Universitatea Tehnică a Moldovei

APLICAȚIE DE PROTECȚIE A DATELOR CU UTILIZAREA METODEI STEGANOGRAFICE

DATA PROTECTION APPLICATION USING THE STEGANOGRAPHIC METHOD

Masterand:

Veaceslav Costin

Conducător: **Catanoi Maxim**

Chişinău 2020

Universitatea Tehnică a Moldovei
Facultatea Calculatoare Informatică şi Microelectronică
Departamentul Ingineria Software și Automatică

Admis la susţinere
Şef de departament: dr. conf.univ.
Fiodorov Ion
„23" decembrie 2020

APLICAȚIE DE PROTECȚIE A DATELOR CU UTILIZAREA METODEI STEGANOGRAFICE

Teză de master

Masterand: (V. Costin)
Conducător: (M.Catanoi)

Chişinău 2020

Rezumat

Steganografia este ştiinţa de a scrie mesaje ascunse astfel încât existenta lor să fie cunoscută numai de destinatar si expeditor.

Asigurarea securităţii datelor se îndreaptă în prezent către steganografie, adăugând un nivel nou în cadrul sistemelor de protecţie a datelor.

Metodele steganografice au fost folosite de mult timp, dar ele şi-au găsit abia acum un loc aparte în domeniul comunicaţiilor digitale. Instrumentele moderne utilizate în steganografie sunt situate deja în domeniul software.

La elaborarea acestei teze s-a efectuat studiul profund asupra temei alese. Rezultatul acestui studiu este elaborarea unei aplicaţii, ce poate fi utilizată în mediul Windows.

Incorporarea şi extragerea mesajelor se efectuează cu algoritmi speciali de criptare şi decriptare. Pentru aceste operaţii, special, a fost creat un algoritm care constă în ascunderea informaţiei în biţii cel mai puţin semnificativi. Astfel este posibilă criptarea şi decriptarea informaţiei, cu pierderi minimale şi chiar fără pierderi a calităţii imaginii rezultante, astfel modificările survenite nu pot fi observate cu ochiul liber.

Tehnologiile steganografice sunt o parte foarte importantă a viitorului securităţii Internet-ului pentru sisteme deschise ca acesta. În acest context steganografia a devenit un subiect de actualitate pe net, în contextul intimităţii electronice dar si a protecţiei copyright. Domeniul steganografiei este important în securitatea datelor. Împreună cu criptografia poate conduce la o securitate sporită.

Abstract

Steganography is the science of writing hidden messages so that their existence is known only to the recipient and the sender.

Ensuring data security is currently moving to steganography, adding a new level within the data protection systems.

Steganographic methods have been used for a long time, but they have only now found a special place in the field of digital communications. Modern tools used in steganography are already located in the software field.

The elaboration of this thesis was carried out in-depth study on the chosen topic. The result of this study is the development of an application, which can be used in the Windows environment.

The embedding and extraction of messages is performed with special encryption and decryption algorithms. For these operations, in particular, an algorithm was created that consists of hiding information in the least significant bits. Thus it is possible to encrypt and decrypt the information, with minimal losses and even without loss of the resulting image quality, so the changes that have occurred cannot be observed with the naked eye.

Steganographic technologies are a very important part of the future of Internet security for open systems like this. In this context, steganography has become a topical topic on the net, in the context of electronic privacy and copyright protection. The field of steganography is important in data security. Together with cryptography it can lead to increased security.

Cuprins

Lista abrevierilor

AVI – Audio Video Interleaved

WAV – Waveform Audio File Format

Mp3 – MPEG-1/2 Layer 3 (format audio multimedia)

DES – Data Encryption Standard

RSA – Rivest-Shamir-Adleman (criptosistem)

DES – Data Encryption Standard

AES – Advanced Encryption Standard

IDEA – International Data Encryption Algorithm

SSL – Secured Socket Layer

SHTTP – Secured HyperText Transfer Protocol

HTTP – HyperText Transfer Protocol

BMP – Bitmap

JPEG – Joint Photographic Experts Group

LSB – Least Significant Bit

ASCII – American Standard Code for Information Interchange

HTML – Hyper Text Markup Language

RGB – Red, Green, Blue

GIF – Graphics Interchange Format

DCT – discrete cosine transform

LZW – Lempel-Ziv-Welch (compresie)

MSB – Most-Significant-Bit

VM – Virtual machine

CLR – Common Language Runtime

Introducere

Reţelele moderne de calculatoare fac posibilă transmiterea documentelor, rapid şi ieftin. Distribuţia electronică a informaţiei protejate prin drepturi de autor, adesea este însoţită de copiere şi distribuţie ilegală. Din acest motiv, oamenii s-au gîndit cum să-şi protejeze munca efectuată, să prevină aceste activităţi ilegale.

Codifiarea informaţiei prin combinarea tehnicilor de criptare cu steganografia este rezolvarea acestei probleme, asigurînd protecţia transferului de date.

Această lucrare tratează codificarea informaţiei folosind aşa metode ca: criptografia, steganografia şi watermarking-ul.

Criptarea a fost folosită pentru protejarea comunicaţiilor de secole. În prezent, este utilizată în protejarea unei mari varietăţi de sisteme. Criptarea sau ascunderea codului de software este folosit în protecţia copierii de software, împotriva ingineriei inverse, analiza aplicaţiilor neautorizată.

Steganografia şi criptografia sunt metode diferite, dar au acelaşi scop şi fac parte din aceeaşi familie de modalităţi de codificare. Criptografia face ca, prin diferite procedee, mesajul să devină de nerecunoscut, însă steganografia ascunde mesajul astfel încît să nu poată fi văzut în mod obişnuit. Un mesaj criptat transmis, poate să fie bănuit, fie în timpul transmisiei, fie în momentul recepţionării, pe cînd un mesaj creat prin steganografie nu va prezenta aceste dezavantaje.

Tot de steganografie este legat şi conceptul de Watermarking şi anume includerea informaţiilor de copyright într-un fişier audio sau imagine, astfel încât fişierul să conţină informaţii despre autor, fară ca cineva să afle despre existenţa lor şi să le poată modifica.

Asigurarea securităţii datelor se îndreaptă în prezent către steganografie, adăugînd un nivel nou în cadrul sistemelor de protecţie a datelor.

Metodele steganografice au fost folosite de mult timp, dar ele şi-au găsit abia acum un loc aparte în domeniul comunicaţiilor digitale. Instrumentele moderne utilizate în steganografie sunt situate deja în domeniul software.

Concluzii

La elaborarea acestei teze s-a efectuat studiul profund asupra temei alese. Rezultatul acestui studiu este elaborarea unei aplicaţii, ce poate fi utilizată în mediul Windows.

Ideea acestui proiect constă în realizarea unei aplicaţii care va avea posibilitatea de a ascunde nişte informaţii secrete în fişierele cu imagini de formatul BMP. Încă un aspect esenţial este posibilitatea de a ascunde orice tip de fişier în imagini BMP. De asemenea şi posibilitatea de a utiliza şi alte formate de imagini, în calitate de purtător al informaţiei secrete, ca fişierele JPEG, GIF, PNG ş.a. Acest lucru reuşit a fost implementat cu o condiţie că aceste fişiere după incorporare a mesajului secret vor fi transformate în imagini BMP.

Incorporarea şi extragerea mesajelor se efectuează cu algoritmi speciali de criptare şi decriptare. Pentru aceste operaţii, special, a fost creat un algoritm care constă în ascunderea informaţiei în biţii cel mai puţin semnificativi. Astfel este posibilă criptarea şi decriptarea informaţiei, cu pierderi minimale şi chiar fără pierderi a calităţii imaginii rezultante, astfel modificările survenite nu pot fi observate cu ochiul liber.

Este bine de menţionat că orice steganosistem nu trebuie să manifeste indicii existenţei sale şi de regulă acest lucru este inacceptabil în domeniul steganografic, deci pentru ca depistarea steganositemului să fie practic imposibilă au fost utilizaţi doar ultimii biţi (a 8-lea bit din fiecare culoare RGB) din cei mai puţin semnificativi. În astfel de algoritmi este posibilă şi utilizarea biţilor 6 şi 7, dar evident acest lucru duce la scăderea bruscă a calităţii imaginii.

Tehnologiile steganografice sunt o parte foarte importantă a viitorului securităţii Internet-ului pentru sisteme deschise ca acesta. În acest context steganografia a devenit un subiect de actualitate pe net, în contextul intimitatii electronice dar si a protectiei copyright. Domeniul steganografiei este important în securitatea datelor. Impreună cu criptografia poate conduce la o securitate sporită.

Bibliografie

1 Securitatea Informationala. [Resursă electronică]. - Mod de acces: http://info--sec.blogspot.com/

2 Principiileşteganografiei. [Resursă electronică]. - Mod de acces: _http://facultate.regielive.ro/proiecte/calculatoare/principiileşteganografiei_digitaleşiăplicarea_lor_utiliz and_fisiere_grafice-63330.html

3 Eerdmans Commentary on the Bible, James D G Dunn, John W Rogerson, eds., Wm. B.

4 James Gannon, Stealing Secrets, Telling Lies: How Spies and Codebreakers Helped Shape the Twentieth Century, Washington, D.C., Brassey's, 2001, ISBN 1-57488-367-4

5 Whitfield Diffie şi Martin Hellman, "New Directions în Cryptography", IEEE Transactions on Information Theory, vol. IT-22, Nov. 1976, pp: 644–654. (pdf)

6 Oded Goldreich, Foundations of Cryptography, Volume 1: Basic Tools, Cambridge University Press, 2001, ISBN 0-521-79172-3

7 AJ Menezes, PC van Oorschot şi SA Vanstone, Handbook of Applied Cryptography ISBN 0-8493-8523-7

8 Securizarea datelor prin stenografie. [Resursă electronică]. - Mod de acces: https://www.scribd.com/doc/40655925/steganografie

9 Solutie steganografie – Care este diferenta dintre cele doua imagini? [Resursă electronică]. - Mod de acces: http://www.worldit.info/articole/solutie-steganografie-care-este-diferenta-dintre-cele-doua-imagini/

10 Cercetări privind utilizarea metodelor steganografice și criptografice în vederea creșterii securității sistemelor cyber-fizice [Resursă electronică]. - Mod de acces: http://old.unitbv.ro/Portals/31/Burse%20doctorale/134378/Seminar/S2-04-Anca%20Nicu.pdf

11 FIPS PUB 197: The official Advanced Encryption Standard

12 Steganografie Sau Cum Ascundem Un Fisier In Alt Fisier Folosind Doar CMD-Ul [Resursă electronică]. - Mod de acces: https://www.tutorialevideo.info/steganografie-sau-cum-ascundem-un-fisier-alt-fisier-folosind-doar-cmd-ul/

13 Steganografia – definitie, istoric, principia [Resursă electronică]. - Mod de acces: https://despretot.info/steganografia-definitie-dex/