A ROBUST COVER GENERATION TECHNIQUE FOR STEGANOGRAPHY USING 2D IMAGES

By
MD. NABIL BIN HJ. AHMAD ZAWAWI

Thesis Submitted to the School of Graduate Studies,
Universiti Putra Malaysia,
In Fulfilment of the Requirement for the Degree of Master of Science

September 2006

This thesis is dedicated to the Steganographers of the
past, present and future…
To my wife, family, friends, supervisors and
superiors…
Thank you for your support.

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Science

A ROBUST COVER GENERATION TECHNIQUE FOR STEGANOGRAPHY USING 2D IMAGES

By

MD. NABIL HJ. AHMAD ZAWAWI

September 2006

Chairman : Associate Professor Ramlan bin Mahmod, PhD

Faculty : Computer Science and Information Technology

Steganography is still in its infancy as in comparison to cryptography in terms of research and development. The word steganography comes from the Greek roots *Steganos Graphos*, that literary means 'covered writing'. While cryptography aims to obstruct information access to unintended third party, the aim of steganography is to deny the very existence of it. Users of steganography do not advertise the existence of information in fact, denies its existence in the first place. Cryptography can be used prior to using steganography for an added layer of data security.

The general model for steganography consists of three main components, that is the embedded data (the message one wishes to secretly send), the CoverObject (the media being used to hide the data) and the StegoObject (the product of using *coverobject* to hide the *embedded data*). Simmons (1984) introduces the Prisoners' Problem as a classic scenario for covert communication. The problem describes a scenario where two prisoners named Alice and Bob that are put in two different cells and needed to communicate an escape plan with each other.

All communications need to go through the warden, Willy and as long as Willy does not suspect anything, the communication can be put through. Many steganographic techniques mainly focus on the information payload and undetectability of the system. In this research, we approach the steganographic problem of a passive warden and also with great considerations the threats of an active attack by an active warden in which the robustness of the stegoobject is concerned. We see this third criteria as equally important as the first and second because an active attack does not require the attacker to know whether an object is a stegoobject or not. An active attack simply change or modify a particular object's characteristic in its path with conditions that the object is still viewable and acceptable for general view. Applying the cover generation technique, the proposed steganographic technique can evade detection, able to carry useful amount of information and also at the same time survives an active attack that can jeopardise the information it carries.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia
sebagai memenuhi keperluan untuk ijazah Master Sains

TEKNIK PENJANAAN SAMARAN TEGAR BAGI STEGANOGRAFI MENGGUNAKAN IMEJ 2D

Oleh

MD. NABIL HJ. AHMAD ZAWAWI

September 2006

Pengerusi : Profesor Madya Ramlan bin Mahmod, PhD

Fakulti : Sains Komputer dan Teknologi Maklumat

Berbanding dengan kriptografi, steganografi merupakan bidang yang masih baharu dari segi penyelidikan dan pembangunan. Perkataan steganografi berasal daripada kata akar Greek, *Steganos Graphos*, yang secara ilmiahnya bermaksud 'penulisan samaran'. Berbanding kriptografi yang bertujuan untuk menghalang capaian maklumat kepada pihak yang tidak sepatutnya, tujuan steganografi adalah untuk menidakkan sepenuhnya kewujudan maklumat tersebut. Pengguna steganografi tidak memberitahu langsung tentang kewujudan maklumat bahkan, menafikan kewujudannya dari awal lagi. Kriptografi boleh digunakan sebelum menggunakan steganografi untuk menambahkan satu lagi lapisan keselamatan data.

Model umum steganografi terdiri daripada tiga komponen utama, iaitu data terbenam (mesej yang ingin dihantar secara rahsia), objeksamaran (media yang digunakan untuk menyembunyikan data) dan juga objekstego (objek yang terhasil daripada penggunaan objeksamaran untuk menyembunyikan data terbenam). Simmons (1984) memperkenalkan permasalahan tahanan sebagai sebuah senario klasik untuk komunikasi rahsia. Permasalahan tersebut

menerangkan sebuah senario di mana dua orang tahanan bernama Alice dan Bob yang telah diletakkan di dalam dua sel tahanan berasingan dan mereka perlu berkomunikasi untuk berbincang tentang rancangan untuk melarikan diri. Semua komunikasi perlu dibuat melalui seorang warden bernama Willy dan selagi Willy tidak mengesyaki apa-apa, komunikasi tersebut akan berjalan lancar.

Kebanyakan teknik steganografi hanya memfokuskan kepada kadar muatan maklumat dan keupayaan sistem tersebut mengelak daripada pengesanan. Dalam penyelidikan ini, kami mendekati permasalahan steganografi dari segi seorang warden yang pasif dan juga dengan pertimbangan yang mendalam terhadap ancaman serangan aktif daripada warden yang aktif di mana ketahanan objekstego diambil kira. Kami melihat kriteria ketiga ini sebagai sama penting dengan ciri pertama dan kedua kerana serangan aktif tidak memerlukan penyerang untuk mengetahui sama ada sesuatu objek itu adalah sebuah objekstego ataupun tidak. Sebuah serangan aktif hanya perlu menukar atau mengubah suai ciri sesebuah objek dalam laluannya dengan syarat objek tersebut masih boleh dilihat dan diterima untuk tatapan umum. Dengan mengaplikasikan teknik penjanaan samaran, teknik steganografi yang dicadangkan mampu mengelak daripada pengesanan, mampu membawa sejumlah maklumat yang berguna dan dalam masa yang sama dapat mengatasi serangan aktif yang boleh mengancam maklumat yang dibawanya.

ACKNOWLEDGEMENTS

Many thanks go firstly, as they should always be, to Allah, who blessed me with the ability to undertake and finally complete this work. With a deep sense of gratitude, I wish to express my sincere thanks to my supervisors, Assoc. Prof. Dr. Ramlan bin Mahmod and Dr. Rahmita Wirza O.K. Rahmat for their immense help and patience in guiding and supervising me throughout completing this research work. Many thanks to my colleagues and fellow friends for the help extended to me when I approached them and the valuable discussions we had during the course of research. The cooperation I received from other faculty members is gratefully acknowledged. I would like to share this moment of happiness with my parents Hj. Ahmad Zawawi bin Hj. Ali and Hjh. Siti Zubaidah bt Abdun, who taught me the values of faith and hard work by their own example.

The episode of acknowledgement would not be complete without the mention of my beloved wife Mrs. Norazmalinda binti Abdullah for her patience and for providing me constant encouragement who have rendered me enormous support during the whole tenure of my research. I am grateful for the inspiration and moral support she provided throughout my research work. Finally, I would like to thank all whose direct and indirect supports helped me upon completing my thesis on time.

I certify that an Examination Committee has met on 14 September 2006 to conduct the final examination of Md. Nabil Ahmad Zawawi on his master of science thesis entitled "A Robust Cover Generation Technique For Steganography Using 2D Images" in accordance with Universiti Pertanian Malaysia (Higher Degree) Act 1980 and Universiti Pertanian Malaysia (Higher Degree) Regulations 1981. The Committee recommends that the candidate be awarded the relevant degree. Members of the Examination Committee are as follows:

Mohamed Othman , PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Hajah Fatimah Dato' Ahmad, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Shyamala Doraisamy, PhD
Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Mohamad Shanudin Zakaria, PhD
Associate Professor
Faculty of Technology and Information Science
Universiti Kebangsaan Malaysia
(External Examiner)

HASANAH MOHD. GHAZALI, PhD
Professor/Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

This thesis submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Master of Science. The members of the Supervisory Committee are as follows:

Ramlan bin Mahmod, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Rahmita Wirza O.K. Rahmat, PhD
Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

AINI IDERIS, PhD
Professor/Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 8 FEBRUARI 2007

DECLARATION

I hereby declare that the thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UPM or other institutions.

MD. NABIL BIN AHMAD ZAWAWI

Date: 18 DECEMBER 2006

LIST OF TABLES

Table Page

LIST OF FIGURES

Figure Page