

В. Г. Грибунин, В. Е. Костюков,
А. П. Мартынов, Д. Б. Николаев, В. Н. Фомченко

СТЕГАНОГРАФИЧЕСКИЕ СИСТЕМЫ. ЦИФРОВЫЕ ВОДЯНЫЕ ЗНАКИ



ФГУП «Российский федеральный ядерный центр –
Всероссийский научно-исследовательский институт
экспериментальной физики»

**В. Г. Грибунин, В. Е. Костюков, А. П. Мартынов,
Д. Б. Николаев, В. Н. Фомченко**

СТЕГАНОГРАФИЧЕСКИЕ СИСТЕМЫ. ЦИФРОВЫЕ ВОДЯНЫЕ ЗНАКИ

Учебно-методическое пособие

Под редакцией доктора технических наук В. Г. Грибунина

Саров
2016

УДК 004.056(075.8)
ББК 32.81Я73
С79

Одобрено научно-методическим советом Саровского физико-технического института Национального исследовательского ядерного университета «МИФИ» и ученым советом ФГМУ «Институт информатизации образования» Российской академии образования

Рецензенты: ректор НГТУ им. Р. Е. Алексеева профессор, д-р техн. наук С. М. Дмитриев; декан радиофизического факультета ННГУ им. Н. И. Лобачевского профессор, д-р физ.-мат. наук А. В. Якимов

С79 Грибунин, В. Г., Костюков, В. Е., Мартынов, А. П., Николаев, Д. Б., Фомченко, В. Н.

Стеганографические системы. Цифровые водяные знаки: Учеб.-метод. пособие / Под ред. д-ра техн. наук В. Г. Грибунина. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2016. – 210 с. : ил.

ISBN 978-5-9515-0330-5

В стеганографии обычно изучаются две группы вопросов: скрытие информации и противодействие ему, а также внедрение цифровых водяных знаков и противодействие осуществляющим это системам. Определенный интерес имеют проблемы, непосредственно не относящиеся к области стеганографии, но близкие к ней, использующие те же методы обработки изображений. Рассмотрены вопросы идентификации изображений по источникам их формирования, а также защита изображений от подделки. Кратко описаны законченные европейские проекты в области цифровых водяных знаков, а также даны аннотации некоторых англоязычных книг по их внедрению.

Учебно-методическое пособие предназначено для студентов, аспирантов, научных работников, изучающих вопросы обеспечения безопасности информации, а также для инженеров-проектировщиков средств обеспечения безопасности информации. Несомненный интерес оно вызовет также у специалистов в области теории информации и цифровой обработки сигналов.

УДК 004.056(075.8)
ББК 32.81Я73

ISBN 978-5-9515-0330-5

© ФГУП «РФЯЦ-ВНИИЭФ», 2016

Содержание

Введение	6
1. Стеганоанализ файлов изображений и видео	7
1.1. Классификация методов стеганоанализа	7
1.2. Стеганоанализ наименьших значащих бит	8
1.2.1. Визуальные атаки	8
1.2.2. Использование для стеганоанализа статистики хи-квадрат	12
1.2.3. Использование для стеганоанализа функции искажение-скорость	15
1.2.4. Использование для стеганоанализа НЗБ статистики пар значений	19
1.2.5. Использование для стеганоанализа НЗБ вейвлет-декомпозиции ..	20
1.2.6. Стеганоанализ НЗБ на основе статистики числа переходов	24
1.2.7. Стеганоанализ НЗБ на основе статистики длин битовых серий ..	25
1.3. Подходы универсального стеганоанализа	26
1.3.1. Критерии информативности системы признаков	26
1.3.2. Построение классификатора признаков. Описание алгоритма SVM	29
1.4. Стеганоанализ изображений формата JPEG	38
1.4.1. Методы стеганоанализа, использующие характеристики качест- ва изображений и классификацию SVM	38
1.4.2. Методы стеганоанализа, использующие дифференциальные ха- рактеристики коэффициентов ДКП и классификацию SVM	45
1.4.3. Дискриминантный метод стеганоанализа, использующийся в программном обеспечении Stegdetect 0.6	47
1.5. Стеганоанализ видео	48
1.6. Программное обеспечение стеганоанализа	53
Вопросы для самопроверки к разделу 1	58
2. Скрытие информации в файлах изображений	60
2.1. Алгоритмы J-steg, Hide and Seek	60
2.2. Алгоритм F5	61
2.3. Алгоритмы модификации НЗБ. Стохастическая модуляция	62
2.4. Алгоритм OutGuess	65
2.5. Алгоритм HUGO	67
2.6. Матричное кодирование	70
Вопросы для самопроверки к разделу 2	80

3. Анализ основных способов разрушения ЦВЗ, в том числе с использованием аффинных преобразований над мультимедийными данными, содержащими ЦВЗ	81
3.1. Основные способы удаления ЦВЗ из изображения	81
3.1.1. Способы удаления ЦВЗ без анализа стего	81
3.1.2. Способы удаления ЦВЗ на основе анализа стего	83
3.2. Геометрические атаки	87
3.2.1. Описание геометрических атак	87
3.2.2. Аффинные преобразования изображений	89
3.3. Анализ способов искажения ЦВЗ в аудиосигналах	96
3.3.1. Используемые обозначения и классификация атак	96
3.3.2. Атаки, работающие во временной области	96
3.3.3. Описание атак, работающих в частотной области	103
3.3.4. Атаки, ориентированные на удаление ЦВЗ из файлов, содержащих аудиоинформацию в сжатом виде	107
3.3.5. Атаки, ориентированные на конкретный тип стегоалгоритмов ..	108
3.3.6. Обзор используемых психоакустических моделей системы слуха человека для подстройки атак	108
3.3.7. Подходы к подстройке атак в соответствии с системой восприятия звука человека	111
Вопросы для самопроверки к разделу 3	112
4. Методы повышения помехоустойчивости внедрения ЦВЗ	114
4.1. Обзор методов	114
4.2. Обзор алгоритмов ЦВЗ изображений, устойчивых к геометрическим атакам	122
4.2.1. Общее описание подходов	122
4.2.2. Анализ стегоалгоритма на основе лог-полярных преобразований	125
4.2.3. Анализ стегоалгоритма на основе деформируемой сетки	133
Вопросы для самопроверки к разделу 4	137
5. Идентификация цифровых фотоаппаратов по аппаратурно-уникальным признакам	138
5.1. Формирование цифрового изображения внутри цифрового фотоаппарата	138
5.1.1. Оптическая система	138
5.1.2. Электронная система цифрового фотоаппарата. Сенсор с цветофильтрами	140
5.1.3. Электронная система ЦФ. Интерполяция цветов	144
5.1.4. Типовые операции тракта цифровой обработки изображений в цифровом фотоаппарате	145
5.1.5. Особенности форматов изображений, регистрируемых цифровым фотоаппаратом	148

5.2. Основные подходы к идентификации моделей ЦФ по ЦИ	148
5.3. Основные подходы к идентификации конкретных экземпляров ЦФ по ЦИ	153
Вопросы для самопроверки к разделу 5	154
6. Методы борьбы с подделками изображений	155
6.1. Подделки изображений как средство информационного противоборства	155
6.2. Методы обнаружения подделок копированием-удалением	158
6.2.1. Метод полного перебора	159
6.2.2. Автокорреляционный метод	160
6.2.3. Обнаружение подделки удалением-копированием путем поблочного сравнения	161
6.3. Самокорректирующиеся изображения	165
6.3.1. Первый метод	165
6.3.2. Второй метод	168
6.3.3. Результаты экспериментов	173
Вопросы для самопроверки к разделу 6	176
7. Известные исследовательские проекты в области ЦВЗ	177
7.1. Проект CNIT – национального межуниверситетского консорциума по телекоммуникациям	177
7.2. Проект GAUSS	180
7.3. Деятельность UNIGE	181
7.4. Проект – Certification for Watermarking	182
7.5. Проект WAVILA	182
7.6. Изданные за рубежом книги по технологиям цифровых водяных знаков	183
Вопросы для самопроверки к разделу 7	185
Ответы на вопросы для самопроверки к разделу 1	186
Ответы на вопросы для самопроверки к разделу 2	190
Ответы на вопросы для самопроверки к разделу 3	192
Ответы на вопросы для самопроверки к разделу 4	196
Ответы на вопросы для самопроверки к разделу 5	198
Ответы на вопросы для самопроверки к разделу 6	199
Ответы на вопросы для самопроверки к разделу 7	200
Список литературы	202

55. Sprenger S. Time and pitch scaling of audio signals, <http://www.dsppdimension.com/html/timepitch.html>
56. Roucos S. и др. High quality time-scale modification for speech // Proc. ICASSP, 1985. P. 493-496.
57. MP3Stego, Интернет.
58. Сэломон Д. Сжатие данных, изображений и звука. М.: Техносфера, 2004.
59. Проект Certimark, документ D 5.2, 2002 г.
60. Campisi P., Kundur D., Neri A. Robust digital watermark in the ridgelet domain // IEEE signal processing letters. 2004. Vol. 11, № 10. P. 826–835.
61. Zhang Z. Digital image watermark algorithm in the curvelet domain // Proc. IIHMSP-2006. To appear.
62. Xu Z. A novel watermarking scheme in contourlet domain based on independent component analysis // Proc. IIHMSP-2006. To appear.
63. Jayalakshmi M. Blind watermarking in contourlet domain with improved detection // Proc. IIHMSP-2006. To appear.
64. Li H. A novel blind watermarking algorithm in contourlet domain // ICPR-2006. To appear.
65. Baaziz N. Adaptive watermarking schemes based on a redundant contourlet transform // Proc. ICIP-2005.
66. 1st Wavila Challenge, Barcelona, 2005.
67. Merhav N., Ordentlich E. On causal and semicausal codes for joint information embedding and source coding // IEEE trans. inform. Theory. 2006. Vol. 52, № 1. P. 213–226.
68. Kesal M., Mıhçak M., Kötter R., Moulin P. Iteratively decodable codes for watermarking applications // 2nd symp. turbo codes and related topics, Brest, France, 2000.
69. Zamir R., Shamai S., Erez U. Nested linear/lattice codes for structured multiterminal binning // IEEE Trans. inf. theory. 2002. Vol. 48, № 6. P. 1250–1276.
70. Chou J., Pradhan S., Ramchandran K. Turbo coded trellis based constructions for data embedding: channel coding with side information // Proc. 35th asilomar conf. 2001. P. 305–309.
71. Chou J., Ramchandran K. Robust turbo-based data hiding for image and video sources // IEEE Int. conf. image processing, Rochester, NY, 2002.
72. Solanki K., Jacobsen N., Madhow U., Manjunath B., Chandrasekaran S. Robust image-adaptive data hiding using erasure and error correction // IEEE Trans. image process. 2004. Vol. 13, № 12. P. 1627–1639.
73. Su J., Girod B. Power-spectrum condition for energy-efficient watermarking // Proc. ICIP, 1999.
74. Voloshynovskiy S., Herrigel A., Pun T. A stochastic approach to content adaptive digital image watermarking // International workshop on information hiding. Vol. LNCS 1768 of Lecture Notes in Computer Science. 1999. P. 212–236.
75. Ruanaidh J., Pun T. Rotation, scale and translation invariant spread spectrum digital image watermarking // Signal processing. 1998. Vol. 66. P. 303–317.

76. Digimarc patent, WO 96/36163, Steganography systems, 1996.
77. Heerger F. Embedding invisible information in color images, ICIP97, 1997.
78. Pereira S., Pun T. Fast robust template matching for affine resistant image watermarking // International workshop on information hiding, 1999.
79. Piva A., Barni M., Bartolini F. Copyright protection of digital images by means of frequency domain watermarking // Proc. of SPIE 3456. 1998. P. 25–35.
80. Kutter M. Watermarking resisting to translation, rotation and scaling // Proc. of SPIE: Multimedia systems and applications, 1998.
81. Pereira S., Voloshynovskiy S., Pun T. Optimal transform domain watermark embedding via linear programming // Signal processing, special issue: information theoretic issues in digital watermarking, 2001.
82. Voloshynovskiy S., Deguillaume F., Pereira S., Herrigel A., Pun T. Method for adaptive digital watermarking robust against geometric transforms, European patent application PCT/IB00/01089, filed August 3, 2000.
83. Kutter M., Bhattacharjee S., Ebrahimi T. Towards Second Generation Watermarking Schemes // Proc. ICIP. 1999. Vol. 1. P. 320–323.
84. Dugelay J., Petitcolas F. Image watermarking: possible counterattacks against random geometric distortions // Proceedings of SPIE: security and watermarking of multimedia content II. 2000. Vol. 3971. P. 24–26.
85. Bas P., Chassery J., Macq B. Robust watermarking based on the warping of predefined regular triangular patterns // Proc. of SPIE: security and watermarking of multimedia content II. 2000. Vol. 3971.
86. Hartung F., Su J., Girod B. Spread spectrum watermarking: malicious attacks and counter-attacks // Proc. of SPIE: security and watermarking of multimedia contents. 1999. Vol. 3657.
87. Dugelay J., Rey C. Method of marking a multimedia document having improved robustness // Patent EP 99480075.3, July 1999.
88. Lin C., Wu M., Bloom J., Cox I., Miller M., Lui Y. Rotation, Scale, and translation resilient public watermarking for images // Proc. of SPIE: security and watermarking of multimedia contents II. 2000. Vol. 3971. P. 90–98.
89. Voloshynovskiy S., Deguillaume F., Pun T. Multibit digital watermarking robust against local non-linear geometrical transformations, ICIP 2001, Int. conf. image processing, Thessaloniki, Greece, October 07–10, 2001.
90. Voloshynovskiy S., Deguillaume F., Pun T. Method for digital watermarking robust against local and global geometrical distortions and projective transforms // US patent application, October, 2001.
91. Lee C., Lee H., Suh Y. Image watermarking resistant to combined geometric and removal attacks // International journal of image and graphics. 2005. Vol. 5, № 1, P. 1–29.
92. Topak E., Voloshynovskiy S., Koval O., Mihcak M., Pun T. Towards geometrically robust data-hiding with structured codebooks // ACM multimedia systems journal, special issue on multimedia and security, 2005. Submitted.

93. Topak E., Voloshynovskiy S., Koval O., Mihcak M., Pun P. Security analysis of robust data-hiding with geometrically structured codebooks // Edward J. Delp III and Ping W. Wong, editors, *Security, Steganography, and Watermarking of Multimedia Contents VII*, San Jose, California, USA, January 2005. SPIE.

94. Topak E., Voloshynovskiy S., Koval O., Vila-Forc'en J., Pun T. On security of geometrically-robust data-hiding // *Proc. 6th international workshop on image analysis for multimedia interactive services*, Montreux, Switzerland, April 2005.

95. Bas P., Lobo Guerrero A. Several considerations on the security of a feature-based synchronisation scheme for digital image watermarking // *First wavila challenge*, WACHA 05, Barcelona, Spain, June 2005.

96. Barni M. Coping with random bending attack by means of exhaustive search detection // *First wavila challenge*, WACHA 05, Barcelona, Spain, June 2005.

97. Barni M. Effectiveness of exhaustive search and template matching against watermark desynchronization // *IEEE signal processing letters*, 2005.

98. Solachidis S., Tsekeridou S., Nikolopoulos S., Pitas I. Self-similar watermarks for counterfeiting geometrical attacks // *First wavila challenge*, WACHA 05, Barcelona, Spain, June 2005.

99. Zaidi A., Boyer R., Duhamel P. Audio watermarking under desynchronization and additive noise attacks // *IEEE Transactions on signal processing*, 2005. Accepted for publication.

100. Avcibas I. Image quality statistics and their use in steganalysis and compression. PhD Thesis, Boğaziçi university, 2001.

101. Fridrich J. Security of fragile authentication watermarks with localization // *Security and watermarking of multimedia contents*. *Proc. SPIE*. 2002. Vol. 4675. P. 691–700.

102. Campisi P., Kundur D., Hatzinakos D., Neri A. Compressive data hiding: An unconventional approach for improved color image coding // *EURASIP journal on applied signal processing*. 2002. Vol. 2002, № 2. P. 152–163.

103. Piva A., Caldelli R., Bartolini F., Barni M. Semi-fragile watermarking for still images authentication and content recovery // *Proc. of WIAMIS 2004*, 5-th international workshop on image analysis for multimedia interactive services, 21–23 April 2004, Lisboa, Portugal.

104. Thiemert S., Vogel T., Dittmann J., Steinebach M. A high-capacity block based video watermark // *30th EUROMICRO Conference*, 2004, Rennes, France.

105. Deguillaume F., Voloshynovskiy S., Pun T. Secure hybrid robust watermarking resistant against tampering and copy attack // *Signal processing*. 2003. No 10. P. 2133–2170.

106. Wong P. A public key watermark for image verification and authentication // *Proc. IEEE ICIP*. 1998. Vol. 1.

107. Holliman M., Memon N. Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes // *IEEE Trans. on Image Processing*. Vol. 9, Issue 3, March 2000. P. 432–441.

108. Barreto P., Kim H., Rijmen V. Toward a secure public-key blockwise fragile authentication watermarking // Proc. IEEE ICIP. 2001. P. 494–497.
109. Boehme R. Statistical characterisation of MP3 encoders for steganalysis // ACM Multimedia and Security Workshop, 2004.
110. Vogel J. Illustration watermarking: An object based approach for digital images // Edward P., Delp J., editor, Security and watermarking of multimedia contents VI, Santa Clara, CA USA, 2005. SPIE.
111. Norcen R., Uhl A. Robust authentication of the JPEG-2000 bitstream // Proc. of NORSIG, 2004.
112. Norcen R., Uhl A. Robust visual hashing using JPEG-2000 // Eighth IFIP TC6/TC11 conference on communications and multimedia security, 2004.
113. Multimedia security technologies for digital rights management. Zeng W., Yu H., Lin C editors // Academic press, 2006.
114. Multimedia fingerprinting forensics for traitor tracing. Liu K., Trappe W., Wang Z., Wu M., Zhao H. // Hindawi Publishing Corporation, 2005.
115. Multimedia security: steganography and digital watermarking techniques for protection of intellectual property. Lu C. // Idea group publishing, 2004.
116. Watermarking systems engineering: enabling digital assets security and other applications. Barni M., Bartolini F. // Marcel Dekker, 2004.
117. Data Hiding fundamentals and applications. Sencar H., Ramkumar M., Akansu A. // ELSEVIER science&technology books, 2004.
118. Techniques and applications of digital watermarking and content protection. Arnold M., Wolthusen S., Schmucker M. // Artech house publishers, 2003.
119. Informed watermarking. Eggers J., Girod B. // Kluwer academic publishers, 2002.
120. Disappearing cryptography. Wayner P. // Morgan kaufmann publishers, 2002.
121. Fridrich J. Multi-class blind steganalysis for JPEG images // Proc. SPIE electronic imaging, Photonics west, January 2006
122. Fridrich J. Security of fragile authentication watermarks with localization // Security and watermarking of multimedia contents. Proc. SPIE. 2002. Vol. 4675. P. 691–700.
123. Campisi P., Kundur D., Hatzinakos D., Neri A. Compressive data hiding: An unconventional approach for improved color image coding // EURASIP journal on applied signal processing, 2002. Vol. 2002, № 2. P. 152–163.
124. Holliman M., Memon N. Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes // IEEE trans. on image processing. Vol. 9, Issue 3, March 2000. P. 432–441.
125. Boehme R. Statistical characterisation of MP3 encoders for steganalysis // ACM multimedia and security workshop, 2004.
126. Vogel J. Illustration watermarking: An object based approach for digital images // Edward P., Delp J., editor, Security and watermarking of multimedia contents VI, Santa Clara, CA USA, 2005. SPIE.

127. Norcen R., Uhl A. Robust authentication of the JPEG-2000 bitstream // Proc. of NORSIG, 2004.
128. Norcen R., Uhl A. Robust visual hashing using JPEG-2000 // Eighth IFIP TC6/TC11 Conference on communications and multimedia security, 2004.
129. Multimedia security technologies for digital rights management. Zeng W., Yu H., Lin C editors // Academic press, 2006.
130. Multimedia fingerprinting forensics for traitor tracing. Liu K., Trappe W., Wang Z., Wu M., Zhao H. // Hindawi publishing corporation, 2005.
131. Multimedia security: steganography and digital watermarking techniques for protection of intellectual property. Lu C. // Idea group publishing, 2004.
132. Watermarking systems engineering: enabling digital assets security and other applications. Barni M., Bartolini F. // Marcel Dekker, 2004.
133. Data hiding fundamentals and applications. Sencar H., Ramkumar M., Akansu A. // ELSEVIER science&technology books, 2004.
134. Techniques and Applications of digital watermarking and content protection. Arnold M., Wolthusen S., Schmucker M. // Artech house publishers, 2003.
135. Informed watermarking. Eggers J., Girod B. // Kluwer academic publishers, 2002.
136. Disappearing cryptography. Wayner P. // Morgan Kaufmann publishers, 2002.
137. Digital watermarking. Cox I., Miller M., Bloom J. // Morgan Kaufmann publishers, 2001.
138. Information hiding: steganography and watermarking – attacks and counter-measures. Neil F. Johnson, Zoran Duric, Sushil Jajodia Hardcover, Kluwer academic publishers, 2001.
139. Information hiding techniques for steganography and digital watermarking. Stefan Katzenbeisser, Fabien A. P. Petitcolas (Editors) // Artech house publishers, 1999.

Грибунин Вадим Геннадьевич, **Костюков** Валентин Ефимович,
Мартынов Александр Петрович, **Николаев** Дмитрий Борисович,
Фомченко Виктор Николаевич

***Стеганографические системы.
 Цифровые водяные знаки***

Учебно-методическое пособие

Редактор *Н. П. Мишкина*
 Компьютерная подготовка оригинала-макета
Н. В. Мишкина
 Дизайн обложки *Е. Л. Соседко*

Подписано в печать 28.10.2016. Формат 70×100/16
 Усл. печ. л. 17,0 Уч.-изд. л. ~16 Тираж 300 экз. Зак. тип. 44-2016

Отпечатано в ИПК ФГУП «РФЯЦ-ВНИИЭФ»
 607188, г. Саров Нижегородской обл., ул. Силкина, 23