STEGANOGRAPHIC APPROACH BASED ON COMPUTER GAME

Krasimir M. Kordov, Daniel E. Yordanov

ABSTRACT: *In this paper we present untraditional steganographic approach for hiding secret information in one of the most famous classical game. Using a game as stegocontainer defines different method for steganography considering the game structure and different method for using steganographic key. Further more the visual steganographic analysis is provided to demonstrate the necessary level of security of the proposed steganographic method.*

KEYWORDS: *Steganography, Steganographic approach, Computer game*

СТЕГАНОГРАФСКИ ПОДХОД, БАЗИРАН НА КОМПЮТЪРНА ИГРА*

Красимир М. Кордов, Даниел Е. Йорданов

1 Въведение в стеганографията

Стеганологията е научно направление, което се състои от две подразделения - Стеганография и Стегоанализ (Стеганализ или Стеганографски анализ) [2, 3, 7, 16, 22]. Стеганографията има за цел разработването на методи, модели и алгоритми за скриване на тайна информация, докато стегоанализът има за цел разкриването на приложена стеганография [23]. Разкриването на самата скрита информация не е обект на стеганализа, но се счита, че стеганографският подход е неуспешен, ако стеганализът отчете наличие на скрита информация [5, 6, 21].

В миналото, информацията [1] се е пренасяла основно под формата на текст, а стеганографията се използва, за да се скрие текст по такъв начин, че единствено очаквания получател да знае за съществуването на скрит текст [4]. В днешни дни, компютърните технологии позволяват пренос на информация, базирана на цифрови и аналогови сигнали, като преносимата информация е многообразна – текст, изображения, аудио, видео и дори игри. В компютърните системи информацията се съхранява и предава в двоичен код и по тази причина съвременната стеганография е фокусирана върху алгоритми скриващи информация в дигитален вид [7].

Стеганографската система е множество от елементи, взаимодействащи помежду си, всяко от които оказва влияние на скритото съобщение (информация), но в последствие съобщението трябва да достигне до желания получател в оригиналният си вид. Частите на системата се наричат подсистеми и всякакви промени в тях могат да доведат до провал на стеганографията [2]. С развитието на високо технологичната стеганография [4] се наблюдава използването на криптографски способи за предаване на секретен ключ между участниците в кореспонденцията или за хаотично скриване на тайната информация. Подобни алгоритми са разгледани в [13, 19] като за целта са използвани псевдослучайни генератори на двоични числа [11, 12, 17, 18].

*Настоящата статия е частично финансирана от фонд „Научни изследвания” на Шуменски Университет „Епископ К. Преславски” по проект № РД-08-122/06.02.2018.

2 Индустрия на компютърните игри

Компютърните игри са се обособили като глобална развлекателна индустрия, популярна за хора от всички възрастови групи. Съвременното информационно общество има достъп до игри на различни платформи (смартфони, таблети, персонални компютри, игрови конзоли и др.). Развитието на компютърните технологии води до развитие и популяризиране на игри от различни категории и жанрове, като някой от най-популярните игри се използват от милиони потребители по целия свят. Огромни количества от информация се пренася на сървъри до потребители на игри (и обратно) по целия свят и потока от данни който се предава непрекъснато е огромен [14, 15]. Това създава условия за използване на стеганографско предаване на тайна информация.

Бурното развитие на компютърните игри води своето начало през 60-те години на миналият век [10, 20]. Въпреки предназначението на компютъра за изчислителни процеси, графичното представяне на информация дава възможност да се измислят игри. Това от своя страна води до производство на специализирани хардуерни конфигурации, наречени игрови конзоли (или само конзоли), предназначени изцяло за игри. За първата компютърна конзола може да се приеме машината PDP-1 (Фигура 1 - а)), на която през 1962 година е създадена играта Spacewars, която се счита за първата компютърна игра [20]. По-късно през 1972 година се появяват аркадните игри. Използвали са се специални машини (Фигура 1 - б)), широко разпространени в барове и други заведения по цял свят. Една от най-популярните игри по това време е била Pong [20]. След нейното преиздаване за домашни конзоли, те се превръща в една от първите игри „първо поколение видео игри“. Второто поколение се играе на конзоли, които позволявали да се играе повече от една видео игра.

а) PDP-1

б) Аркадна конзола

Фигура 1: Първите компютърни конзоли.

През 1983 започва т. нар. сребърна епоха на видео игрите. По това време двамата гиганти в гейм индустрията са Nintendo[24] и Sega[25]. В наши дни мястото на Nintendo и Sega е заето от PlayStation[27] и Xbox[26], които продължават войната на конзолите. Борбата за потребители води до непрекъснати подобрения в качеството на игрите и генерира огромни приходи на производителите на конзоли и игри.

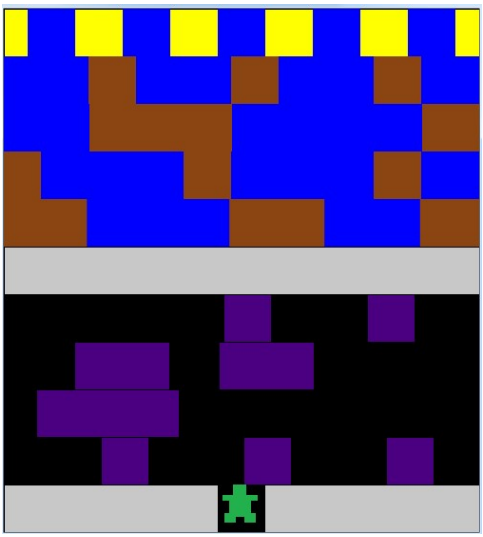
Индустрията на компютърни игри води до надпревара сред производителите на хардуер, но също така и до надпревара между производителите на игри. Съществуват компютърни компании, с хиляди специалисти, работещи изцяло върху създаването на нови игри, купува-

ни от милиони потребители по цял свят. Едни от най-известните производители на игри са Bethesda[28], Ubisoft[29], Rockstar games[30], CD Project RED[31] и други.

3 Стеганографски подход, базиран на компютърна игра

Преди идеята за скриване на информация в игри, създателите на игри са допускали грешки в разработката на своите продукти, което довежда до множество неочаквани резултати – гличове (glitches). Но не всички грешки имали лоши последици, защото някои играчи били заинтригувани и с интерес търсели други подобни необичайни елементи в игрите [8, 9]. Програмистите се възползват от това неочаквано постижение и започват да добавят скрито съдържание във своите игри, а ако има гличове, които се харесват от играчите, то тези „грешки“ не биват премахвани. Това и до ден днешен се харесва на играчите по цял свят и повишава интереса към компютърните игри. Тази практика се е превърнала в практика за предаване на тайна информация от производителите на игри към играчите, като дори се използват за рекламни послания за продукти от ежедневието в реалния свят [9].

В нашият случай, предаването на скрита информация е предназначено от един потребител до друг, като за целта е използвана собствена реализация на една от класическите аркадни игри - Frogger. Тази игра от златната епоха на видео игрите е популярна и в наши дни и по тази причина има много разновидности. Реализацията която предлагаме е направена на Java и изглежда по следният начин.



Фигура 2: Реализация на играта Frogger

3.1 Скрита функционалност на играта

Реализираната игра е опростена, с цел да се наблегне на стеганографският модел, вграден в играта. Няма нива на сложност, промяна на скоростта или допълнителни графични промени. Скритата функционалност на играта дава възможности на потребителите да обменят скрита информация, при активиране на скритата функционалност. Трябва да се изпълнят следните действия:

Стъпка 1: При натискане на конкретен бутон от клавиатурата (в нашият случай „C”) се включва режим за стеганография, като може да бъде изключен по същия начин. Реална

индикация не се визуализира с цел запазване на потайността на скритата функционалност.

Стъпка 2: Прави се избор за кодиране или декодиране на информация, като се позиционира игровия обект (frog) съответно в долният-ляв или долният-десен край на екрана.

Стъпка 3: За изпълнение на кодиране или декодиране трябва да се въведе правилен ключ. В нашият случай, това означава да се изиграе играта по точно определен начин.

Стъпка 4: След проверка на въведения ключ, в диалогов прозорец, на потребителя се предоставя възможност да въведе тайно съобщение (при режим на кодиране) или се показва тайното съобщение (при режим на декодиране).

3.2 Методи за скриване на информация

Реализацията на игра, позволява изпробването на различни методи за скриване информация. Стеганографията е реализирана по следните начини:

1) Метод на празните редове - при този метод се използват празни редове в програмния код на играта. Това по никакъв начин не променя функционалността на играта и остава скрито за потребителите. За целта всеки символ от скритото съобщение се трансформира в двоичен код, чрез своят ACSII код и в празен ред с разделители (интервали и табулатори) последователно се записват в празният ред от кода. Интервалите и табулаторите също не влияят на програмния код и на функционалността на играта.

2) Метод за добавяне на разделители - този метод отново използва преобразуване на тайното съобщение в двоичен код и скриване на информацията в програмния код на играта. Принципът на скриване е използването на разделителите (интервали и табулатори) в края на всеки ред от програмния код. Този метод избягва поява на излишни празни редове, за да не се предизвиква съмнение за стеганография, дори и при прочитане на програмния код.

3) Използване на динамичен файл - при този метод се използва файла за записване на резултатите от играта. Това е динамичен файл, в който постоянно се записват данни, което не предизвиква съмнение при стеганографски анализ.

4 Стеганографски анализ

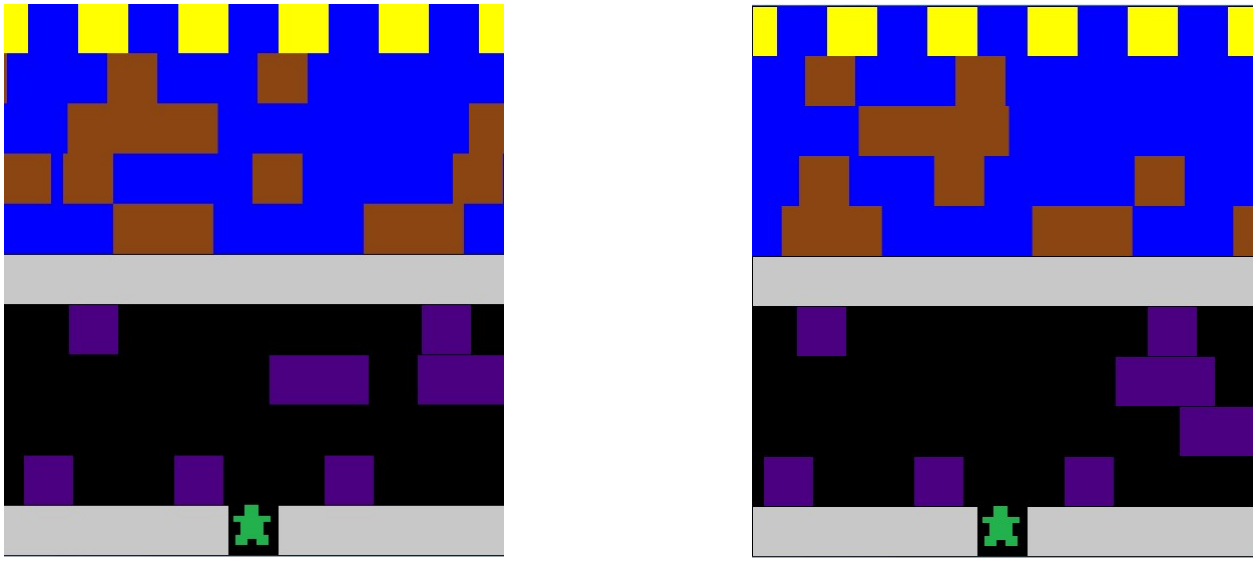
Стеганографският анализ е изследване, което има за цел да провери за наличие на стеганография. Изборът на нетрадиционен метод за скриване на тайна информация в компютърна игра, прави традиционните изследвания неприложими. По тази причина са разгледани само двата най-важни аспекта на стеганографията - визуалният анализ и чувствителността към секретния ключ.

4.1 Визуален анализ

Визуалният анализ определя наличието на видими разлики в началните условия, преди и след използването на стеганография. При предложеният метод на стеганография се прави сравнение във функционалността на играта и на програмната библиотека при скриване на тайна информация.

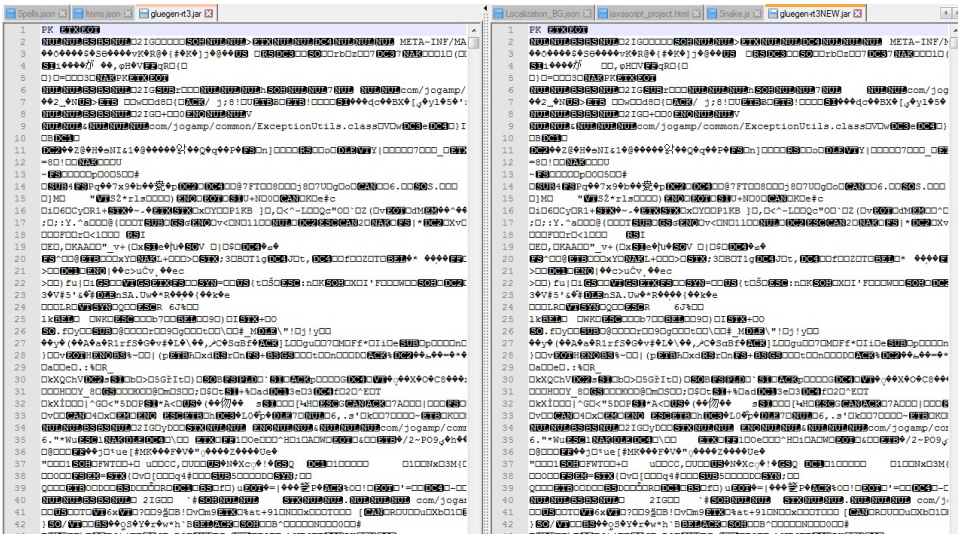
Показаният визуален анализ на (Фигура 3) нагледно показва, че няма забележима разлика във функционалността на играта, независимо дали присъства стеганография.

При сравнението на библиотечните файлове, съдържащи програмния код на играта (Фигура 4) се демонстрира невъзможност да се разчете някаква информация, поради специфичният начин на визуализиране на библиотечните файлове с програмен код на Java.



а) без скрита информация б) при скрита информация

Фигура 3: Визуален анализ - функционалност на играта.

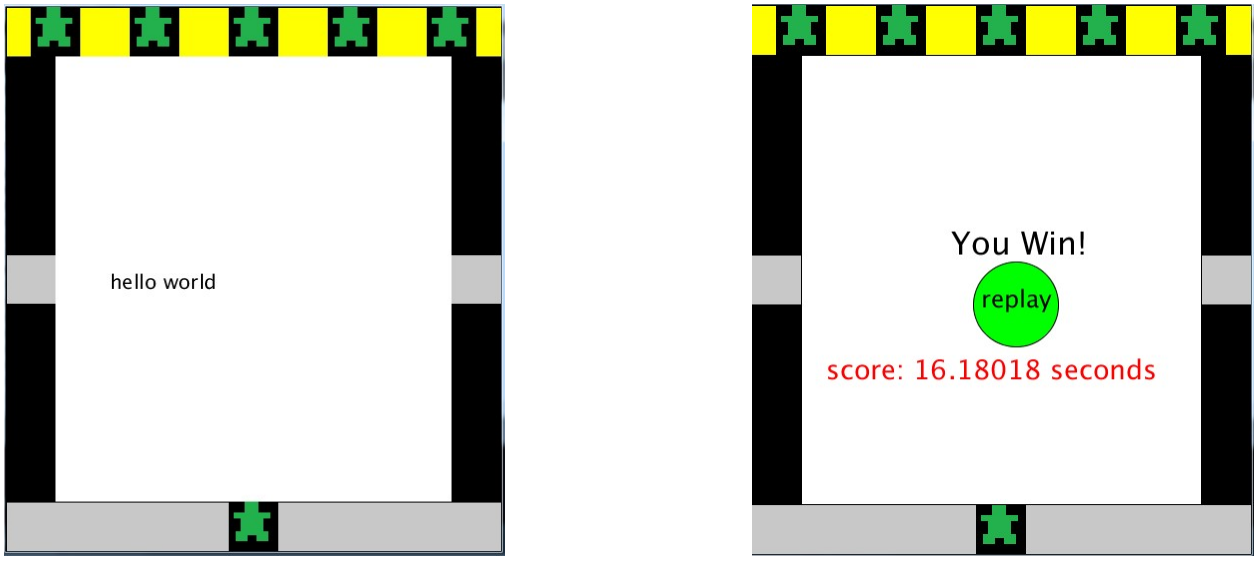


Фигура 4: Визуален анализ - сравнение на програмния код.

4.2 Чувствителност към секретният ключ

Използването на компютърна игра за скриване на информация, променя донякъде разбирането за секретен ключ, в този случай. Под секретен ключ се разбира фиксирана последователност от действия, които трябва да се извършат в играта. Играта трябва да се изиграе по точно определен, предварително зададен начин, като последователността е следната - 2, 0, 3, 1, 4. Тази последователност представлява секретния ключ на стеганографският метод. Това е изследване, което показва чувствителността към секретния ключ, като за целта се използва ключ K1 и леко променен ключ K2. Експериментите показват, че дори и при малка промяна на секретния ключ е невъзможно да се разкрие скритата информация. За експерименталното

тестване, оригиналният ключ К1 е избран с позиционна последователност 2,0,3,1,4 и ключ К2 е избран с минимална разлика - 2,0,3,4,1. На (Фигура 5) е показано, че при минимални разлики в ключа, дори самата стеганографска функционалност остава скрита.



а) секретен ключ К1 б) секретен ключ К2

Фигура 5: Чувствителност към секретния ключ.

При използване на вярна последователност (К1) играта коректно активира стеганографската функционалност, но при всички останали случаи потребителят приключва играта по стандартен начин.

5 Заключение

Компютърните игри са световен феномен в последните години и са се превърнали в едни от печелившите индустриални фактори в глобален мащаб. Те са широко разпространени, динамични (променяни, подобрявани и обновявани) и дори вече повечето игри целенасочено съдържат скрита информация с апелативна функция към потребителите, което прави скриването на допълнителна информация още по удобно и неочаквано. Подобно скриване на информация предлага много по-добра защита от други стеганографски методи, защото компютърните игри могат да предоставят огромен стегокапацитет и да бъдат хранилище за скрита информация, без това да указва влияние на качеството на самата игра.

Представеният стеганографски алгоритъм, базиран на компютърна игра демонстрира нетрадиционна стеганография на цифрова информация, а направеният стеганографски анализ, показва наличие на необходимото ниво на сигурност при използване на предложеният алгоритъм.

ЛИТЕРАТУРА:

[1] Семерджиев, Ц., (2007) Сигурност и защита на информацията. София: Класика и стил. 2007. ISBN 978-954-327-034-7.

[2] Станев, С., (2013), Стеганологична защита на информацията. Университетско издателство „Епископ Константин Преславски”. Шумен, 2013. ISBN 978-954-577-825-4. 320.

[3] Станев, С., Стоянов, Б., (2016), Предизвикателствата на стеганографията към информационната сигурност и обучението на специалисти, Годишник на ШУ „Епископ К. Преславски" Факултет по математика и информатика, том XVII С, 2016

[4] Станев, С., Железов, С., Параскевов, Х., Христов, Х., (2015), Ръководство за упражнения по стеганография, Университетско издателство „Епископ Константин Преславски", Шумен 2015.

[5] Станев, С., Железов, С., Якимов, И., (2012), Реализация на паралелен стеганализ с клъстерна система, Международна научна конференция" Съвременни методи и технологии в научните изследвания", Варна 2012.

[6] Fridrich, J., (2006), Steganalysis. In Multimedia Security Technologies for Digital Rights Management (pp. 349-381).

[7] Fridrich, J.,(2010), Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press, 437 p. ISBN 978-0521190190.

[8] Gibbs, C., Shashidhar, N., (2015), StegoRogue: Steganography in Two-Dimensional Video Game Maps. Advances in Computer Science: an International Journal, 4(3), 141-146.

[9] Hale, C., Chen, L., Liu, Q., (2012, December), A new villain: Investigating steganography in source engine based video games. In Proceedings of the 2012 Hong Kong International Conference on Engineering & Applied Science (HKICEAS), Hong Kong, China, December 14 (Vol. 16).

[10] Kent, S. L., (2010). The Ultimate History of Video Games: from Pong to Pokemon and beyond... the story behind the craze that touched our lives and changed the world. Three Rivers Press.

[11] Kordov, K., (2014), Modified Chebyshev Map Based Pseudo-random Bit Generator. In AIP Conference Proceedings (Vol. 1629, pp. 432-436).

[12] Kordov, K., (2015), Signature Attractor Based Pseudorandom Generation Algorithm. Advanced Studies in Theoretical Physics, 9(6), 287-293.

[13] Kordov, K., Stoyanov, B., (2017), Least Significant Bit Steganography using Hitzl-Zele Chaotic Map, International Journal of Electronics and Telecommunications, 63(4), 417-422. doi: https://doi.org/10.1515/eletel-2017-0061

[14] Marchand, A., Hennig-Thurau, T., (2013), Value creation in the video game industry: Industry economics, consumer benefits, and research opportunities. Journal of Interactive Marketing, 27(3), 141-157.

[15] Novak, J., (2011), Game development essentials: an introduction, Cengage Learning.

[16] Stanev, S., Szczypiorski, K., (2016), Steganography Training: a Case Study from University of Shumen in Bulgaria, International Journal of Electronics and Telecommunications, 62(3), 315-318. doi: https://doi.org/10.1515/eletel-2016-0043

[17] Stoyanov, B., (2014), Pseudo-random Bit Generation Algorithm Based on Chebyshev Polynomial and Tinkerbell Map. Applied Mathematical Sciences, 8(125), 6205-6210.

[18] Stoyanov, B., (2014, November), Using circle map in pseudorandom bit generation. In AIP Conference Proceedings (Vol. 1629, No. 1, pp. 460-463). AIP.

[19] Stoyanov, B., Zhelezov, S, Kordov, K., (2016), Least significant bit image steganography algorithm based on chaotic rotation equations, Comptes rendus de l'Académie bulgare des Sciences, 69(7), 845-850.

[20] Wolf, M. J. (Ed.). (2008). The video game explosion: a history from PONG to Playstation and beyond. ABC-CLIO.

[21] Zhelezov, S., (2016), Modified Algorithm for Steganalysis, Mathematical and Software Engineering, 1(2), 31-36.

[22] Zhelezov S., Paraskevov H., (2015), Possibilities for steganographic parallel processing with a cluster system, Contemporary Engineering Sciences, 8(20).

[23] Zielińska, E., Mazurczyk, W., Szczypiorski, K., (2014)., Trends in steganography. Communications of the ACM, 57(3), 86-95.

[24] URL: https://www.nintendo.com/ - официален сайт на Nintendo (20.06.2018).

[25] URL: http://www.sega.com/ - официален сайт на Sega (20.06.2018)

[26] URL: https://www.xbox.com/ - официален сайт на XBOX (20.06.2018)

[27] URL: https://www.playstation.com/ - официален сайт на Playstation (20.06.2018)

[28] URL: https://bethesda.net/ - официален сайт на Bethesda (20.06.2018)

[29] URL: https://www.ubisoft.com/en-gb/ - официален сайт на Ubisoft (20.06.2018)

[30] URL: https://www.rockstargames.com/ - официален сайт на Rockstar games (20.06.2018)

[31] URL: http://en.cdprojektred.com/ - официален сайт на CD Project RED (20.06.2018)

Красимир Кордов, Даниел Йорданов
Шуменски университет ”Еп. Константин Преславски”
E-mail: krasimir.kordov@shu.bg