paper is structured as follows: The encryption and decryption algorithms are explained in Section II. Experimental and result are discussed in Section III. In Section IV concludes the paper.

II. Encryption and Decryption Algorithms

A. Chaotic System and Logistic Map

Chaotic system is the type of nonlinear dynamical system which consists of a few parameter interactions and it is ruled by simple mathematic function. Despite their simplicity, the system is capable of producing a totally unpredictable value over time and widely divergent sequence parameter which is known as the chaotic behavior.

Logistic map is the one-dimensional chaotic system [8] defined by the following equation:

$$X_{i+1} = r \times X_i \times (1-X_i) \quad (1)$$

where r represents the growth rate and X_i denotes the population at a given index i. The distribution graph of the growing population X with respect to r from 0 to 4 is illustrated in the bifurcation diagram in Fig. 1.

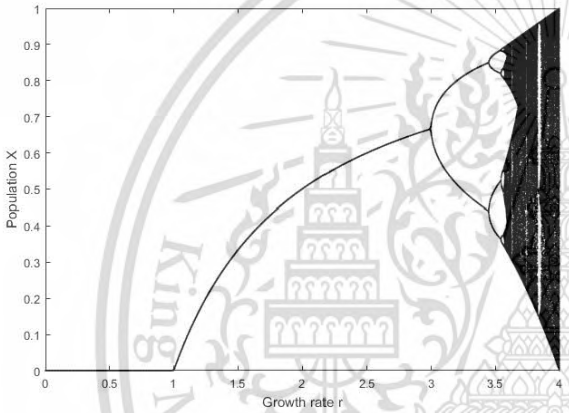


Fig. 1. The chaotic behavior of the Logistic map function.

Each vertical slide in the Fig. 1 depict the population X of 100 generations toward the 1,000 discrete values of growth parameter r. At $r < 1.0$, the system population are always almost zero. Between 1.0 and 3.0, the population starts to settle into the exact point for each generation. From 3.0, the population is bifurcated into two different path and bifurcated into four different paths after the growth rate is set to 3.4. However, after $r > 3.6$, the system begins to oscillate into two then four, eight, sixteen and so on follow 2^n formula. At $r = 3.9$, it has bifurcated so many times that the system populations jump randomly in between all the paths. In this work, the value of growth parameter r is chosen to be 3.99, where the system produces highest randomness of the population X_i.

B. Perceptron Model

Our work employs Logistic map and perceptron model to encrypt images similar to that proposed in [6]. The perceptron model is very suitable for image encryption due to the complex relationship between the input and the output of the model. However, in [6], the encryption is done on each pixel separately, making the approach vulnerable to differential analysis attack. To overcome this problem, a new encryption/decryption algorithm called Cipher Stream Chaining Process (CSCP) is introduced.

C. Cipher Stream Chaining Process

Cipher Stream Chaining Process (CSCP) is a symmetric-key encryption and decryption method that perform XOR cipher, adding previous cipher pixel on the key that is used in the current pixel. In turn, the encryption result of each pixel depends on the previous pixel, creating a chain of encryptions.

To be more precise, after a pixel is encrypted Linear Feedback Shift Register (LFSR) [5] is applied to the cipher pixel. Then it is XORed with the key used to encrypt the next pixel. This novel approach ensures that the pixels are chained to each other, making highly sensitive to given plain image. Fig. 2 shows the encryption process. Decrypting an image is simply reversing the encryption process. LFSR is applied to the cipher image. Then the result is XORed with the key. (See Fig. 3.)

Our method is a symmetric-key method such that, different pixels being encrypted and decrypted with the different keys. Corresponding plain and cipher pixels use the same key to encrypt and decrypt respectively. Detail of the encryption and decryption processes are described in the following sections.

D. Encryption Algorithms

Image encryption process is as follows:

1) Given an 8-bit grayscale image of size $M \times N$ pixels, the image can be represented as a one-dimensional array $P = \langle P_1, P_2, \ldots\ldots, P_n \rangle$, where P_i denotes values the i^{th} pixel of the image, $1 \le i \le n$, $n = M \times N$ and the value of a pixel is the 8-bit binary number corresponding to intensity of that pixel.

2) Set X_0 to any value within the range of [0,1] and r to any value between [3.99,4] as the initial parameters of the logistic map.

3) Calculate the Eq. (1) 2×n times, starting with X_0 to produce a sequence of population $X = \langle X_1, X_2, \ldots\ldots, X_{2n} \rangle$.

4) Normalize each value X_i, $1 \le i \le 2n$, as 8-bit binary representation using the following steps:

- Transform the value of X_i into unsigned integer in the range of [0, 255] by multiplying with 255:

$$X_i = X_i \times 255 \quad (2)$$

- Use round function to the sequence elements for converting them into their nearest decimal value:

$$X_i = \text{Round}(X_i) \quad (3)$$

- Convert each rounded X_i into 8-bits binary representation. This 8-bit representation will be used as encryption keys.

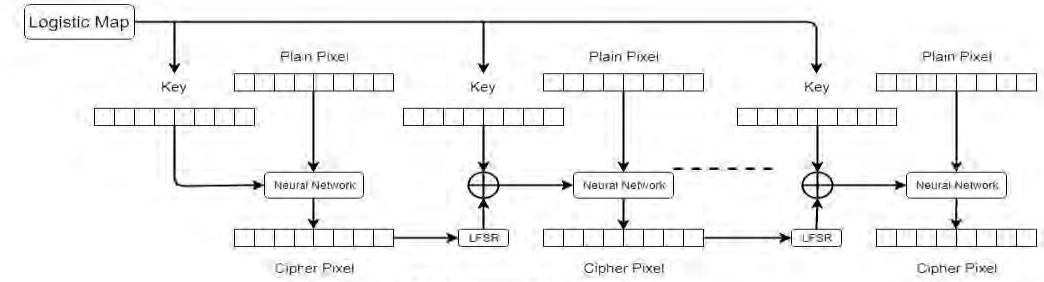


Fig. 2. Encryption Process

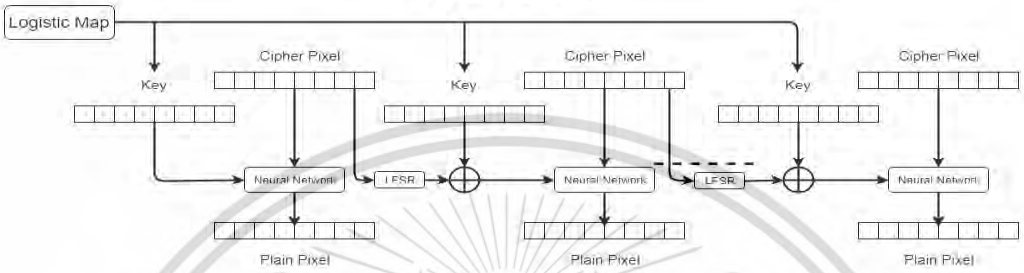


Fig. 3. Decryption Process

After repeating Step (4) for all elements in X, the sequence of the keys $K = <K_1,K_2,\ldots\ldots,K_{2n}>$, where K_i is an 8-bit representation of rounded X_i is obtained.

5) To encrypt each pixel P_i in image $P = <P_1,P_2,\ldots\ldots,P_n>$, two keys in K, K_{2i-1}, K_{2i}, are required. Both keys are fed into the structure of perceptron to generate the values of weight and threshold for the perceptron model. The algorithm for producing the perceptron model is well explained in [6]. The overview process of encrypting the a plain pixel into a cipher pixel is described in Eq. (4).

$$C_i = NeuronNet(P_i,(K_{2i-1}, K_{2i})) \quad (4)$$

where C_i, P_i, K_{2i-1} and K_{2i} denote i^{th} cipher pixel, i^{th} plain pixel and encryption keys at index $2i-1$ *and* $2i$, $1 \le i \le n$, respectively. *NeuronNet*() is the function to encrypt the pixel using perceptron model.

6) To make our method more robust to differential analysis attack, pixel-chaining process is employed.

For the first plain pixel, we encrypt it using perceptron model directly. The cipher pixel is then applied by LFSR process. Next, it is XORed with the corresponding key. The process is repeated until the last pixel is encrypted. Chaining the pixel create better chaos to the cipher image, and thus more prone to differential analysis attack. The encryption process is described in Fig. 4.

For i from 1 to n do
  If i equal to 1
    $C_i = NeuronNet(P_i,(K_{2i-1}, K_{2i}))$
  Else
    $C'_{i-1} = LFSR(C_{i-1})$
    $K'_{2i-1} = K_{2i-1} \oplus C'_{i-1}$
    $K'_{2i} = K_{2i} \oplus C'_{i-1}$
    $C_i = NeuronNet(P_i,(K'_{2i-1}, K'_{2i}))$
  End if
End for

Fig. 4. Encryption Pseudo Code

7) After finishing the Step 6, the array of cipher pixels $C = <C_1,C_2,\ldots\ldots,C_n>$ is generated. Then, the array is converted back into 8-bits grayscale cipher image. The encryption process is illustrated in Fig. 2.

E. Decryption Algorithms

In the decryption process, the cipher image is received. The procedure of the proposed image decryption process is described as follow:

1) An 8-bit grayscale of the cipher image of size $M \times N$ is obtained. It is then converted into array of pixels $C = <C_1, C_2,\ldots\ldots,C_n>$, where $n = M \times N$ and the value of a pixel is the 8-bit binary number corresponding to intensity of that pixel.

2) As the proposed method is symetric-key algorithm, the same key is used for both encryption and decryption process. Thus, the values of X_0 and r are chosen the same as Step 2 of the encryption process.

3) The value of X_0 and r obtained from Step 2 are used to generated the sequence of population $X = <X_1, X_2, \ldots\ldots, X_{2n}>$ using Eq. (1).

4) Normalize each value of X_i, $1 \le i \le 2n$, into 8-bit binary representation as described in Step 4 of the encryption process.

5) The perceptron model which is used for decrypting the pixel is the same as the encryption [6]. Thus, the process of decrypting the a cipher pixel into a plain pixel can be expressed as in Eq. (5):

$$P_i = NeuronNet(C_i, (K_{2i-1}, K_{2i})) \quad (5)$$

6) To decrypt the image, the reverse of CSCP is employed. (See Fig. 5.)

For i from 1 to n do
  If i equal to 1
    $P_i = NeuronNet(C_i, (K_{2i-1}, K_{2i}))$
  Else
    $C'_{i-1} = LFSR(C_{i-1})$
    $K'_{2i-1} = K_{2i-1} \oplus C'_{i-1}$
    $K'_{2i} = K_{2i} \oplus C'_{i-1}$
    $P_i = NeuronNet(C_i, (K'_{2i-1}, K'_{2i}))$
  End if
End for

Fig. 5. Decryption Pseudo Code

7) The one dimensional array of plain pixels $P = <P_1, P_2, \ldots\ldots, P_n>$ is generated. Finally, it is converted back into original 8-bit grayscale image. The decryption process is shown in Fig. 3.

III. Experimental Set Up and Result

Simulation was done in MATLAB to explore the efficiency of the proposed image encryption method. Grayscale images are used in the experiment because of high redundancy of adjacent pixels. As the initial value of logistic map, population $X_0 = 0.1$ and grow rate parameter $r = 3.99$ are chosen. In our experiments, we apply our method to the same images, Lenna and Peppers, that have been used in previous works [9][10]. Both, shown in Fig. 6, are grayscale images of size 256×256.

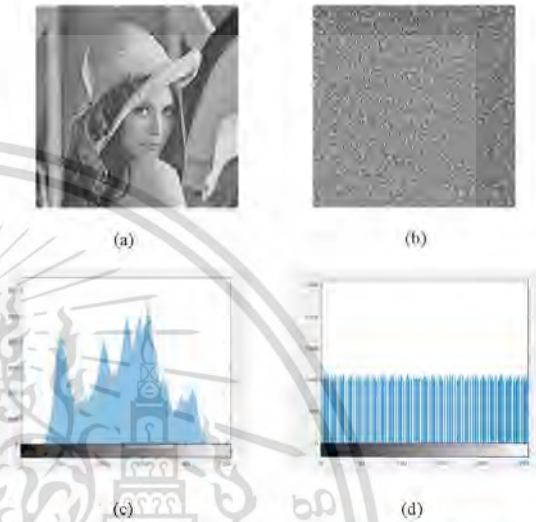
(a) (b)

Fig. 6. The images, Lenna and Peppers, that are used in the experiments.

A. Histogram Analysis

A histogram is used to present the frequency distribution of pixel intensities of the image. An ideal cipher image should have the flat or uniform distribution, which is difficult to analyze the relationship between plain and cipher images.

In Fig. 7(a) and Fig. 7(b), it is shown that the image after encryption show no information about the original image. More importantly, the histogram of the encrypted image in Fig. 7(d) is flat and does not resemble the the histrogram of the original image shown in Fig. 7(c).



(a) (b)

(c) (d)

Fig. 7. Fig. 7(a) and (b) illustrate the plain and cipher images. Histograms corresponding to Fig. 7(a) and (b) are shown in Fig. 7(c) and (d), respectively.

B. Entropy Analysis

Entropy, introduced by Shannon in 1949 [12], is the important concept to study the degree of randomness of the given information. In our work, we use entropy to measure unpredictability or the randomness of the image pixel intensities. In other words, how random the intensity values of the cipher image is. To calculate the entropy, we use the following formula:

$$H(m) = \sum_{i=0}^{L-1} p(m_i) \log_2 \frac{1}{p(m_i)} \quad (6)$$

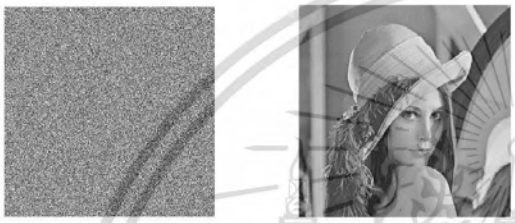
where L is the total number of the pixel intensity (normally L=256 for the 8-bit grayscale image), m_i denotes each of the pixel intensity values and $p(m_i)$ is the probability of m_i. According to the equation, the optimal value of the entropy is 8, which means that each pixel intensity has the same probability. Table 1 shows the comparison of the image entropy of the proposed scheme with other scheme in the literature. As shown in the table, entropies of cipher images of all approaches are almost 8.

Table 1 Comparison of the entropy value of proposed method with other methods

Entropy of Encrypted image	Proposed Method	[6]	[9]	[10]
Fig. 6(a)	7.997637	7.9072	7.997279	7.9976
Fig. 6(b)	7.996949	7.6514	7.997114	7.9972

C. Key Sensitivity and Key space analysis

As mentioned earlier, good cryptosystem should be sensitive to keys. This is to make sure that different two keys cannot be used produce similar cipher image or to decrypt the same cipher image. In our experiment, we change the value of X_0 by 0.0000000000000001, while using the same parameter r, to study the effect of infinitesimal difference of key values.



(a) Decrypted image with wrong key.

(b) Decrypted image with right key.

Fig. 8. Decrypted images with different and same key.

As shown in Fig. 8(a), decrypting image with the wrong key cannot be reversed back to the original image.

Another aspect of the strength of encryption algorithm is the size of the key space or the amount of all possible key values. The larger the key space, the more difficult to conduct the brute force attack. In logistic map, number of possible values of both X_0 and r are 10^{16} [14]. The key space of the algorithm is, therefore, $10^{16} \times 10^{16} = 10^{32}$.

D. Differential Attack Analysis

Strong cryptography algorithms should be sensitive to the plaintext attack or differential analysis attack where the algorithms produce two different cipher images from two plain images with a small difference. Let C_1 and C_2 be the cipher images which are corresponding to the original image P_1 and P_2 with only one-pixel difference, respectively. Number of Pixels Change Rate (NPCR) can be used to calculate the percentage of different pixel between C_1 and C_2 and the Unified Average Changing Intensity (UACI) can be used to measure the average differences of pixel intensity between C_1 and C_2 [11]. NPCR and UACI are defined as follows:

$$NPCR = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times 100\% \quad (7)$$

$$UACI = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\% \quad (8)$$

where M and N are the width and height of the image, respectively, $C_1(i,j)$ and $C_2(i,j)$ are the intensity values of the two cipher images at position (i,j) and $D(i,j)$ is the bipolar array which is defined as the following formula:

$$D(i,j) = \begin{cases} 0 & if\ C_1(i,j) \neq C_2(i,j) \\ 1 & if\ C_1(i,j) = C_2(i,j) \end{cases} \quad (9)$$

The results of NPCR and UCAI evaluations are shown in Table 2 and 3.

Table 2 Comparison of number of pixel change rate results with other methods

Image	Proposed Method	[6]	[9]	[10]
	NPCR	NPCR	NPCR	NPCR
Fig. 6(a)	100	0.00152587	99.61	99.62
Fig. 6(b)	100	0.00152587	N/A	99.63

Table 3 Comparison of UACI results with other methods

Image	Proposed Method	[6]	[9]	[10]
	UACI	UACI	UACI	UACI
Fig. 6(a)	33.53	0.00040091	33.46	33.54
Fig. 6(b)	33.59	0.00129250	N/A	33.43

E. Peak Signal-to-Noise Ratio

To measure the ratio of mean square difference between the original image the encrypted image, Peak Signal-to-Noise Ratio (PSNR) [13] is used. In this case, the original image and the cipher image are considered as the signal and noise, respectively. The formula is defined as below:

$$PSNR = 10log_{10}\left(\frac{255^2}{MSE}\right) \quad (10)$$

where MSE is the mean square error between two images and computed as follow.

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (P(i,j) - C(i,j))^2 \quad (11)$$

where M is the width of the image, N is the height of the image and $P(i,j)$ and $C(i,j)$ are the pixel intensity of the plain image and cipher image at location (i,j), respectively.

As the difference between two image pixel value in the same position is higher, the value of PSNR has become lower and approach to zero for the maximum of different pixel value between two grayscale images. Table 4 shows the comparison result of PSNR of the proposed method.

Table 4 Comparison of the Peak Signal-to-Noise Ratio result of proposed method with other method

Image	Proposed Method	[6]	[9]
	PSNR	PSNR	PSNR
Fig. 6(a)	9.226572	11.1648	9.215507
Fig. 6(b)	8.463215	9.2049	8.924724

IV. CONCLUSION

In this research work, a new image encryption method based on the Logistic map combined the perceptron model, called Cipher Stream Chaining Process (CSCP), is proposed. It is equipped with cipher-pixel chaining making it highly sensitive to input image. The experiment results show that the encrypted image is completely different from the original, both in terms of human vision and statistics. The pixel change rate and unified average changing intensity of the proposed method suggest that it is robust against the differential attack analysis. In the future, we will evaluate our approach on other images with different sizes. Potential implementations on color images and video files must also be investigated.

REFERENCES

[1] R. A Mollin. 2006. "An Introduction to Cryptography". Boca Raton, FL: CRC Press.

[2] J A. K. Mandal, C. Parakash and A. Tiwari, "Performance evaluation of cryptographic algorithms: DES and AES, " *2012 IEEE Students' Conference on Electrical, Electronics and Computer Science*, Bhopal, 2012, pp. 1-5.

[3] S. Lian, Multimedia Content Encryption: Techniques and Application, CRC, 2008.

[4] G. Srividya and P. Nandakumar, "A Triple-Key chaotic image encryption method," 2011 International Conference on Communications and Signal Processing, Calicut, 2011, pp. 266-270.

[5] S. Rohith, K. N. H. Bhat and A. N. Sharma, "Image encryption and decryption using chaotic key sequence generated by sequence of logistic map and sequence of states of Linear Feedback Shift Register," *2014 International Conference on Advances in Electronics Computers and Communications*, Bangalore, 2014, pp. 1-6.

[6] Xing-Yuan Wang, Lei Yang, Rong Liu. "A Chaotic image encryption algorithm based on perceptron model", Springer Science + Business Media B.V. 2010.

[7] Alvarez, G., Li, S.J.: "Some basic cryptographic requirement for chaos-based cryptosystem", Int. J. Bifurcation Chaos, 2006, 16, (8), pp. 412-417

[8] Z. Yan-Bin and D. Qun, "A New Digital Chaotic Sequence Generator Based on Logistic Map," *2011 Second International Conference on Innovations in Bio-inspired Computing and Applications*, Shenzhan, 2011, pp. 175-178.

[9] Hanchinamani,G.; Kulkarn,L. ; "An Efficient Image Encryption Scheme Based on a Peter De Jong Chaotic Map and a RC4 Stream Cipher", in 3D Res 6:30, DOI 10.1007/s13319-015-0062-7, 2015.

[10] M. Long and L. Tan, "A Chaos-Based Data Encryption Algorithm for Image/Video," *2010 Second International Conference on Multimedia and Information Technology*, Kaifeng, 2010, pp. 172-175.

[11] Y. W. Joseph, P. Noonan and S. Agaian, "NPCR and UACI Randomness Tests for Image Encryption", Department of electrical and Computer Engineering Tufts University Medford, MA, USA.

[12] C. Shannon, "Communication theory of secrecy sytem", Bell system Technical Journal 28:656-715, 1949.

[13] Taneja, N., Raman, B., & Gupta, I. "Combinational domain encryption for still visual data", Multimedia Tools and Application, (2012), 159(3), 775-793. doi:10.1007/s11042-011-0775-4.

[14] X. Wang, C. Jin, "Image encryption using game of life permutation and PWLCM chaotic system", Opt. Commun., 2012, 285, pp. 412-4.

[15] M. Budhraja, N. Kumar, and L. M. Saha. The 0-1 test applied to peter-de-jong map. *Int. J. Eng. Innov. Tech.*, 2(6):253-257, 2012.

[16] Wong, K.K., Carter, G., Dawson, E.(2010). An analysis of the RC4 family of stream ciphers against algebraic attacks. *Proceeding 8th Australasian information security conference, 103*, pp. 67-74.

ข้อมูลประวัติคณะผู้วิจัย

หัวหน้าโครงการวิจัย

ชื่อ - นามสกุล (ภาษาอังกฤษ) Asst. Prof. Dr. Isara Anantavrasilp

ตำแหน่งปัจจุบัน ผู้ช่วยศาสตราจารย์

หน่วยงานและสถานที่อยู่ที่ติดต่อได้สะดวก วิทยาลัยนานาชาติ สจล. โทร 081-659-8619

ประวัติการศึกษา

- Bachelor of Science (Information Technology), Sirindhorn International Institute of Technology, Thammasat University
- Master of Computer Science (Computational Logic), Technische Universität Dresden
- Doctor rer. nat.,Technische Universität München

สาขาวิชาการที่มีความชำนาญพิเศษ (แตกต่างจากวุฒิการศึกษา) ระบุสาขาวิชาการ

สาขาวิศวกรรมซอฟต์แวร์เทคโนโลยีสารสนเทศ

ประสบการณ์ที่เกี่ยวข้องกับการบริหารงานวิจัยทั้งภายในและภายนอกประเทศ

1. หัวหน้าโครงการวิจัย
- Nucleic Acid Sequences Model and Analysis Tool, 2015
- โครงการระบบกำหนดตำแหน่งภายใน อาคารบนอุปกรณ์เคลื่อนที่, 2012-2013
- UHF RFID Tags Localization using Machine Learning, 2010-2011

2. ผู้ร่วมวิจัย
- Reverse Vending Machine for Municipal Waste Management in Thailand, 2012-2013

ผลงานวิจัยที่ได้รับการตีพิมพ์

Tiyarattanachai, R., Kongsawatvoragul, I., and Anantavrasilp, I. (2015) Reverse Vending Machine and Its Impacts on Quantity and Quality of Recycled PET Bottles in Thailand. KMITL Science and Technology Journal, 15(1), pp. 24-33.

Tiyarattanachai, R., Han, T., and Anantavrasilp, I. Quality management of municipal solid waste at material recovery facilities. Proc. of the 2nd AUN/SEED-Net Regional Conference on Energy Engineering (RCEneE), Bangkok, Thailand, November 13-14, 2014, p. 31.

Willnecker, F., Anantavraslip, I., Brügge, B., "Machine Learning Assisted Position Detection of UHF RFID Tags", In European Conference on Smart Objects, Systems and Technologies, Munich, 2012.

Anantavrasilp, I., "Approximating IP Traffic Characteristics Using Partial Flows", In The 4th Regional Conference on Information and Communication Technology, Ho Chi Minh City, 2011.

Anantavrasilp, "Intelligent IP traffic / flow classification system", In Proceedings of the 8th International Network Conference, Heidelberg, 2010. (Selected Paper Award)

Anantavrasilp, "A unified framework for flow classification", In Proceedings of International Conference on Computer Design and Applications, Singapore, 2009.

Anantavrasilp and T. Schöler, "Automatic flow classification using machine learning", In Proceedings of the 15th International Conference on Software, Telecommunications and Computer Networks, Dubrovnik, 2007.

Anantavrasilp, I. and T. Schöler, "Providing quality-of-service support to legacy applications using machine learning", In Proceedings of IADIS International Conference on Telecommunications, Networks and Systems, Lisbon, 2007. (Outstanding Paper Award)

ผู้ร่วมวิจัย

ชื่อ - นามสกุล (ภาษาอังกฤษ) Asst. Prof. Dr. Ronnachai Tiyarattanachai
ตำแหน่งปัจจุบัน ผู้ช่วยศาสตราจารย์
หน่วยงานและสถานที่อยู่ที่ติดต่อได้สะดวก วิทยาลัยนานาชาติ สจล. โทร 081-659-8619 email Ronnachai.ti@kmitl.ac.th
ประวัติการศึกษา

- วศ.บ. (วิศวกรรมสิ่งแวดล้อม) จุฬาลงกรณ์มหาวิทยาลัย
- วท.ม. (การจัดการสิ่งแวดล้อม) จุฬาลงกรณ์มหาวิทยาลัย
- Ph.D. (Environmental Policy) New Jersey Institute of Technology

ประสบการณ์ที่เกี่ยวข้องกับการบริหารงานวิจัยทั้งภายในและภายนอกประเทศ

หัวหน้าโครงการวิจัย

1. Current Situation and Future of Site Remediation Work in Thailand: A survey with related government agencies, 2010-2011
2. Reverse Vending Machine for Municipal Waste Management in Thailand, 2012-2013
3. Green Campus: a concept of sustainability for higher educational institutions in Thailand – A comparative case study on Green- and Non-Green-Campus universities in Thailand, 2014-2015
4. Carbon Tax System for Vehicles Used in Logistic Activities in Thailand, 2016
5. Consumer Perception of Environmental Label of Construction Material Products in Bangkok, 2017
6. Environmental Performance and Business Competitiveness of DJSI-Indexed Refineries in AEC, 2017
7. Relationship between Sustainability and Stock Performance of Listed Companies in Thailand, 2018

ผู้ร่วมโครงการวิจัย

1. Smart Bicycle Fleet Management System for Green University

ผลงานวิจัยที่ได้รับการตีพิมพ์

วารสารทางวิชาการ

Tiyarattanachai, R. and Hollmann (2016) Green Campus initiative and its impacts on quality of life of stakeholders in Green and Non-Green Campus universities. SpringerPlus, 5(1), pp. 1-17.

Tiyarattanachai, R., Kongsawatvoragul, I., and Anantavrasilp, I. (2015) Reverse Vending Machine and Its Impacts on Quantity and Quality of Recycled PET Bottles in Thailand. KMITL Science and Technology Journal, 15(1), pp. 24-33.

Jackson, N. L., Smith, D. R., Tiyarattanachai, R. and Nordstrom, K. F. (2007). Use of a small beach nourishment project to enhance habitat suitability for horseshoe crabs. Geomorphology. (89), pp. 172-185.

Tiyarattanachai, R., Kanatharana, P., and Hsieh, H. (2004). Treatment of trichloroethylene contaminated wastewater using Fenton's reagent. Malaysian Journal of Science. (23), pp. 169-177.

การประชุมวิชาการ

Chhang, R. and Tiyarattanachai, R. The impact of greenhouse gas emissions on financial performance of Thai listed Companies for sustainable investment. *Proc. Of the 14th International Asian Urbanization Conference*, Bangkok, Thailand, January 11-13, 2018.

Mathias, M. G. and Tiyarattanachai, R. Analysis of stock market performance of Thai companies practicing sustainability management. *Proc. Of the 14th International Asian Urbanization Conference*, Bangkok, Thailand, January 11-13, 2018.

Lim, K. and Tiyarattanachai, R. Relationship between environmental performance and business performance of oil refinery in AEC+6 countries. *Book of Extended Abstract of the 10th Regional Conference on Environmental Engineering 2017*, Ha Noi, Vietnam, 30 October – 1 November, ISBN: 978-604-95-0308-5, p. 42-44.

Chhang, R. and Tiyarattanachai, R. Relationship between environmental performance and financial performance of Thai listed companies for sustainable investment. *Book of Extended Abstract of the 10th Regional Conference on Environmental Engineering 2017*, Ha Noi, Vietnam, 30 October – 1 November, 2017, ISBN: 978-604-95-0308-5, p. 36-38.

Vuthy, S., Tiyarattanachai, R., and Prabnasak, J. Carbon pricing system for vehicles used in freight transport. *Proc. Of the 7th Conference on Operations and Supply Chain Management,* Phuket, Thailand, December 18-21, 2016, p. 429-440.

Tiyarattanachai, R., Han, T., and Anantavrasilp, I. Quality management of municipal solid waste at material recovery facilities. Proc. of the 2nd AUN/SEED-Net Regional Conference on Energy Engineering (RCEneE), Bangkok, Thailand, November 13-14, 2014, p. 31.

Jirasit, N., Tiyarattanachai, R., and Hollmann, N. Comparison of quality of life among stakeholders in green and non-green campus universities. Proc. of the 2nd AUN/SEED-Net

Regional Conference on Energy Engineering (RCEneE), Bangkok, Thailand, November 13-14, 2014, p. 30.

Bhu-anantanondh, T., Tiyarattanachai, R., and Hollmann, N. Environmental performance benchmarking of refineries in ASEAN Economic Community. Proc. of the 6th ASEAN Environmental Engineering Conference (AEEC), Bangkok, Thailand, November 21-22, 2013, p. E-8.

Tiyarattanachai, R. and Watts, D. J. (2011). Institutional controls in the views of state regulators and licensed site professionals. Proc. of the 4th ASEAN Environmental Engineering Conference, Yogyakarta, Indonesia, November 22-23, 2011.

Tiyarattanachai, R. and Watts, D. J. (2011). Institutional controls and brownfield redevelopment. Proc. of the 3rd AUN/SEED-Net Regional Conference on Global Environment, Kuala Lumpur, Malaysia, February 21-22, 2011, p.22.

Tiyarattanachai, R. and Watts, D. J. (2011). Institutional controls and sustainable remediation. Proc. of the 10th EEAT National Environmental Conference, March 23-25, 2011, pp. 151-152.

Tiyarattanachai, R., Kanatharana, P., and Hsieh, H. (2003). Treatment of trichloroethylene contaminated wastewater using Fenton's reagent. Proc. of International Conf. on Environmental Management and Technology, Malaysian University Consortium for Environment and Development – Industry and Urban Areas (MUCED – I&UA), Putrajaya, Malaysia, August 4-6, 2003, p. 20.