МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ВІННИЦЬКИЙ ДЕРЖАВНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

В.О. Хорошко, О.Д. Азаров, М.Є. Шелест, Ю.Є. Яремчук

ОСНОВИ КОМП'ЮТЕРНОЇ СТЕГАНОГРАФІЇ

Затверджено Ученою радою Вінницького державного технічного університету як навчальний посібник для студентів і аспірантів, що навчаються з напрямку підготовки 1601 - "Інформаційна безпека". Протокол № 4 від 28 листопада 2002 р.

Вінниця ВДТУ 2003

УДК 681.322:621.391
Х 87

Рецензенти:
В.П. Тарасенко, доктор технічних наук, професор
Ю.Я. Самохвалов, доктор технічних наук, професор
В.П. Майданюк, кандидат технічних наук, доцент

Рекомендовано до видання Ученою радою Вінницького державного технічного університету Міністерства освіти і науки України (протокол №4 від 28.11.2002 р.) та Ученою радою Інституту інформаційно-діагностичних систем Національного авіаційного університету Міністерства освіти і науки України (протокол №3 від 21.10.2002 р.)

В.О. Хорошко, О.Д. Азаров, М.Є. Шелест, Ю.Є. Яремчук
Х87 Основи комп'ютерної стеганографії. Навчальний посібник. – Вінниця: ВДТУ, 2003. – 143 с.

В посібнику розглядаються питання, що відносяться до одного з перспективних напрямків інформаційної безпеки – стеганографії. Розглядаються основні проблеми і методи стеганографії.

Рекомендується для студентів і аспірантів, що навчаються з напрямку підготовки 1601 «Інформаційна безпека», а також для фахівців, що працюють в галузі захисту інформації.

УДК 681.322:621.391

ПЕРЕДМОВА

Під інформаційною безпекою, як правило, розуміють складову частину національної безпеки, що характеризує стан захищеності національних інтересів в інформаційній сфері як від зовнішніх, так і внутрішніх загроз.

Державна політика в сфері інформаційної безпеки спрямована на нагромадження і захист національних інформаційних ресурсів, розробку і впровадження сучасних безпечних інформаційних технологій, побудову захищеної національної інформаційної інфраструктури.

Сучасні умови розвитку обчислювальної техніки й інформаційних технологій висувають певні вимоги до зберігання конфіденційної інформації. Найбільш розповсюдженим засобом її захисту є використання криптографічних методів, однак їхнє застосування при транспортуванні носіїв інформації або передаванні в локальних мережах та Інтернет не завжди можливе. У таких ситуаціях досить актуальними стають стеганографічні методи приховування інформації. Ці методи основані на вже відомих теоріях і технологіях.

Принцип стеганографії – приховування одного масиву інформації в іншому – в останні роки знайшов широке застосування. Комп'ютерні файли (зображення, звукові записи і т.п.) мають області, що не використовуються або не є важливими, й, відповідно, існує можливість заміщати їх необхідною спеціальною інформацією. Розвиток інформаційних технологій привів до створення цілого класу методів і програмних продуктів, що дозволяють розмістити приховану інформацію в цифрові документи практично всіх типів.

Навчальний посібник «Основи комп'ютерної стеганографії» є однією з перших спроб системного викладення стеганографічних методів.

Наукову новизну книги визначають:

– розроблена вперше класифікація методів приховування інформації;

– узагальнена модель стеганографічної системи;

– відомості про нові прикладні напрямки розвитку та застосування комп'ютерної стеганографії.

Великий науковий та практичний інтерес викликають розділи книги, які присвячені класифікації стеганографічних методів, основним

положенням теорії комп'ютерної стеганографії, цифровим водяним знакам та відбиткам.

Головною метою книги є огляд сучасного стану та шляхи розвитку нового наукового напрямку «Комп'ютерна стеганографія».

Деякі положення і висновки, що зроблені авторами, можуть стати предметом окремих наукових дискусій і обговорень, цим самим підкреслюється її цінність з погляду активізації процесів розробки і досліджень у сфері інформаційної безпеки.

У цілому книга, без сумніву, є значним внеском у подальший розвиток теорії і методів захисту інформації. Її положення викликають інтерес і будуть корисні для широкого кола науковців і практиків, що працюють в області інформаційної безпеки України.

А. В. Литвиненко.
Заступник директора
Національного інституту
стратегічних досліджень

ВСТУП

Стрімкий розвиток цифрових технологій та засобів телекомунікацій стимулює створення різноманітних методів захисту інформації. Відомо, що для гарантованого захисту вмісту повідомлення існує два різних по суті підходи.

Перший - це блокування несанкціонованого доступу до інформації шляхом шифрування повідомлення. Для цієї мети використовуються криптографічні методи захисту. У криптограмах, як правило, відсутні структура і закономірності, які властиві відкритим текстам. Тому, при проведенні моніторингу мереж телекомунікацій, вони легко автоматично виділяються з інформаційного потоку.

Другий підхід полягає в тому, що повідомлення, яке передається, намагаються приховати так, що б його неможливо було знайти. Для приховування факту існування інформації застосовуються стеганографічні методи захисту, які значно знижують ймовірність її виявлення. На відміну від криптографічного захисту, коли в «зловмисника» існує можливість знайти, перехопити та зробити спробу дешифрувати криптограму, стеганографічні методи дозволяють вмонтувати передавану інформацію в невинні на вигляд послання так, щоб не можна було навіть запідозрити існування підтексту. Шанси знайти приховане повідомлення - невеликі, але на той випадок, якщо повідомлення все-таки буде виявлено, його можна ще додатково зашифрувати. У цьому випадку стеганографія являє собою більш високий рівень захисту інформації в порівнянні з методами криптографії.

Стеганографія – це мистецтво і наука організації зв'язку, при якій приховується, власне, наявність самого зв'язку.

В найближчі роки інтерес до стеганографії буде підсилюватися. Основна передумова для цього сформована вже сьогодні. Це стрімкий розвиток комп'ютерної мережі загального користування Інтернет з такими невирішеними і суперечливими проблемами, як захист авторських прав, захист прав на особисту таємницю, організація електронної торгівлі, протиправна діяльність хакерів і терористів.

В запропонованій роботі проведений огляд сучасного стану порівняно нового наукового напрямку в галузі захисту інформації - комп'ютерної стеганографії. Систематизовані деякі теоретичні положення

і досліджені практичні методи стеганографічного захисту, які з'явилися в науковій літературі до 2003 року.

Даний матеріал базується на лекціях, які були прочитані в 2000-2002 роках у Національній академії Служби безпеки України і Національному авіаційному університеті на кафедрі засобів захисту інформації з дисципліни «Методи та засоби захисту інформації», а також у Вінницькому державному технічному університеті на кафедрі захисту інформації з дисципліни "Стеганографія".

У двох перших розділах роботи проведений аналіз існуючих уявлень про стеганографію та стеганографічний аналіз. Зокрема, дана класифікація стеганографічних систем та можливих атак на них.

У третьому розділі систематизовані відомі підходи до стеганографічного приховування в різних типах інформаційного середовища. Описані відомі методи приховування інформації в текстовому середовищі, у звуковому середовищі, у зображеннях і відео.

В останніх трьох розділах роботи наводяться відомості про нові прикладні напрямки комп'ютерної стеганографії, а саме, приховані канали у комп'ютерних мережах, технології цифрових водяних знаків і цифрових відбитків, які останнім часом мають усе більше практичне значення.

Автори висловлюють глибоку подяку професору Ю.Я.Самохвалову, професору В.П. Тарасенку та доценту В.П. Майданюку за уважне резензування книги, що сприяло значному поліпшенню її змісту.

ЛІТЕРАТУРА

1. *Артёхин Б.В.* Стеганография // Информационно-методический журнал «Защита информации. Конфидент». – 1996. – №4. – С. 47–50.
2. *Kahn D.* The History of Steganography // Information Hiding: First International Workshop "InfoHiding'96", Springer as Lecture Notes in Computing Science, vol.1174, 1996. - pp.1-6.
3. *Кан Д.* Взломщики кодов: Пер. с англ. - М.: Центрполиграф, 2000. - 472с.
4. *Scott G.* Schola steganographica, Jobus Hertz, printer, 1680.
5. *Шеннон К.* Теория связи в секретных системах / Работы по теории информации и кибернетике. - М.: Иностр. лит, 1963. – С.333–402.
6. *Клопов В.А., Мотуз О.В.* Основы компьютерной стеганографии // Информационно-методический журнал «Защита информации. Конфидент». – 1997. – №4. – С.43–48.
7. *Трубей А.И., Шелест М.Е.* Обзор современных представлений о цифровой стеганографии // Научно-технический журнал «Проблемы защиты информации». – Минск: БГУ. – 2001. – №3. – С.5–15.
8. *Phitzmann B.* Information hiding terminology // Information Hiding: First International Workshop "InfoHiding'96", Springer as Lecture Notes in Computing Science, vol.1174, 1996. - pp. 374-350.
9. *Simmons G.I.* The prisoners' problem and subliminal channel // Advances in cryptography: Processing of CRYPTO'83. - pp.51-67.
10. *Craver S.* On public-key steganography in the presence of an active warden. Technical report RC 20931, IBM, 1997.
11. *Cachin C.* An Information-Theoretic Model for Steganography // Information Hiding: Second International Workshop "InfoHiding'98", Springer as Lecture Notes in Computing Science, vol.1525. - pp.306-318.
12. *Bender W., Gruhl D., Morimoto N.* Techniques for data hiding // IBM system journal, vol.35, no 3/4, 1996, pp.313-336.
13. *Cox I.J.* Secure spread spectrum watermarking for multimedia. Technical report, NEC institute, 1995.
14. *Wayner P.* If sb266 wants plaintext, give them plaintext // RISKS Digest, 11(71), may 1991.
15. *Wayner P.* Mimic function // Cryptologia v.XVI no 3 (july 1992), pp. 193-214.

16. *Moller S., Pfitzmann A., Stirand I.* Computer based steganography: how it works and why therefore any restriction on cryptography are nonsence, at best // Information Hiding: First International Workshop "InfoHiding'96", Springer as Lecture Notes in Computing Science, vol.1174, 1996. - pp. 7-21.
17. *Aura T.* Practical invisibility in digital communication // Information Hiding: First International Workshop "InfoHiding'96", Springer as Lecture Notes in Computing Science, vol.1174, 1996. - pp. 265-278.
18. *Fridrich J.* A new steganographic method for palette-based image // Proceedings of the ISBT PISP conference, Savannah, Georgia, Apr.1998, pp.285-289.
19. *Matsui K., Tanaka K.* Video-steganography: how to secret embed a signature in a picture // IMA intellectual property project proceeding, vol.1, no.1, 1994, pp.187-205.
20. *Zao J., Koch E.* Embedding robust labels into images for copyright protection // Proceeding of the international conference on intellectual property rights for information, knowledge and new techniques, Munchen-Wien, Verlag, 1995, pp.242-251.
21. *Smith J., Comiskey B.* Modulation and information hiding in image // Information Hiding: First International Workshop "InfoHiding'96", Springer as Lecture Notes in Computing Science, vol.1174, 1996. - pp.207-227.
22. *Pitas I.* A method for signature casting on digital images // International conference on image processing, vol.3, IEEE Press, 1996, pp.215-218.
23. *Sandford M.T., Handel T.G., Ettinger J.M.* Data embedding method // Proceeding of the SPIE 2615, Integration issues in large commercial media delivery systems, 1996, pp.226-259.
24. *Коростиль Ю.М., Шелест М.Е.* Принципы построения стеганографических систем со структурной технологией // Праці VII міжнародної конференції з автоматичного управління "Автоматика-2000", Львів, вересень 2000 р., секція 7, частина 1. - Львів: ДНДІІІ. - С.286–273.
25. *Chang L., Moskowitz I.* Critical analysis of security in voice hiding techniques // First international conference "Information and communication security" ICIS'97, China, nov.11-14, 1997. Lecture notes in computer science, no.1334. - pp.203-215.

26. *Шелест М.Е.* Некоторые подходы к сокрытию информации в звуковой среде // Сборник научных трудов КМУГА "Защита информации". - Киев: КМУГА, 2000. – С.20–26.
27. *Мухачев В.А., Шелест М.Е.* Метод внедрения текстовых сообщений в звуковую среду музыкальных произведений // Збірник наукових праць Інституту проблем моделювання в енергетиці НАН України, вип.16. - Київ: ІПМЕ НАНУ, 2001.
28. *Мухачев В.А., Шелест М.Е.* Возможность скрытой передачи данных в криптопротоколах, основанных на свойствах эллиптических кривых // Науково-технічний збірник "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип.4. – Київ: КПІ, 2002.– С. 132–136.
29. *Kutter M., Petitcolas F.A.P.* Fair benchmarking for image watermarking system // Proceeding of the SPIE 3657, Security and watermarking of multimedia contents, 1999, p.226-239.
30. *Bender W., Gruhl D., Morimoto N.* Techniques for data hiding // Proceedings of the SPIE 2420, Storage and retrieval for image and video databases III, 1995, pp.164-173.
31. *Hartung F., Girod B.* Fast public-key watermarking of compressed video // International conference on image proceeding, Santa Barbara, California, oct.1997.
32. *Jonson N., Jajodia S.* Exploring steganography: seeing the unseen // IEEE Computer, vol.31, no.2, 1998, pp.26-34.
33. *Zhao J.* A WWW service to embed and prove digital copyright watermarks // Proceeding of the European conference on multimedia application, services and techniques, 1996, pp.695-709.
34. *O'Ruanaidh J., Pun T.* Rotation, translation and scale invariant digital image watermarking // International conference on image proceeding, Santa Barbara, California, oct.1997, pp.536-539.
35. *Antonini M.* Image coding using wavelet transform // IEEE Transactions on image processing, vol.1, no.2, 1992, pp.205-220.
36. *Xia X., Boncelet C., Arce G.* Wavelet transform based watermark for digital images // Optic express, vol.3, no.12, 1998, pp.497-511.
37. *Hartung F., Girod B.* Digital watermarking secure spread spectrum watermarking for multimedia // Proceeding of the IEEE International

conference on acoustics, speech and signal processing, vol.4, Germany, Apr.1997, pp.2621-2624.

38. *Braudway G.* Protecting publicly-available image with an invisible image watermark // International conference on image proceeding, Santa Barbara, California, oct.1997.
39. *Delaige J.-F.* Digital image protection techniques in a broadcast framework: overview // Proceeding of the European conference on multimedia application, service and techniques, Louvain-la-Neuve, Belgium, May 1996, pp.711-728.
40. *Hayes M.H.* The reconstruction of a multidimensional sequence // IEEE Transactions on acoustics, speech and signal processing, Apr. 1992, pp.140-154.
41. *Kutter M., Jordan F., Bossen F.* Digital signature of color image using amplitude modulation // Proceeding of the SPIE 3022, storage find retraival for image and video database *V*, 1997, pp.518-526.
42. *Koch E., Zhao J.* Towards robust and hidden image copyright labeling // IEEE workshop on nonlinear signal and image processing, Thessaloniki, Greece, Oct. 1995, pp.452-455.
43. *Bruyndonckx O., Quisquater J.-J., Macq B.* Spatial method for copyright labeling on digital images // Nonlinear signal processing workshop, Thessaloniki, Greece, 1995, pp.456-459.
44. *Puate J., Jordan F.* Using fractal compression scheme to embed a digital signature into an image // Proceeding of the SPIE 2915, Video techniques and software for full-service network, 1996, pp.108-118.
45. "Talisman" <htpp://www.cordis.lu/espirit/src/talisman.htm>.
46. *Wagner N.R.* Fingerprint // Proceeding of the 1983 IEEE symposium on security and privacy, Oakland, California, USA, Apr.1983, pp.18-22.
47. *Pfitzmann B., Schunter M.* Asymmetric fingerprint // Advances in cryptology, Proceeding of EUROCRYPT'96, vol.1070 of lecture notes in computer science, Springer-Verlag, 1996, pp.84-95.
48. *Chaum D.* Blind signature for untraceable payment // Advances in cryptology proceeding of CRYPTO'82, Plenum press, 1983, pp.199-203.
49. *Katzenbeisser S.* Breaking PGMStealth Using Laplace Filters // Information Hiding: Second International Workshop "InfoHiding'98", Springer as Lecture Notes in Computing Science, vol.1525, 1998.

50. *Jonson N.F., Jajodia S.* Steganalysis of images created using current steganography software // Information Hiding: Second International Workshop "InfoHiding'98", Springer as Lecture Notes in Computing Science, vol.1525, 1998.
51. *Simmons G.J.* Subliminal Channels: Past and Present // European Trans. on Telecommunication, 5(4), 1994, pp.459-473.
52. *Silverman J.* The Arithmetic of Elliptic Curves. - New York: Springer, 1986, - 400 p.
53. *Young A., Yung M.* The Dark Side of Black-Box Cryptography // Advances in Cryptology – CRYPTO'96, pp.89-103, Springer-Verlag.
54. *Young A., Yung M.* Kleptography: using cryptography against cryptography // Advances in Cryptology – CRYPTO'97, pp.52-63, Springer-Verlag.
55. *Барсуков В.С.* Стеганографические технологии защиты документов, авторских прав и информации // Обзор специальной техники. – 2000. – №2. – С.31–40.
56. *Андерсон Р., Нидхем. Р., Шамир А.* Стеганографическая система файлов // Информационно-методический журнал «Защита информации. Конфидент». – 1999. – №4–5. – С.97–99.
57. *Шелест М.Е.* Особенности организации алгоритмических сообщений для стеганосистем // Збірник наукових праць «Моделювання та інформаційні технології», вип.2. - Київ: НАНУ ІПМЕ, 1999. – С.60–67.

ЗМІСТ

Навчальне видання

Хорошко Володимир Олексійович
Азаров Олексій Дмитрович
Шелест Михайло Євгенович
Яремчук Юрій Євгенович

ОСНОВИ КОМП'ЮТЕРНОЇ СТЕГАНОГРАФІЇ

Навчальний посібник

Оригінал-макет підготовлено Яремчуком Ю.Є.

Редактор В.О. Дружиніна

Начально-методичний відділ ВДТУ
Свідоцтво Держкомінформу України
серія ДК № 746 від 25.12.2001 р.
21021, м. Вінниця, Хмельницьке шосе, 95, ВДТУ

Підписано до друку 04.03.2003 р.
Формат 29.7×42 $^{1}/_{4}$
Друк різографічний
Тираж 175 прим.
Зам. № 2003-031

Гарнітура Times New Roman
Папір офсетний
Умови. друк. арк. 6,04

Віддруковано в комп'ютерному інформаційно-видавничому центрі
Вінницького державного технічного університету
Свідоцтво Держкомінформу України
серія ДК № 746 від 25.12.2001 р.
21021, м. Вінниця, Хмельницьке шосе, 95, ВДТУ