به نام خداوند بخشنده مهربان

نهان نگاری در رایانامه با ظرفیت نامحدود از طریق لغت نامه

اعضای گروه: فرخنده ارضی، نازنین آریان متین

استاد مربوطه: دکتر منصور فاتح

دانشگاه صنعتی شاهرود

اسفند ۱۴۰۱

مقدمه

روش های موجود برای مخفی سازی اطلاعات

مشکلات اساسی روش های رمزنگاری

جنبه های نهان نگاری

بستر های نهان نگاری

نهان نگاری در بستر رایانامه

مرور کارهای پیشین

روش های نهان نگاری

زبانی، ساختاری، تصادفی-آماری،

استفاده از پیام های کوتاه در پوشانه و مخفی سازی اطلاعات در شکلک ها، استفاده از سند های اینترنتی به عنوان متن پوشانه و مخفی سازی اطلاعات در صفت ها، خلاصه سازی متن، نهان نگاری در فایل های html بر بستر وب، مخفی سازی متن در شبکه های اجتماعی، مخفیسازی اطالعات تشخیص هویت درون دنباله DNA

نهان نگاری در رایانامه با تکرار نویسه ها

روش پیشنهادی

- مفاهیم اولیه و فرضیات
- جاسازی پیام
- استخراج پیام
- تحلیل امنیتی

مفاهیم اولیه و فرضیات

شمای پیشنهادی مبتنی بر یک لغت نامه است. این لغت نامه شامل ۶۹۸۸۸ کلمه پرتکرار در زبان انگلیسی است که در آن کلمات بر حسب میزان تکرار آنها در ادبیات انگلیسی مرتب شده اند. به کلمات با تکرار بیشتر یک اندیس کمتر و به کلمات با تکرار کمتر یک اندیس بیشتر در لغتنامه اختصاص داده شده است.

مقادیر مشترک بین گیرنده و فرستنده:

$x`$, بیشینه تعداد دفعات خواندن رایانامه

$y`$, بیشینه تعداد جملات از بدنه رایانامه

$z`$: بیشینه تعداد نویسه های بدنه رایانامه

و کلید A و مجموعه S

ردیف	پسوند نشانی رایانامه	کد ۳ بیتی
۱	gmail.com	**000**
۲	hotmail.com	**001**
۳	yahoo.com	**010**
۴	rediffmail.com	**011**
۵	btinternet.com	**100**
۶	aol.com	**101**
۷	msn.com	**110**
۸	verizon.net	**111**

تحلیل امنیتی

رعایت مهم ترین پارامتر های امنتی در نهان نگاری مثل عدم تشخیص توسط چشم انسان، عدم تشخیص توسط روشهای آماری و ظرفیت نهان نگاری

کاهش تعداد نویسه های متن پوشانه مطلوب نیست.

نتایج ارزیابی

محیط ارزیابی

ظرفیت نهان نگاری

تعداد نشانی های رایانامه تولید شده

محیط ارزیابی

کارایی روش نهان نگاری پیشنهادی با کمک دو پارامتر ظرفیت و تعداد نشانی های رایانامه تولیدشده مورد ارزیابی قرار میگیرد.

Capacity = Nm / Nc 10

Nm: تعداد بیت های پیام Nc: تعداد بیت های متن پوشانه

ظرفیت نهان نگاری

"in the research area of text steganography, algorithms based on font format have advantages of great capacity, good imperceptibility and wide application range. However, little work on steganalysis for such algorithms has been reported in the literature. based on the fact that the statistic features of font format will be changed after using font-format-based steganographic algorithms, we present a novel support vector machine-based steganalysis algorithm to detect whether hidden information exists or not. this algorithm can not only effectively detect the existence of hidden information, but also estimate the hidden information length according to variations of font attribute value. as shown by experimental results, the detection accuracy of our algorithm reaches as high as 99.3% when the hidden information length is at least 16 bits."

(شکل-۳): متن ارسالی (پوشانه) مورد استفاده در مرجع [18].

(Figure-3): Cover text used in [18].

"behind using a cover text is to hide the presence of secret messages the presence of embedded messages in the resulting stego text cannot be easily discovered by anyone except the intended recipient"

(شکل-۴): پیام مخفی مورد استفاده در مرجع [18].

(Figure-4): Secret message used in [18].

(جدول-۵): ظرفیت روش‌های مختلف نهان‌نگاری در متن.

(Table-5): Capacity of different text-steganography approaches.

مرجع	ظرفیت
[1]	**7.017**
[3]	**6.92**
[6]	**7.03**
[20]	**7.21**
[28]	**نامحدود**
روش پیشنهادی	**نامحدود**

تعداد نشانی های رایانامه تولید شده

(جدول-۶): تعداد نشانی رایانامه‌های ساخته‌شده به‌ازای پیغام شکل (۵) و پوشانه شکل (۶).

(Table-6): Number of email addresses generated for the secret message and cover text shown in Figure 5 and Figure 6, respectively.

مرجع	تعداد نشانی‌های رایانامه
[28]	10
روش پیشنهادی	7

(جدول-۷): تعداد بیت‌های پیام بعد از فشرده‌سازی برای روش‌های با ظرفیت نامحدود.

(Table-7): Number of bits after compressions for two methods providing unlimited capacity.

مرجع	تعداد بیت‌های پیام بعد از فشرده‌سازی
[28]	150
روش پیشنهادی	104

10010 00111 00000 00111 10001 01110 01110
00011 10100 01101 01000 10101 00100 10001
10010 01000 10011 11000 01110 00101 10011

00100 00010 00111 01101 01110 01011 01110
00110 11000

(الف) دودویی پیام مخفی با روش LZW.

A) Binary form of the secret message compressed by LZW.

11 1000 1010011 1101000 1100001 1101000
1110010 1101111 1101111 1100100 01
111000110011 00 00011100 10
1111100001110000

(ب) دودویی پیام مخفی به‌کمک لغت‌نامه.

B) Binary form of the secret message compressed by Dictionary.

(شکل-۷): نتایج فشرده‌سازی متن مخفی شکل (۵) با کمک روش LZW و لغت‌نامه.

(Figure-7): Compression results of the LZW and Dictionary algorithms over the secret message shown in Figure 5.

نتیجه گیری

روش پیشنهادی محدود به زبان و نوع متن پوشانه خاص نیست و با هر متن پوشانه ای میتوان نهان نگاری را انجام داد.

فشرده کردن متن پیام مخفی به کمک لغت نامه -> تبدیل به رشته بیت -> شکسته شدن رشته بیت -> تولید نشانی های رایانامه با توجه به عدد دهدهی هر بخش و تعداد نویسه های موجود در متن پوشانه -> ارسال متن پوشانه همزمان به گیرنده و تمام نشانیهای رایانامه

عدم تغییر متن پوشانه -> عدم تشخیص توسط چشم انسان

ارسال همزمان رایانامه به چندین نشانی تولیدشده -> مشخص نبودن گیرنده پیام

ارائه ظرفیت نامحدود برای نهان نگاری

منابع

1 [M. Taleby Ahvanooey, Q. Li, J. Hou, AR. Rajput, C. Yini, “Modern Text Hiding, Text Steganalysis, and Applications: A Comparative Analysis,” Entropy, 2019 Apr; 21(4):355.]

2 [M. Taleby Ahvanooey, Q. Li, HJ. Shim, Y. Huang, “A comparative analysis of information hiding techniques for copyright protection of text documents,” Security and Communication Networks, 2018.]

3 [B. Gupta Banik, SK. Bandyopadhyay, “Novel Text Steganography Using Natural Language Processing and Part -of-Speech Tagging”, IETE Journal of Research, vo. 13, pp. 1 -2, 2018.]

4 [NS. Kamaruddin, A. Kamsin, LY. Por, H. Rahman, “A Review of Text Watermarking: Theory, Methods, and Applications,” IEEE Access, vol. 6:80, pp. 11 -28, 2018.]

5 [M. Taleby Ahvanooey, H. Dana Mazraeh, SH. Tabasi, “An innovative technique for web text watermarking (AITW),” Information Security Journal: A Global Perspective, 1;25(4 -6):191 -6. 2016.]

6 [SG. Rizzo, F. Bertini, D. Montesi, C. Stomeo, “Text watermarking in social media,“ In Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2017, 2017, vol. 31, pp. 208 -211, ACM.]

7 [MS. Rahman, I. Khalil, X. Yi, “A lossless DNA data hiding approach for data authenticity in mobile cloud based healthcare systems,” International Journal of Information Manage - ment, vol. 1, no. 45, pp. 276 -88, 2019.]

8 [E. Satir and H. Isik, “A Huffman compression based text steganography method,” Multimedia tools and applications, vol. 70, no. 3, pp. 2085 - 2110, 2014.]

9 [C.C. Chang, “A reversible data hiding scheme using complementary embedding strategy,” Information Sciences, vol. 180, no. 16, pp. 3045 -3058, 2010.]

10 [E. Satirand H. Isik. “A compression -based text steganography method,” Journal of Systems and Software, vol. 85, no. 10, pp. 2385 -2394, 2012.]

11 [S. Bhattacharyya, P. Indu, and G.Sanyal, “Hiding Data in Text using ASCII Mapping Technology (AMT),” International Journal of Computer Applications, vol. 70, no. 18, 2013.]

12 [R. Kumar, A. Malik, S. Singh, B. Kumar, and S. Chand, “A space based reversible high capacity text steganography scheme using font type and style,” In International Conference on Computing, Communication and Auto - mation (ICCCA), pp. 1090 -1094, 2016.]

13 [S.A. Al -Asadi and W.Bhaya, “Text Steganography in Excel Documents Using Color and Type of Fonts,” Research Journal of Applied Sciences, vol. 11, no. 10, pp. 1054 - 1059, 2016.]

14 [S. Roy and M.Manasmita, “A novel approach to format based text steganography,” In Proceedings of the 2011 International Conference on Communication, Computing & Security, pp. 511 -516, 2011.]

15 [B.K. Ramakrishnan, P.K.Thandra, and A.V. Srinivasula, “Text steganography: a novel character -level embedding algorithm using font attribute,” Security and Communication Networks, vol. 9, no. 18, pp. 6066 -6079, 2016.]

16 [A.M. Hamdan and A.Hamarsheh, “AH4S: an algorithm of text in text steganography using the structure of omega network,” Security and Communication Networks, vol. 9, no. 18, pp.6004 -6016, 2016.]

17 [M. Shirali -Shahreza, “Text steganography by changing words spelling,” In Advanced Communication Technology, 10th Inter - national Conference on, vol. 3, pp. 1912 -1913, 2008.]

18 [J. Gardiner, “StegChat: A Synonym - Substitution Based Algorithm for Text Steganography,” PhD Thesis, School of Computer Science University of Birmingham, pp. 1 -64, 2012.]

19 [C.Y. Chang and S. Clark, “Linguistic steganography using automatically generated paraphrases,” In Human Language Technologies: The 2010 Annual Conference of the North American Chapter of the Association for Computational Linguistics, pp. 591 -599, 2010.]

20 [T.P. Nagarhalli, “A New Approach to SMS Text Steganography using Emoticons,” In International Journal of Computer Appli - cations (0975 -8887), National Conference on Role of Engineers in Nation Building (NCRENB -14), pp. 1 -3, 2014.]

21 [M. Garg, “A novel text steganography technique based on html documents,” International Journal of Advanced Science and Technology, vol. 35, pp. 129 -138, 2011.

22 [A. Majumder and S. Changder, “A novel approach for text steganography: Generating text summary using Reflection Symmetry,” Procedia Technology, vol. 10, pp. 112 -120, 2013.]

23 [L.Y. Por, K. Wong, and K.O. Chee, “UniSpaCh: A text -based data hiding method using Unicode space characters,” Journal of Systems and Software, vol. 85, no. 5, pp. 1075 -1082, 2012.]

24 [R. Kumar, S. Chand, and S. Singh, “An Email based high capacity text steganography scheme using combinatorial compression,” In Confluence The Next Generation Information Technology Summit (Confluence), 5th International Conference, pp. 336 -339, 2014.]

25 [A. Malik, G. Sikka, and H.K. Verma, “A high capacity text steganography scheme based on LZW compression and color coding,” Engineering Science and Technology, an International Journal, vol. 20, no. 1, pp.72 - 79, 2016.]

26 [R. Kumar, A. Malik, S. Singh, and S. Chand, “A high capacity email based text steganography scheme using Huffman compression,” In Signal Processing and Integrated Networks (SPIN), 3rd International Conference on Signal Processing and Integrated Networks (SPIN), pp. 53 -56, 2016.]

27 [T. Ahmad, M.S. Marbun, H. Studiawan, W. Wibisono, and R.M.Ijtihadie, “A Novel Random Email -Based Steganography,” International Journal of e -Education, e - Business, e -Management and e -Learning, vol. 4, no. 2, pp. 129 -134, 2014.]

28 [M. Fateh, M. Rezvani, “An email -based high capacity text steganography using repeating characters,” International Journal of Computers and Applications, pp. 1 -7, 2018.]29 [Chang CY, Clark S. “Practical linguistic steganography using contextual synonym substitution and a novel vertex coding method,“ Computational linguistics, vol, 40, no. 2, pp. 403 -48, 2014

سپاس از توجهتون