UNIVERSITI SAINS MALAYSIA

LAPORAN AKHIR PROJEK PENYELIDIKAN JANGKA *PENDEK*

FINAL REPORT OF SHORT TERM RESEARCH PROJECT

Sila kemukakan laporan akhir ini melalui Jawatankuasa Penyelidikan di Pusat Pengajian dan Dekan/Pengarah/Ketua Jabatan kepada Pejabat Pelantar Penyelidikan

1. **Nama Ketua Penyelidik:** Azman bin Samsudin
Name of Research Leader

☑ Profesor Madya/ *Assoc. Prof.* ☐ Dr./ *Dr.* ☐ Encik/Puan/Cik/ *Mr/Mrs*

2. **Pusat Tanggungjawab (PTJ):** School of Computer Sciences
School/Department

3. **Nama Penyelidik Bersama: -**
Name of Co-Researcher

4. **Tajuk Projek:** *Visual Public-Key Cryptosystems*
Title of Project

5. **Ringkasan Penilaian/*Summary of Assessment***	Tidak Mencukupi *Inadequate*		Boleh Diterima *Acceptable*	Sangat Baik *Very Good*	
	1	2	3	4	5
i) **Pencapaian objektif projek:** *Achievement of project objectives*	☐	☐	☐	☑	☐
ii) **Kualiti output:** *Quality of outputs*	☐	☐	☐	☑	☐
iii) **Kualiti impak:** *Quality of impacts*	☐	☐	☐	☑	☐
iv) **Pemindahan teknologi/potensi pengkomersialan:** *Technology transfer/commercialization potential*	☐	☐	☑	☐	☐
v) **Kualiti dan usahasama :** *Quality and intensity of collaboration*	☐	☐	☑	☐	☐
vi) **Penilaian kepentingan secara keseluruhan:** *Overall assessment of benefits*	☐	☐	☑	☐	☐

6. **Abstrak Penyelidikan**
(Perlu disediakan di antara 100 - 200 perkataan di dalam **Bahasa Malaysia dan juga Bahasa Inggeris**. Abstrak ini akan dimuatkan dalam Laporan Tahunan Bahagian Penyelidikan & Inovasi sebagai satu cara untuk menyampaikan dapatan projek tuan/puan kepada pihak Universiti & masyarakat luar).

Abstract of Research
(An abstract of between 100 and 200 words must be prepared in Bahasa Malaysia and in English). This abstract will be included in the Annual Report of the Research and Innovation Section at a later date as a means of presenting the project findings of the researcher/s to the University and the community at large)

Many public-key cryptosystems are being used in our daily lives to attain privacy, authenticity, integrity and non-repudiation. However, most of the existing public-key algorithms are based on complex mathematical computations. Until recently, building a highly secured public-key cryptosystem without utilizing complex computations has been a serious challenge, making it necessary for investigations to develop new cryptography methods. Visual cryptography is special because the scheme requires visual inspection or the equivalence of simple Boolean computation and therefore, does not require complex computations. The basic design of visual cryptography exploits the human visual system, to recover secret images. Moreover, the visual inspection process could be carried out very easily by humans, but hard for the computer to imitate. Indirectly, such scheme adds extra protection to the visual scheme against brute-force search on the visual secret key. However, visual cryptography currently exists only for secret-key cryptography. Therefore, in the current study, alternative public-key primitives are proposed, based on non-expansion visual cryptography and Boolean operations. The proposed visual cryptosystem include: visual key exchange protocol, visual digital signature protocol and visual zero-knowledge proof of identity protocols. The security of the proposed visual public-key protocols is assured by the K-SAT NP-hard problem and non-solvability of the non-invertible matrix problem. Security analyses showed that the proposed visual public-key cryptosystem is secure, especially when used with large sizes of shadow images (visual shares). The time required to brute-force the secret values (visual secret keys) increased exponentially with the increase in the size of shadow images. The wide potential use, specific niche on visual applications, simplicity and ease of implementation of shadow images, therefore makes the proposed visual public-key cryptosystem a suitable alternative to the classical public-key cryptosystems that are currently in use today.

Banyak system kripto kunci-awam digunakan dalam kehidupan sehanian kita untuk mencapai privasi, kesahihan, integriti dan bukan-penolakan. Walau bagaimanapun, kebanyakan algoritma kunci-awam yang sedia ada adalah berdasarkan kepada pengiraan matematik yang kompleks. Sehingga kini, membina sistem kripto kunci-awam dengan keselamatan yang tinggi tanpa menggunakan pengiraan kompleks telah menjadi satu cabaran, oleh itu kajian untuk membangunkan kaedah kriptografi baru adalah diperlukan. Kriptografi visual adalah satu kaedah kriptografi istimewa kerana skim ini memerlukan pemeriksaan visual yang mana pengiraannya adalah setara dengan pengiraan Boolean mudah dan oleh itu, tidak memerlukan pengiraan kompleks. Reka bentuk asas kriptografi visual mengeksploitasi sistem visual manusia untuk memulihkan imej rahsia. Selain itu, proses pemeriksaan visual boleh dijalankan dengan mudah oleh manusia tetapi sukar untuk komputer untuk meniru. Secara tidak langsung, skim seperti ini memberi perlindungan tambahan kepada serangan carian-kasar terhadap kekunci rahsia visual. Bagaimanapun, kriptografi visual kini wujud hanya untuk kriptografi kekunci simetrik. Oleh itu, dalam kajian ini, primitif kunci-awam alternatif adalah dicadangkan, berdasarkan kriptografi bukan-pengembangan visual dan operasi Boolean. Sistem kripto visual yang dicadangkan adalah: protokol pertukaran kunci visual, protokol tandatangan digital visual dan protokol pengetahuan-sifar pembuktian identiti visual. Keselamatan protokol visual kunci-awam yang dicadangkan adalah terjamin kerana pengunaaan permasalahan *NP-hard* K-SAT dan masalah matriks bukan tersongsangkan. Analisis keselamatan menunjukkan bahawa cadangan sistem kripto kunci-awam visual adalah selamat, terutamanya apabila digunakan dengan saiz imej bayang-bayang (*visual shares*) yang besar. Masa yang diperlukan untuk membuat carian-kasar terhadap kekunci rahsia (kunci rahsia visual) meningkat secara eksponen dengan peningkatan saiz imej bayang-bayang. Potensi penggunaan yang meluas, pengkhususan pada aplikasi visual, kesederhanaan dan kemudahan pelaksanaan imej bayang-bayang, membuat sistem kripto kunci-awam visual yang dicadangkan sesuai untuk dijadikan alternatif kepada sistem kripto kunci-awam klasik yang sedia-ada pada hari ini.

7. Sila sediakan laporan teknikal lengkap yang menerangkan keseluruhan projek ini.
[Sila gunakan kertas berasingan]
Applicant are required to prepare a Comprehensive Technical Report explaning the project.
(This report must be appended separately)

Please see attachment.

Senaraikan kata kunci yang mencerminkan penyelidikan anda:
List the key words that reflects your research:

Bahasa Malaysia	*Bahasa Inggeris*
Kriptografi visual	*Visual cryptography*
Kriptografi kunci-awam	*Public-key cryptography*
Operasi Boolean	*Boolean Operation*

8. Output dan Faedah Projek
Output and Benefits of Project

(a) * Penerbitan Jurnal
Publication of Journals
(Sila nyatakan jenis, tajuk, pengarang/editor, tahun terbitan dan di mana telah diterbit/diserahkan)
(State type, title, author/editor, publication year and where it has been published/submitted)

1. Abdullah M. Jaafar and Azman Samsudin, "A New Public-Key Encryption Scheme Based on Non-Expansion Visual Cryptography and Boolean Operation," *International Journal of Computer Science Issues*, vol. 7, issue 4, no. 2, July 2010.

2. Abdullah M. Jaafar and Azman Samsudin, "Visual Digital Signature Scheme: A New Approach," *IAENG International Journal of Computer Science*, vol. 37, issue 4, Nov. 2010. (http://www.iaeng.org/IJCS/issues_v37/issue_4/index.html). (Scopus)

3. A. Jaafar and A. Samsudin, "Visual Zero-Knowledge Proof of Identity Scheme: A New Approach," *International Conference on Computer Research and Development (ICCRD)*, pp. 205 - 212, May 2010, Malaysia. doi: 10.1109/ICCRD.2010.38. (Scopus)

Accepted for publication

4. Abdullah M. Jaafar and Azman Samsudin, "A Survey of Black-and-White Visual Cryptography Models," *International Journal of Digital Content Technology and its Applications*, Issue xx, vol. xx, 2012. (Scopus)

5. Abdullah M. Jaafar and Azman Samsudin, "An Improved Version of the Visual Digital Signature Scheme," *International Arab Journal of Information Technology*, Issue xx, vol. xx, 2013. (ISI IF 0.065)

(b) **Faedah-faedah lain seperti perkembangan produk, pengkomersialan produk/pendaftaran paten atau impak kepada dasar dan masyarakat.**
State other benefits such as product development, product commercialisation/patent registration or impact on source and society

Impact: We believe this work is the first in visual public-key.

* Sila berikan salinan/*Kindly provide copies*

(c) **Latihan Sumber Manusia**
Training in Human Resources

i) Pelajar Sarjana:
Graduates Students
(Perincikan nama, ijazah dan status)
(Provide names, degrees and status)

Abdullah M. Jaafar, PhD, graduated in Sep. 2011.

ii) Lain-lain: -
Others

9. Peralatan yang Telah Dibeli:
Equipment that has been purchased

-

Komen Jawatankuasa Penyelidikan Pusat Pengajian/Pusat
Comments by the Research Committees of Schools/Centres

A pioneering work in visual public work. with good output.

FINAL REPORT ON SHORT-TERM RESEARCH PROJECT

VISUAL PUBLIC-KEY CRYPTOSYSTEMS

(Project No.: 304/Pkomp/6310017)

SUBMITTED BY

ASSOC. PROF. DR. AZMAN SAMSUDIN

SCHOOL OF COMPUTER SCIENCES
UNIVERSITI SAINS MALAYSIA

TABLE OF CONTENTS

Objectives

The primary objectives of our research are:

- To introduce alternative methods to the classical public-key primitives based on non-expansion visual cryptography concept and Boolean operations with a comparatively low and simple computation.
- To assess the security of the proposed visual public-key cryptosystem which is based on the strength and the performance of the proposed visual public-keys algorithms.

Abstract

Many public-key cryptosystems are being used in our daily lives to attain privacy, authenticity, integrity and non-repudiation. However, most of the existing public-key algorithms are based on complex mathematical computations. Until recently, building a highly secured public-key cryptosystem without utilizing complex computations has been a serious challenge, making it necessary for investigations to develop new cryptography methods. Visual cryptography is special because the scheme requires visual inspection or the equivalence of simple Boolean computation and therefore, does not require complex computations. The basic design of visual cryptography exploits the human visual system, to recover secret images. Moreover, the visual inspection process could be carried out very easily by humans, but hard for the computer to imitate. Indirectly, such scheme adds extra protection to the visual scheme against brute-force search on the visual secret key. However, visual cryptography currently exists only for secret-key cryptography. Therefore, in the current study, alternative public-key primitives are proposed, based on non-expansion visual cryptography and Boolean operations. The proposed visual cryptosystem include: visual key exchange protocol, visual digital signature protocol and visual zero-knowledge proof of identity protocol. The security of the proposed visual public-key protocols is assured by the *K-SAT NP*-hard problem and non-solvable of the non-invertible matrix problem. Security analyses showed that the proposed visual public-key cryptosystem is secure, especially when used with large sizes of shadow images (visual shares). The time required to brute-force the secret values (visual secret keys) increased exponentially with the increase in the size of shadow images. The wide potential use, specific niche on visual applications, simplicity and ease of implementation of shadow images, therefore makes the proposed visual public-key cryptosystem a suitable alternative to the classical public-key cryptosystems that are currently in use today.

1. Introduction

Cryptography is one of the trusted practical methods for performing information security. The main purpose of cryptography is to provide confidentiality by converting the sensitive private information (known as plaintext) into unreadable and useless form (known as ciphertext). Figure 1 shows different