

Ministerul Educației, Culturii și Cercetării al Republicii Moldova

Universitatea Tehnică a Moldovei

Programul de masterat „Securitatea informației în sisteme și rețele de comunicații”

Admis la susținere

Șef departament: conf., dr. inginer Pavel Nicolaev

„\_\_\_” \_\_\_\_\_ 2020

**CERCETAREA POSIBILITĂȚII  
IMPLEMENTĂRII STEGANOGRAFIEI CA METODĂ  
DE PROTECȚIE ASCUNSĂ A INFORMAȚIEI**

Teză de master

Masterand:  (Maxim Zaharov)

Conducător:  (Iurie Pușneac)

Chișinău – 2019

## CUPRINS:

INTRODUCERE.....	4
1. ANALIZA OBIECTULUI DE CERCETARE – STEGANOGRAFIEI .....	7
1.1. Istoria dezvoltării steganografiei .....	7
1.2. Noțiuni generale cu privire la steganografia în contextul asigurării protecției informației.....	11
2. ANALIZA MECANISMELOR DE FUNCȚIONARE ALE STEGANOGRAFIEI ÎN DIFERITE MEDIILE INFORMAȚIONALE .....	19
2.1. Examinarea principiilor de baza de funcționare ale steganografiei.....	19
2.2. Analiza modalității implementării steganografiei în text.....	28
2.3. Cercetarea posibilității implementării steganografiei în imagini.....	31
2.4. Investigația metodelor implementării steganografiei în fișiere audio.....	37
2.5. Studiarea mecanismelor de implementare ale steganografiei în fișiere video.....	39
3. IMPLEMENTAREA METODELOR, ALGORITMILOR ȘI MIJLOACELOR STEGANOGRAFICE .....	45
3.1. Cercetarea produselor soft, utilizate în steganografia.....	45
3.2. Implementarea metodelor, algoritmilor și mijloacelor steganografice în text.....	52
3.3. Implementarea metodelor, algoritmilor și mijloacelor steganografice în imagini.....	55
CONCLUZII.....	59
BIBLIOGRAFIE.....	66

## REZUMAT

la teza de master cu tema „*CERCETAREA POSIBILITĂȚII IMPLEMENTĂRII STEGANOGRAFIEI CA METODĂ DE PROTECȚIE ASCUNSĂ A INFORMAȚIEI*”, Chișinău, 2019,  
autorul Maxim Zaharov

**Structura tezei:** Teza cu tema „*Cercetarea posibilității implementării steganografiei ca metodă de protecție ascunsă a informației*” este constituită din introducere, trei capitole, concluzii și recomandări, bibliografie cu 90 titluri, 66 pagini.

**Cuvintele cheie:** steganografia; criptografia; protecția informației; informația ascunsă; metodele, algoritmele și mijloacele steganografice; container; marcarea transparentă; semnal digital; document digital; protecția dreptului de autor.

**Scopul și obiectivele lucrării.** În conformitate cu actualitatea și gradul de investigare a temei, ne propunem drept scop analiza posibilității implementării steganografiei ca metodă de protecție ascunsă a informației. În vederea realizării scopului propus, au fost formulate următoarele obiective:

- studierea principiilor de bază ale steganografiei;
- examinarea tehnologiilor steganografice în diferite medii informaționale;
- cercetarea produselor soft, folosite în steganografia;
- cercetarea metodelor, algoritmilor și mijloacelor steganografice;
- implementarea metodelor, algoritmilor și mijloacelor steganografice în text și imagini.

**Caracterul inovator** al investigației rezidă în faptul de a construi un tablou integrat a posibilității implementării steganografiei ca metodă de protecție ascunsă a informației. Pornind de la premisa importanței și necesității implementării steganografiei ca metodă de protecție ascunsă a informației realizarea acestui studiu prezintă o semnificație valorică multiplă:

- studiul dat poate servi drept izvor practicienilor în domeniu, care sintetizează principalele aspecte ale steganografiei ca metodă de protecție ascunsă a informației;

- concepțiile prezentate pot completa arsenalul factologic al cercetărilor în domeniu, oferind posibilitatea structurării domeniului implementării steganografiei ca metodă de protecție ascunsă a informației;

- relevând cele mai bune practici din domeniul steganografiei, autorul alege și propune soluții optime pentru implementarea steganografiei ca metodă de protecție ascunsă a informației.

## ANNOTATION

to the Master's thesis on topic "*RESEARCHING THE POSSIBILITY OF THE IMPLEMENTATION OF STEGANOGRAPHY AS A METHOD OF SECRET PROTECTION OF INFORMATION*", Chisinau, 2019, compiled by Maxim Zaharov

**Structure of the thesis:** Master's thesis on topic "*Researching of the possibility of implementation of steganography as a method of secret protection of information*" consists of introduction, three chapters, conclusions, references and bibliography with 90 headlines, 66 pages.

**Key words:** steganography; cryptography; information protection; secret information; steganographic methods, algorithms and tools; container; water marking; digital signal; digital document; copyright protection.

**Purpose and objectives.** In accordance with the actuality and degree of investigation of the topic, we aim to analyze the possibility of implementing steganography as a method of secret protection of information. In order to achieve the proposed purpose, the following objectives were:

- study of the basic principles of steganography;
- examination of steganographic technologies in different information environments;
- research of software products, used in stenography;
- research of steganographic methods, algorithms and means;
- implementation of steganographic methods, algorithms and tools in text and images.

**The innovative nature** of the investigation is in the fact of building a complete picture of the possibility of implementing steganography as a method of secret protection of information. Starting from the precondition of the importance and necessity of the implementation of steganography as a method of secret protection of information, the carrying out of this research provides a multiple value significance:

- this study may serve as a source for practitioners in the field, who summarise the main aspects of steganography as a method of secret protection of information;

- the provided concepts can complement all the facts of research in the field, offering the possibility to structure the field of implementation of steganography as a method of secret protection of information;

- *emphasising the best practices in the field of steganography, the author selects and proposes optimal solutions for the implementation of steganography as a method of secret protection of information.*

## INTRODUCERE

Cuvântul *Steganografie* vine din limba greacă unde *steganos* înseamnă ascuns și *graph* scris. Am putea spune că steganografia este știința de a scrie mesaje ascunse astfel încât existența lor să fie cunoscută numai de destinatar și expeditor.

În domeniul tehnologiilor informaționale, steganografia reprezintă metoda de a ascunde mesaje (fișiere) în alte fișiere mai mari și anume în imagini de tip jpg, bmp, în fișiere audio (mp3 sau wav) sau chiar video (avi) fără a exista posibilitatea de a afla de existența mesajelor.

Steganografia nu trebuie confundată cu criptografia. Acesta din urmă face ca un mesaj să devină indescifrabil, dar existența lui este vizibilă, pe când steganografia ascunde existența mesajului și nu mesajul.

Tot de steganografie este legat și conceptul de Watermarking și anume înglobarea informațiilor de copyright într-un fișier audio sau imagine astfel încât fișierul să conțină info despre autor și copyright fără ca cineva să știe despre existența lor și să le poată șterge/modifica. Mesajul este ascuns în interiorul fișierului acoperitor în "clar" astfel încât oricine bănuiește existența mesajului îl poate recupera. Majoritatea programelor de steganografie realizează comprimarea, criptarea și abia apoi ascunderea mesajului. Astfel folosind *strong cryptography*, atât existența mesajului este ascunsă cât și mesajul în sine. Steganografia și criptografia nu se exclud, fiecare are alt scop. Există momente când un mesaj criptat trezește suspiciune și atunci steganografia reprezintă soluția.

Există foarte mulți algoritmi de steganografie, foarte cunoscut fiind algoritmul care modifică LSB (*least significant bit*). Dacă vom schimba pentru fiecare *byte*, bitul cel mai puțin semnificativ al fiecărui pixel cu un bit care compune mesajul pe care vrem să-l ascundem, atunci efectul asupra fiecărui pixel este atât de mic încât imaginea modificată rămâne practic aproape identică cu originalul. În realitate ochiul uman nu poate sesiza vreo diferență între imaginea modificată (în care se ascunde mesajul) și cea originală. Interesant este că LSB este 1 sau 0, deci avem șanse de 50% ca nici măcar să nu fie nevoie să modificăm bitul cel mai puțin semnificativ. Același principiu se poate aplica și fișierelor audio (wav, mp3) sau video doar că în loc să se modifice pixeli se modifică frecvențele audio. Diferențele trec complet neobservate de urechea umană. Făcând un calcul simplu pentru fiecare 8 biți ai lui "*cover-file*", un bit este informația care compune mesajul ascuns, deci 12,5% din imagine reprezintă mesajul ascuns. Astfel într-un fișier jpg de 500KB putem ascunde un alt fișier de 62,5KB. În practică informația ascunsă reprezintă între 5% și maxim 10% din *cover-file*. Bineînțeles că există și contra-măsuri și atacuri

împotriva stenografiei. Steganaliza este știința care se ocupa cu spargerea algoritmilor de steganografie și descoperirea fișierelor care ascund alte mesaje secrete (la fel cum criptanaliza se ocupa cu spargerea algoritmilor de criptare).

**Actualitatea temei investigate.** Odată cu dezvoltarea și extinderea sferei de aplicare a instrumentelor de tehnologie informațională, problema protecției informațiilor în sistemele informatice devine acută din mai multe motive obiective. Astfel, cu trecerea timpului se face tot mai evidentă creșterea încrederii în sistemele informatice și tehnologiile informaționale. Acestea sunt însărcinate cu cele mai importante sarcini, de calitate cărora depinde viața și bunăstarea multor oameni. Sistemele informatice controlează procesele tehnologice din întreprinderi și sistemele energetice, mișcarea aeronavelor și a sateliților, realizează operațiuni financiar-bancare și procesează informații clasificate.

**Gradul de investigare a temei.** Studiind resursele informaționale, în Republica Moldova nu au fost identificate lucrări teoretice sau practice speciale, dedicate cercetării posibilității implementării steganografiei ca metodă de protecție ascunsă a informației.

**Scopul și obiectivele lucrării.** În conformitate cu actualitatea și gradul de investigare a temei, ne propunem drept scop cercetarea posibilității implementării steganografiei ca metodei de protecție ascunsă a informației în Republica Moldova.

În vederea realizării scopului propus au fost formulate următoarele obiective:

1. studierea principiilor de bază ale steganografiei;
2. examinarea tehnologiilor steganografice în diferite mediile informaționale;
3. cercetarea produselor soft, folosite în steganografia;
4. cercetarea metodelor, algoritmilor și mijloacelor steganografice;
5. implementarea metodelor, algoritmilor și mijloacelor steganografice în text și imagini.

**Semnificația teoretică și valoarea aplicativă a lucrării.** **Semnificația** epistemică și pragmatică a cercetării derivă din concluziile obținute, ca urmare, a cercetării posibilității implementării steganografiei ca metoda de protecție ascunsă a informației. **Caracterul inovator** al cercetării rezidă în faptul de a construi un tablou integru al steganografiei ca metoda de protecție ascunsă a informației. Pornind de la premisele necesității implementării steganografiei în scopul protecției informației, realizarea acestui studiu prezintă o semnificație valorică multiplă:

- studiul dat poate servi practicienilor în domeniu ca un izvor ce sintetizează principalele aspecte de protecție a informației cu ajutorul steganografiei;

- concepțiile prezentate pot completa arsenalul factologic al cercetărilor în domeniu, oferind posibilitatea structurării metodelor steganografice;

- determina rolul și gradul de importanță a steganografiei în domeniul protecției informației, autorul identifică avantajele, cât și dezavantajele utilizării steganografiei ca metoda de protecție a informației;

- prezenta lucrarea poate servi drept suport informațional pentru studenții ciclului I (licența) sau II (masterat) pe tematica protecției informațiilor în sistemele și rețelele informaționale;

- releva cele mai bune practici și soluții în domeniul steganografiei, autorul propune soluții de implementare a steganografiei ca metoda de protecție ascunsă a informației.

## BIBLIOGRAFIE

### ACTE NORMATIVE NAȚIONALE

1. Constituția Republicii Moldova: adoptată la 29 iulie 1994. *Monitorul Oficial al Republicii Moldova*. 1994, nr. 1.
2. Legea cu privire la informatizare și la resursele informaționale de stat: nr.467 din 21.11.2003. *Monitorul Oficial al Republicii Moldova*. 2004, nr. 6-12.
3. Legea **privind semnătura electronică și documentul electronic**: nr.91 din 29.05.2014 *Monitorul Oficial al Republicii Moldova*. 2014, nr. 174-177;.
4. Legea cu privire la informatică: nr.1069 din 22.06.2001. *Monitorul Oficial al Republicii Moldova*. 2001, nr.73-74.

### MANUALE, MONOGRAFII, LUCRĂRI DIDACTICE, BROȘURI

5. Dumitrescu M., Curs de Statistică Matematică, Editura Universității București, 1989.
6. Naccache D., Simion E., Mihăiță, Olimid R.F., Oprina A.G., Criptografie și Securitatea informației. Aplicații, Matrixrom 2011.
7. Preda V., Teoria Deciziilor Statistice, Ed. Academiei, 1991.
8. Simion E., Opreșan Ghe., Elemente de Cercetări Operaționale și Criptologie, Ed. Politehnica Press, 2003.
9. Simion E., Andrașiu M., Naccache D., Simion Gh., Cercetări operaționale, Probabilități și Criptologie. Aplicații, Academia Tehnică Militară, 2011.
10. Voicu I., Inserarea Mesajelor Secret Digitale în Imagini și Secvențe Video, Ed. Medro, 2000.
11. Gorobievski S. Tehnici, instrumente și metode de comunicare managerială și utilizarea lor în cadrul firmelor contemporane.// În: Managementul industrial. Coord.: A.Cojuhari, dr.hab., prof.univ.; V. Mămăliga, dr. econ., conf. univ. Chișinău: UTM, 2017.
12. Mihai Ioan-Cosmin; „Securitatea sistemului informatic”, Galați, Ed. Dunărea de Jos, 2007.
13. Atanasiu A. - Teoria codurilor corectoare de erori, Editura Univ. București, 2001.
14. Oprea, D. – Analiza și proiectarea sistemelor informaționale economice, Editura Polirom, Iași, 1999.
15. Oprea, D. – Managementul proiectelor: teorie și cazuri practice, Editura Sedcom Libris, Iași, 2001.



16. Oprea, D., Airinei, D., Fotache, M. (coord.) – Sisteme informaționale pentru afaceri, Editura Polirom, Iași, 2002.
17. Oprea, D., Meșniță, G. – Sisteme informaționale pentru manageri, Editura Polirom, Iași, 2002.
18. Patriciu, V.V., Pietroșanu-Ene, M., Bica, I., Cristea, C. – Securitatea informatică în Unix și Internet, Editura Tehnică, București, 1998.
19. Zgureanu Aureliu, Metode criptografice, de protecție a informației, Note de curs, Chișinău 2014, Tipografia Centrului Editorial-Poligrafic al ASEM.
20. Zgureanu Aureliu, Bazele securității informației, 2018, Tipografia Centrului Editorial-Poligrafic al ASEM.
21. Salomaa, Arto, Criptografie cu chei publice, Editura Militara, Bucuresti, 1993.
22. Аграновский А. В., Хади Р. А., Практическая криптография, алгоритмы и их программирование, Москва, 2009.
23. Мао В., Современная криптография (теория и практика), М.: Вильямс, 2005.
24. Шнайер Б., Секреты и ложь. Безопасность данных в цифровом мире, Москва, 2003.
25. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.: Книжный мир, 2009. — 352 с.
26. Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property, by Lu, Chun-Shien, Publication: Hershey : Idea Group Publishing, 2005.
27. Hiding in Plain Sight: Steganography and the Art of Covert Communication, by Cole, Eric, Publication: Indianapolis, IN John Wiley & Sons, Inc. (US), 2003.
28. Information Hiding Techniques for Steganography and Digital Watermarking Artech House Computer Security Series, by Katzenbeisser, Stefan.; Petitcolas, Fabien A. P., Publication: Boston Artech House, Inc., 2000.
29. Coding for Data and Computer Communications, by Salomon, D., Publication: New York, NY Springer Science & Business Media, 2005.
30. Techniques and Applications of Digital Watermarking and Content Protection Artech House Computer Security Series, by Arnold, Michael.; Schmucker, Martin.; Wolthusen, Stephen D., Publication: Boston Artech House, Inc., 2003.
31. Devours C., Kahn D., Kruh L., Mellen G., Winkel B., Cryptology: Machines, history and Methods, Artech House, 1989
32. Devours C., Kruh L., Machine Cryptography and Modern Cryptanalysis, Artech House, 1985
33. Diffie W. and Hellman M. E., New Directions in Cryptography. IEEE Transactions on Information Theory, vol. IT-22, Nov. 1976, pp. 644–654

34. El Gamal T., A Public Key Cryptosystem and Signature Scheme Based on Discrete Logarithms, *IEEE Transactions in Information Theory* 31 (4), 1985, pp. 469–472
35. Ferguson N. and Schneir B., *Practical Cryptography*, Wiley N. Y. (2003)
36. Friedman W. F., *Military Cryptanalysis – Part I, Monoalphabetic Substitution Systems*, United States Government Printing Office, Washington, 1939
37. Friedman W. F., *Military Cryptanalysis – Part II: Simpler Varieties of Polyalphabetic Substitution Systems*, United States Government Printing Office, Washington, 1938
38. Kahn D., *The Codebreakers - The Story of Secret Writing*, abridget ed. New York, NY: Signet, 1973
39. Rivest R. L., Shamir A., Adleman L., A method for obtaining digital signatures and public key cryptosystems, *Comm ACM* 21, 1978, pp. 120–126
40. Rivest R. L., The RC5 encryption algorithm, In: *Fast software encryption–Leuven 1994. LNCS*, vol. 1008. Berlin: Springer; 1995, pp. 86–96
41. Rueppel R. A., Stream ciphers, In: G. J. Simmons, Editor, *Contemporary Cryptology–The Science of Information Integrity*, IEEE Press, New York, 1992, pp. 65–134.
42. Nematollahi, M. A., Vorakulpipat, C., & Rosales, H. G. (2016). *Digital Watermarking: Techniques and Trends* (Vol. 11). Springer.
43. Sadek, M. M., Khalifa, A. S., & Mostafa, M. G. (2015). Video steganography: a comprehensive review. *Multimedia tools and applications*, 74(17), 7063-7094.
44. Hartung, F., and B. Girod. 1998. Watermarking of uncompressed and compressed video. *Signal Processing* 66(3): 283–301.
45. Paul, R. T. (2011). Review of robust video watermarking techniques. *IJCA Special Issue on Computational Science*, 3, 90-95.
46. Isac, B., & Santhi, V. (2011). A study on digital image and video watermarking schemes using neural networks. *International Journal of Computer Applications*, 12(9), 1-6.
47. Liu, Y., & Zhou, P. (2014, January). A survey of Video Watermarking based on Motion Vector. *În 2014 International Conference on Computer, Communications and Information Technology (CCIT 2014)*. Atlantis Press.

#### PUBLICAȚIILE ÎN MATERIALELE CONFERINȚELOR, SIMPOZIOANELOR

48. Popescu A., Transformata Walsh-Hadamard în Criptografie, Sesiunea de Comunicări Științifice a Universității Hyperon, 2004.

49. Zgureanu Aureliu, dr., conf. Univ., Aspectul organizatoric de asigurare a securității informaționale, Culegere de articole selective ale Conferinței Științifice Internaționale „Competitivitatea și Inovarea în Economia Cunoașterii”, 22-23 septembrie 2017, Chișinău, Vol. V.
50. Colun Tatiana, drd, Școala Doctorală Economie, Finanțe și Management, UTM, 6<sup>th</sup> International Conference “Telecommunications, Electronics and Informatics” ICTEI 2018, Chisinau, 24—27 May 2018. - Securitatea sistemelor informatice - pilon de bază al siguranței informaționale.
51. Doinea, M. și Dumitrescu, F. 2014. Tehnici de securitate pe baza de ontologii în sistemele de biblioteci virtuale, Workshopul Colecțiile de patrimoniu în era digitală, 24-25 noiembrie 2014.
52. Nadejda Scripnic, Olga Cerbu – Utilizarea instrumentelor de securizare a informației/ Materiale ale conferinței științifico-practice cu participare internațională 23 mai 2014, Academia de Administrare Publică, Chișinău.
53. Pavel Macari – Securitatea și siguranța informației în sectorul public/ Materiale ale Conferinței științifico-practice cu participare internațională 22 mai 2012, Academia de Administrare Publică, Chișinău.
54. Nadejda Vacarov – Transparența și securitatea informației/ Administrația publică în statul de drept/ Institutul de Științe administrative din Rep. Moldova, Sesiune de comunicări științifice, 27-28 sept. 2008.
55. Nicolae Chirpat, Olga Cerbu – Metode de utilizare a instrumentelor de securitate a informației, Materiale ale conferinței științifico-practice cu participare internațională, 20 mai 2013, Chișinău.
56. Nicoleta Duca, Rodica Bulai – Optimizarea sistemelor de securitate informațională utilizând teoria probabilităților/ Conferința Tehnico-Științifică a Colaboratorilor, Doctoranzilor și Studenților, 15-17 noiembrie 2012. Vol. 1.

#### ARTICOLE DIN EDIȚII PERIODICE

57. Doinea, M., Securitatea sistemelor de biblioteci virtuale în contextul colaborativ al spațiului european, Revista Română de Informatică și Automatică, 2015, 25(3), pp. 37-42.
58. Oprea, D. – „Particularități ale securității sistemelor informatice bazate pe partajarea resurselor”, în Tribuna Economică, 13, 1995.28.
59. Oprea, D. – „Vulnerabilitatea securității sistemelor bazate pe microcalculatoare”, în Tribuna Economică, 15, 1995.
60. Oprea, D. – „Pericole ce vizează sistemele informatice”, în Tribuna Economică, 16, 1995.
61. Oprea, D. – „Protecția fizică a sistemelor informatice”, I-IV, în Tribuna Economică, 39-42, 1995.
62. Oprea, D. – „Securitatea comunicațiilor”, I-II, în Tribuna Economică, 40, 43, 1996.

63. Tank RM, Vasava HD, Agrawal V. DNA-based audio steganography. *Oriental Journal of Computer Science and Technology*. 2015;8(1):43-48.
64. Anderson RJ, Petitcolas FAP. On the limits of the steganography. *IEEE Journal of Selected Areas in Communications*. 1998;16(4):474-481.
65. Artz D. Digital steganography: Hiding data within data. *IEEE Internet Computing Archive*. 2001;5(3):75-80.
66. Vitaliev D. *Digital Security and Privacy for Human Rights Defenders*. Dublin: The International Foundation for Human Right Defenders; 2007. pp. 77-81.
67. Sharma S, Yadav VK, Trivedi MC, Gupta A. Audio steganography using ZDT: Encryption using indexed based chaotic sequence. In: *ICTCS '16 Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies*, Article No. 66 , Udaipur, India — March 04–05, 2016.
68. Xiang S, Kim JH, Huang J. Audio watermarking robust against time-scale modification and MP3 compression. *Signal Processing*. 2008;88(10):2372-2387.
69. Mansour M, Tewfik A. Data embedding in audio using time-scale modification. *IEEE Transactions on Speech and Audio Processing*. 2005;13(3):432-440.
70. Fallahpour M, Megías D. High capacity audio watermarking using fft amplitude interpolation. *IEICE Electronics Express*. 2009;6:1057-1063.

#### RESURSE ELECTRONICE

71. [http://www.rasfoiesc.com/educatie/informatica/STEGANOGRAFIA42.php#\\_ftnref1](http://www.rasfoiesc.com/educatie/informatica/STEGANOGRAFIA42.php#_ftnref1).
72. <http://www.worldit.info/articole/solutie-steganografie-care-este-diferenta-dintre-cele-doua-imagini/>.
73. <http://itransfer.space/marcarea-digitala-a-fisierelor-video/>.
74. <http://www.jjtc.com/Security/stegtools.htm>.
75. <https://delightfullylinux.wordpress.com/2016/12/14/hide-text-in-text-files-using-stegsnow/>.
76. <https://www.ukessays.com/essays/information-technology/examining-the-importance-of-steganography-information-technology-essay.php>.
77. <https://en.wikipedia.org/wiki/Steganography>.
78. <https://en.wikipedia.org/wiki/Steganographia>.
79. <https://www.geeksforgeeks.org/image-steganography-in-cryptography/>.
80. <https://securelist.com/steganography-in-contemporary-cyberattacks/79276/>.
81. <https://www.edureka.co/blog/steganography-tutorial>.
82. <https://www.scss.tcd.ie/~munnellg/projects/steganography.html>.

83. <http://dbpedia.org/page/Steganography>.
84. <https://itnext.io/steganography-101-lsb-introduction-with-python-4c4803e08041>.
85. <https://www.carbonblack.com/2019/04/09/steganography-in-the-modern-attack-landscape/>.
86. <https://towardsdatascience.com/steganography-hiding-an-image-inside-another-77ca66b2acb1>.
87. <https://www.researchgate.net/publication/49587597> Steganography A Data Hiding Technique.
88. <https://folk.uio.no/jeanra/Informatics/AfewWordsSteganography.html>.
89. <http://www.crypto-it.net/eng/theory/steganography.html>.
90. <https://www.pandasecurity.com/mediacenter/interviews/daniel-lerch-steganography/>.