AN ALGORITHM FOR AUTHENTICATION USING COLOR MECHANISM

SOUNG YONG CAI

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGESAHAN STATUS TESIS

JUDUL: AN ALGORITHM FOR AUTHENTICATION USING COLOR MECHANISM

SESI PENGAJIAN: 2017

Saya SOUNG YONG CAI

mengaku membenarkan tesis (PSM/Sarjana/Doktor Falsafah) ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. ** Sila tandakan (/)

_____ SULIT (Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

_____ TERHAD (Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)

_____ TIDAK TERHAD

_____ _____

(TANDATANGAN PENULIS) (TANDATANGAN PENYELIA)

Alamat tetap: NO 25,
LORONG BUKIT CINA
75100, MELAKA.

DR SITI RAHAYU BINTI SELAMAT

NAMA PENYELIA

Tarikh: _____ Tarikh: _____

CATATAN: * Tesis dimaksudkan sebagai Laporan Akhir Projek Sarjana Muda (PSM)
** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

AN ALGORITHM FOR AUTHENTICATION USING COLOR MECHANISM

SOUNG YONG CAI

This report is submitted in partial fulfilment of the requirements for the Bachelor of Computer Science (Computer Security)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2017

DECLARATION

I hereby declare that this project report entitled

AN ALGORITHM FOR AUTHENTICATION USING COLOR MECHANISM

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT : _____ Date : _____

(SOUNG YONG CAI)

I hereby declare that I have read this project report and found this project report is sufficient in term of the scope and quality for the award of Bachelor of Computer Science (Computer Security) With Honours.

SUPERVISOR: _____ Date : _____

(DR SITI RAHAYU BINTI SELAMAT)

DEDICATION

Special thanks to my family who supported in me from the beginning of the project until the completion of the project. I would like to dedicate this project to my supervisor, Dr. Siti Rahayu Binti Selamat who has gave me guidance along the progress until the end of this project. Furthermore, I also would like to thank all my friends who are willing to lend their hands to assist me especially when I face problems or issues in this project.

ACKNOWLEDGEMENTS

I would like to express my highest gratitude to my supervisor in this project, Dr. Siti Rahayu Binti Selamat for giving assistant and guidance along this project to complete this project successfully. She also providing me with materials such as reference books, article and links that related to my project which able to use it as references for my project. She always help me to check my documentation in this project and inform me to do correction on mistake in order to produce a high quality documentation.

I also would like to express my sincere appreciation to other lecturers who are willing to spend their time to guide me and giving me opinion for this project. They provided me valuable information and opinion which help me to complete this project on time with better results.

ABSTRACT

Authentication is widely used nowadays due to greatly expansion of the technology in order to verify a person identity and the most common used is textual authentication. Textual authentication has a lot vulnerabilities that caused the password easily been stolen by using visual hacking, sniffed by capturing the keyboard input using keylogger and easily being brute force attack using specified tools. In order to solve these issues, two main objectives are derived in this project which are to analyse authentication mechanism and to create an color mechanism authentication algorithm. Therefore, the aim of this project is to construct a new authentication algorithm using color mechanism in order to solve the issues occurred in textual authentication. This authentication will increase the complexity of the password compared to textual password which require users to memorize their color selection to provide as maximum security. The color mechanism authentication algorithm consists of three processes which are Color Selection, Hexadecimal Password Encryption and Password Verification. Waterfall model was chosen as the methodology of this project and used throughout the entire project which consists of several phase such as analysis, requirement specification, design, implementation, testing and maintenance which able ensure smooth progression along the project. This project will contributes on a new authentication mechanism that called as Color Authentication Mechanism that able to solve the weaknesses of textual authentication and harden the level of security in authentication layer. This new algorithm also may able to fully replace textual authentication in the future.

ABSTRAK

Pada masa kini, pengesahan digunakan secara meluas disebabkan oleh pengembangan teknologi yang besar dan pantas bagi membantu dalam proses mengesahkan identiti seseorang individu dan yang paling umum digunakan adalah pengesahan teks. Pengesahan tekstual amat terdedah kepada pelbagai jenis serangan seperti penyaduran, penggodaman visual, kejuruteraan sosial, serangan kamus, serangan kekerasan dan lain-lain. Pengesahan mengunakan teks yang digunakan secara meluas oleh pengguna mempunyai banyak kelemahan yang menyebabkan kata laluan mudah dicuri dengan menggunakan penggodam visual, menangkap input papan kekunci menggunakan keylogger dan mudah menjadi serangan kekerasan menggunakan alat yang tertentu. Bagi menyelesaikan isu-isu ini, dua objektif utama diperolehi dalam projek ini iaitu untuk menganalisis mekanisme pengesahan dan untuk mewujudkan algoritma pengesahan mekanisme warna. Oleh itu, matlamat projek ini adalah untuk membina atau mencipta algoritma pengesahan baru menggunakan mekanisme warna untuk menyelesaikan isu-isu yang berlaku dalam pengesahan mengunakan teks. Pengesahan ini akan meningkatkan kerumitan kata laluan berbanding dengan kata laluan mengunakan teks yang memerlukan pengguna untuk menghafal pemilihan warna mereka untuk memberikan keselamatan maksimum yang semungkin ada. Algoritma pengesahan mekanisme warna terdiri daripada tiga proses iaitu Pemilihan Warna, Penyulitkan Kata Laluan Heksadesimal dan Pengesahan Kata Laluan. Model waterfall telah dipilih dan digunakan sepanjang keseluruhan projek yang terdiri daripada beberapa fasa seperti analisis, spesifikasi keperluan, reka bentuk, pelaksanaan, pengujian dan penyelenggaraan yang dapat memastikan kemajuan yang lancar sepanjang projek. Projek ini akan menyumbang kepada mekanisme pengesahan baru yang menggunakan mekanisme warna yang dapat menyelesaikan banyak kelemahan pengesahan mengunakan teks dan menguatkan tahap keselamatan dalam lapisan pengesahan. Algoritma pengesahan ini mempunyai potensi menggantikan sepenuhnya pengesahan megunakan teks pada masa akan datang.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

CHAPTER I

INTRODUCTION

1.1 Introduction

Authentication is used to verify the identity of a person in order to allow them or reject them to access to the specific categories of information. However, each method has their problem or issues present such as an attacker may guess forge or steal a password or token. This issues caused many major problem such as information leakage, financial loss, and modification of data. Hence, this issues should be get attention by public to prevent further loss.

An algorithm for authentication approach using color mechanism is the new method of authentication that able to replace current textual authentication which is vulnerable to many types of attacks such as eavesdropping, visual hacking, social enginnering, dictionary attack, brute force attack and others. This authentication will use its own algorithm to store the data and validate the data when user login. This authentication will increase the complexity of the password compare to textual password which require users to memorize their chosen password in order provide as maximum security as possible.

1.2 Problem statement

Table 1.1: Summary of Problem Statement

PS	Problem Statement
PS_1	Password authentication nowadays has a lot vulnerability caused the password easily been stolen by using visual hacking and sniffed by capturing the keyboard input using keylogger and easily being brute force attack using specified tools.

1.3 Project Question

Based on the problem statements, one project question (PQ) are constructed as shown in Table 1.2.

Table 1.2: Summary of Project Question

PS	PQ	Project Question
PS_1	PQ_1	How can we improve the problem in authentication?

1.4 Project Objective

In order to solve the problem identified as in section 1.2, two project objectives (PO) are derived as shown in Table 1.3.

Table 1.3: Summary of Project Objective

PS	PQ	PO	Project Objective
PS_1	PQ_1	PO_1	To analyse authentication mechanism.
		PO_2	To create an color mechanism authentication algorithm.

1.5 Project Scope

The scope for this project are:

1. The algorithm will be implement on system logon.
2. Encryption on hexadecimal of color as password.

1.6 Project Contribution

This project is expected to create a new authentication method which will replace the current modern plaintext authentication which has some vulnerabilities.

Table 1.4: Summary of Project Contribution

PS	PQ	PO	PC	Project Contribution
PS_1	PQ_1	PO_1	PC_1	Proposed a new authentication mechanism
		PO_2	PC_2	Proposed an algorithm for encryption of color information.

1.7 Thesis Organization

This report consists of seven chapters namely Chapter I: Introduction, Chapter II: Literature Review, Chapter III: Project Methodology, Chapter IV: Analysis And Design, Chapter V: Implementation, Chapter VI: Testing and Chapter VIIL Project Conclusion. The brief explanation of these chapters are as follow:

Chapter I: Introduction

This chapter explained about the introduction, problem statement, objective, project contribution and expected output of this project which is related to authentication method.

Chapter II: Literature review

This chapter explained about the authentication, color, modern authentication method characteristic and vulnerabilities in modern authentication. It will help to more understanding in order to create a new authentication method. Analysis on the current or existing methods and techniques are also provided in order to identify and justify the selected methods and technique that will be used in this project.

Chapter III: Project Methodology

This chapter explained how the project is carried out. All the main process to complete the project are discussed in this chapter and a milestone with Gantt chart are provided in order to ensure smooth progression and completion on time of this project.

Chapter IV: Analysis and Design

The design of color mechanism authentication algorithm which consists of several processes is describe in this chapter. All the software requirement and hardware requirement that needed in this project also will be listed in this chapter. The feature of the color mechanism authentication algorithm and design of the encryption of the color hexadecimal password with it security strength will be explained in this chapter before conducting implementation in this project.

Chapter V: Implementation

This chapter will perform implementation on coding and development of color mechanism authentication algorithm. This chapter will illustrate the color mechanism authentication architecture and discuss the structure of the color mechanism authentication algorithm by using figure and pseudocode. Details of the encryption algorithm used by color mechanism authentication algorithm also will be explained in this chapter.

Chapter VI: Testing

This chapter will elaborate the testing conducted on the color mechanism authentication algorithm. Several testing methods on the color mechanism authentication algorithm to measure the usability of the proposed authentication method and the compatibility on different browsers. This chapter is important in order to ensure the outcome of this project is reliable and suitable to be use by users before distribute it to public.

Chapter VII: Project Conclusion

This chapter compile the entire chapter in a final documentation which include discussion on project summarization, project contribution, project limitation and future work. Suggestion of improving this project also will be discussing in this chapter based on the responses of the responders through testing.

1.8 Summary

Password authentication widely used nowadays which has plenty of vulnerabilities should be concerned and find another alternative method to replace this kind authentication method. There are several of authentication attack can be launch on different types of authentication. Hence, it is imperative that an explanatory study of authentication and cryptography should be conducted. All the topic discussed and stated in this chapter which are problem statement, project question, project objective, project scope and project contribution are important to use as a reference or aim for this project throughout the whole progress of this project. In the next chapter, it will explain the details about the authentication and the cryptography that will used in this project.

CHAPTER II

LITERATURE REVIEW

2.1 Introduction

In this chapter, some research about the related topics as shown in Figure 2.1 will be conducted and explained in this chapter. The literature is based on the several resources such as journal articles, proceeding, technical reports and white papers.

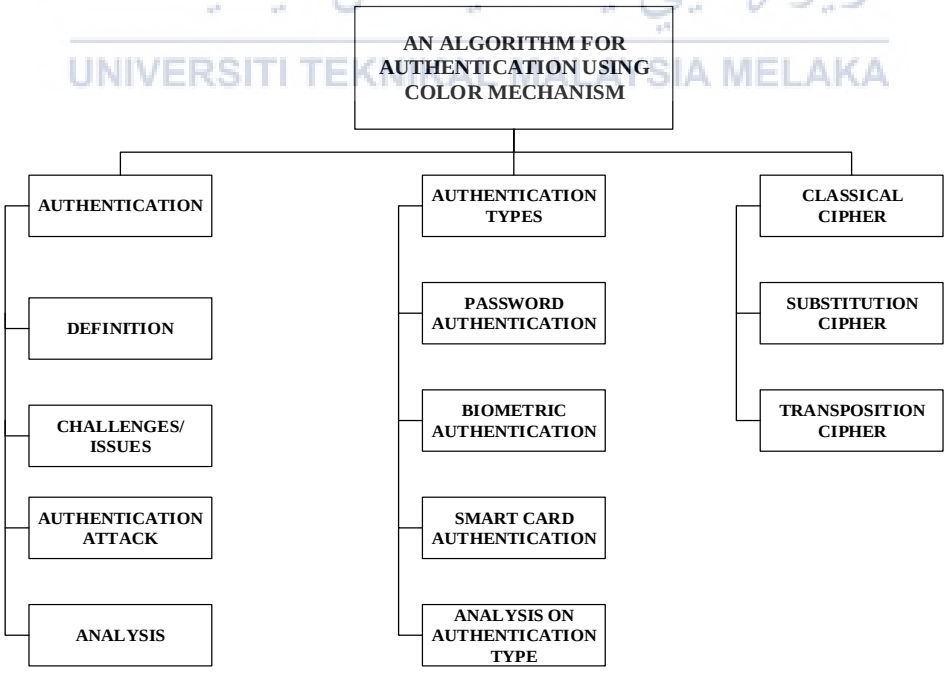

Figure 2.1: Framework of literature review

Figure 2.1 shows the topics that will elaborate and analyse in this chapter. There are three main topics will be discussed which are authentication, authentication types and encryption/cryptography technique.

2.2 Authentication

In this section, the definition, challenges or issues, technique, methods, cryptography technique are elaborated and analyse.

2.2.1 Definition of authentication

The term of authentication covers a wide area which has plenty of explaination on the word authentication. There are several definitions by different authors and sources on the meaning of authentication as shown in Table 2.1.

Table 2.1: Definition of Authentication

No	Author/Sources	Definition
1	Farlex, 2012.	Verification and confirmation of a user's identity to get the access right.
2	Margaret Rouse, 2014.	Verification by using active human-to-machine transfer of credentials and machine authentication which are required for confirmation of a user's authenticity and automated processes that doesn't needed any user input respectively.
3	Dawn M. Turner, 2016	An electronic process that perform identity confirmation on a legal person and confirming the data in electronic form of it origin and integrity.
4	Paul A. Grassi,2017	Authentication is a process of determining the validity of 1 or more credentials in order to claim a digital identity.
5	Spencer, Will 2013	A process of an entity identify itself before network logon is granted.

Table 2.1 shows several definition of authentication by different authors or sources. Based on the definitions, it can be summarized that the authentication is used to verify the identity of a person in order to allow them or reject them to access to the specific categories of information. There are four general means to authenticate a user's identity by using single or combination of several means which are a) what a user knows, b) what a user has, c) what a user is (static biometrics) and d) what a user does (dynamic biometrics) as summarized in Table 2.2.

Table 2.2: General means of authentication (Computer Security Principles and Practice, 2012)

No	Means	Example
1	what a user knows	– Password – Personal identification number (PIN)
2	what a user has	– Smartcard – Physical keys
3	what a user is (static biometrics)	– Fingerprint – Retina – Face
4	What a user does (dynamic biometrics)	– Voice Pattern – Handwriting – Typing rhythm

All the methods shown in Table 2.2 able to provide secure user authentication if implemented properly. However, there are several challenges/issues on the authentication that reflect to protect the data transmission.

2.2.2 Challenges/Issues on authentication

Nowadays, protecting data transmissions as well as safeguarding data files attracts disproportionate attention. The major threats originate from perpetrators masquerading as persons who already have the necessary access privileges. However, each method has their problem or issues present such as an attacker may guess forge or steal a password or token. User also may forgotten their password or lose their token.

False positive and false negatives, cost, convenience also present on biometric authenticator. As the technology advancing day by days, the authentication in correct protocol doesn't longer applied to the group of people which are called as hacker. Those group of people will find the vulnerability on the system and perform the attack in order to gain access to the system through various of illegal ways. This causes the authentication attack become the main challenge in protecting the data transmission.

2.2.3 Authentication Attack

As the technology advancing, the study and research on how to perform attack on authentication is getting common and popular nowadays. However this also causes some negative effect in which the attacker may using these knowledge and tools that can easily obtain through online to launch authentication attack on a victim. There are various of authentication attacks that are common in nowadays as shown in Table 2.3.

Table 2.3: Example of authentication attack

Attack types	**Attack description**
Brute Force	An attacker may using brute force tools which is automated looping to repeating input the different combination of password in authentication layer. Attacker also may guess the person password by collecting the victim data such as birthday, identity card number, and others.
Spoofed logon screens	Attacker may create a fake logon screen which will lure a user login and the logon screen will send the username and password to the attacker.
Social Engineering	Attacker can performing social engineering on a victim by collecting the information of the victim through questioning the victim directly, public information of victim on social media and others in order to perform authentication attack.
Key Logger	An attacker may use a hidden program to track all the user keystroke that input through their keyboard. Attacker will find various method to install their malware into victim computer.