СИСТЕМЫ И ПРОЦЕССЫ УПРАВЛЕНИЯ

УДК 621.327:681.5

МЕТОД ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РОЗМЕЖУВАННЯ ДОСТУПУ ДО АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

БАРАННІК Н.В., БАБЕНКО Ю.М., ПАРХОМЕНКО М.В. ЖУЙКОВ Д.Б., ЄРОШЕНКО В.П., ПІСКУН Я.А.

Встановлюється, що методи підвищення інформаційної безпеки мають низку недоліків: захист та дискримінація, можливість підробки паролю, невиконання інструкцій по створенню безпечного паролю користувачем, існування і наявність у вільному доступі спеціалізованих додатків для підбору і злому паролів, пароль може бути отриманий шляхом застосування насильства до користувача, може бути вкрадений, тобто перехоплений при введенні власником.

Ключові слова: біотехнолгії, ідентифікація, аутентифікація, верифікація, системи доступу, шаблон, зіставлення, сховище даних.

Key-words: biotechnology, identification, authentication, verification, access system, template, mapping, related data.

1. Вступ

У сучасному суспільстві інформація стала одним із найважливіших стратегічних ресурсів, що забезпечує подальший розвиток підприємства. Саме тому інформація, як і решта ресурсів, потребує особливого захисту. Проблема інформаційної безпеки набула великого значення в сучасних умовах широкого застосування автоматизованих інформаційних систем. У зв'язку із зростаючою роллю інформаційних ресурсів у житті сучасного суспільства, а також через реальність численних загроз проблема інформаційної безпеки вимагає до себе постійної і значної уваги. Одним з можливих рішень задачі підвищення інформаційних систем є створення біометричної системи ідентифікації доступу з застосуванням стеганографічного методу захисту інформації [1-7].

Методи стеганографії дозволяють не тільки приховано передавати дані, але й успішно вирішувати завдання завадостійкої автентифікації, захисту інформації від несанкціонованого копіювання, відстеження поширення інформації мережами зв'язку, пошуку інформації в мультимедійних базах даних.

2. Аналіз останніх досліджень і публікацій

Проаналізувавши останні наукові публікації, можна зробити висновок, що методи цифрової стеганографії мають ряд недоліків [8-15]: захист та дискримінація, можливість підробки паролю, невиконання інструкцій по створенню безпечного паролю користувачем, існування і наявність у вільному доступі спеціалізованих додатків для підбору і злому паролів, пароль може бути отриманий шляхом застосування насильства до користувача, може бути вкрадений, тобто перехоплений при введенні власником. Людський фактор є основним недоліком даних систем для захисту від підміни законного користувача, наприклад, користувач може відлучитися від робочого місця, забувши вийняти USB-ключ.

Основною перевагою біометричних технологій (біометрії або біометрики) є можливість швидкої і простої ідентифікації або верифікації здебільшого без спричинення якихось незручностей індивідуумові. Використання досягнень комп'ютерно-інформаційних і телекомунікаційних технологій дозволяє здійснювати ідентифікацію користувача в режимі реального часу. Біометричні технології засновані на інтеграції досягнень у галузі електроніки, інформатики, математики, медицини й біометрії, а останнім часом і на основі нанотехнологій, що дозволяє істотно зменшити габарити використовуваної апаратури для біометричних систем, що розробляються [16-22].

3. Розробка методу підвищення інформаційної безпеки інформаційно-телекомунікаційної системи

Метод розпізнавання особи за райдужною оболонкою та реакцією очного яблука людини на подразники складається з таких етапів:

1) Запит на процес ідентифікації, тобто встановлення відповідності особи та визначення її прав на виконання тих чи інших дій. Особа, яка хоче отримати доступ до даних, повинна наблизити обличчя до сканера, зафіксувати його положення і направити погляд на спеціальну мітку на дисплеї сканера. Далі камера робить знімки з швидкістю десятки кадрів за секунду, і отримані зображення обробляються спеціальною програмою. Промінь, що падає на викривлену поверхню, згинається, чим більша кривизна поверхні, тим сильніший вигин променя. Спочатку при цьому застосовувалося джерело видимого світла. Потім видиме світло було замінене на інфрачервоне.

2) Введення людиною ключа (паролю). Ключ – це правило для стеганографічного перетворення зробленого системою знімку. Ключ – певна послідовність літер/цифр, відомих системі, особі, яка подає запит на ідентифікацію та адміністратору системи. За допомогою нього система розміщує дані по контейнеру. Таким чином, зловмисник не знатиме, в які блоки контейнера занесено стеганографічні зміни. Кори-

стувач повинен ввести 2 ключі: перший – для закриття інформації; другий – для стеганографічного розміщення в контейнері.

Отже, підвищується складність доступу в систему неавторизованих користувачів.

3) Формування шаблону на основі зробленого знімку. На першому етапі обробки видаляються зображення, на якому обличчя не видно взагалі або присутні сторонні предмети, що заважають ідентифікації. За отриманими знімками відновлюється 3-D модель особи, на якій виділяються і віддаляються непотрібні перешкоди (зачіска, борода, вуса й окуляри). Потім проводиться аналіз моделі – виділяються антропометричні особливості. Проходить виділення «кола» зіниці із загального зображення очного яблука та виділення сліпих зон. Вимірюється час реакції очного яблука людини на подразники.

4) Формування контуру зображення. Для цифрових зображень найбільш корисним семантичним навантаженням є контури об'єктів. Контури являють собою лінії, які проходять на межах однорідних областей. Елементи $z_{i,j}$ просторово-часового подання зображення, значення яких не перевищують певного порогу, формують однорідні області. Це задається умовою:

$$\left| z_{\max} - z_{\min} \right| \le 1 , \qquad (1)$$

де z_{max} – елемент області зображення, який має найбільше значення, визначається на основі виразу:

$$z_{\max} = \max_{1 \le i \le x} \{ z_{i,j} \} , \; j = \overline{1, y} . \qquad (2)$$

Тут z_{min} – елемент області зображення, який має найменше значення, визначається на основі формули:

$$z_{\min} = \min_{1 \le i \le x} \{ z_{i,j} \} , \; j = \overline{1, y} , \qquad (3)$$

де 1 – поріг виявлення однорідних областей.

Найбільш поширеним способом пошуку контурів є обробка зображення ковзною маскою. Маска являє собою квадратну матрицю з коефіцієнтами. Процес обробки зображення на основі матриці називається фільтрацією або маскуванням і задається функціоналом $f(Z, K)$:

$$M = f(Z, K), \qquad (4)$$

де M – зображення, отримане в результаті обробки зображення Z на основі маски K.

Процес фільтрації заснований на поступовому просторовому переміщенні маски фільтра від елемента до елемента зображення. Видно, що значення елемента m_{ij} (відгуку фільтрації) обчислюється з використанням значень попередніх і наступних елементів у двомірній площині.

В цьому випадку значення елемента m_{ij} маски зображення M, отриманого в результаті маскування, визначається за формулою:

$$m_{i,j} = \sum_{\xi=i-1}^{i+1} \sum_{\tau=i-1}^{\tau+1} z_{\xi,\tau} \cdot k \; . \qquad (5)$$

5) Вбудовування даних в найменш значущі біти (НЗБ) просторового представлення зображення. НЗБ обираються за допомогою введеного другого ключа користувачем на етапі №2. Вбудовування повідомлення відбувається в молодший біт зображення, який несе в собі найменше інформації. Розмір вбудованого повідомлення може складати 1/8 загального обсягу контейнера. Наприклад, в зображення розміром 512x512 можна вбудувати 32 кБайт інформації. Якщо модифікувати два найменших біта, то пропускну спроможність можна збільшити вдвічі.

Метод вбудовування даних в спектральну область є дещо складнішим, в порівнянні з вбудовою повідомлення в просторово-часову область зображення. Вбудовування інформації відбувається після дискретно-косинусного перетворення (ДКП) зображення.

6) Надсилання стеганографічно перетвореного зображення в «хмарне» середовище. Кожна біометрична система має підсистему зберігання даних – реєстраційну базу, яка служить для зберігання шаблонів. Пропонується зберігати, стеганографічно перетворювати шаблони та порівнювати їх в захищеному хмарному середовищі.

7) Порівняння шаблону з інформацією в реєстраційній базі даних. Отриманий шаблон для проведення верифікації порівнюється з тим, що зберігається, для того, щоб визначити, чи збігаються ці шаблони. Ця технологія використовує установчі дані (ключі, введені користувачем) користувача як покажчика для отримання облікового запису абонента системи, який зберігається, та перевірки відповідності «один до одного» (аутентифікація або верифікація) між шаблоном, отриманим під час верифікації параметрів біометричного показника, і вже наявним для цього імені користувача шаблоном. У іншому випадку (процедура ідентифікації) шаблон параметра біометричного показника, що пред'являється, зіставляється з усім набором шаблонів, які зберігаються.

8. Прийняття рішення системою («свій» / «чужий»).

4. Висновки

Запропоновано принцип роботи ідентифікаційної системи розпізнавання за райдужною оболонкою та реакцією очного яблука людини на подразники з використанням стеганографічного перетворення (використання двох ключів вводу користувачем для закриття та стеганографічного розміщення інформації). Збереження даних буде відбуватись в хмарному середовищі.

Як наслідок, створення системи захисту інформації з використанням біометричних методів ідентифікації користувачів зменшить вплив «людського» фактору, що підвищить ефективність процедур ідентифікації й аутентифікації. Тому застосування систем біометричної ідентифікації можливе тільки в автоматизованих системах, що обробляють і зберігають персональні дані та частково комерційну й службову таємницю.

Література: 1. *Gribunin VG, Okov IN, Turincev IV*, Cifrovaja steganografija. M.: Solon-Press, 2018. 248 s. **2.** *Grundmann M., Kwatra V., Han M., Essa I.* Efficient hierarchical graph based video segmentation // IEEE CVPR. 2010. P. 85-91. **3.** *Melnik A.C.* Information systems and networks. Bulletin [Text] / M.M. Goloborodko NU "Lviv Polytechnic". Lviv, 2010. №. 673. P. 365-374. **4.** *Gonzalez R.* Digital image processing. 4th edition. [Text] / R. Gonzalez, R. Woods. K.: Tekhnosfera, 2018. 1104 p. **5.** *Konakhovich G.F.* Computer steganography. Theory and practice [Text] / G.F. Konakhovich, A.Yu. Puzyrenko. Kiev: To Press, 2016. 288 p. **6.** *Miano J.* Formats and image compression algorithms in action [Text]. K.: Triumph, 2013. 336 p. **7.** *Ablamejko S.V., Lagunovskij D.M.* Obrabotka izobrazhenij: teh-nologija, metody, primenenie. Minsk: Amalfeja, 2000. 303 s. **8.** *Miano J.* Compressed image file formats: JPEG, PNG, GIF, XBM, BMP / by John Miano. 1999. 264 p. **9.** *Pratt W. K.*, *Chen W. H., Welch L. R.* Slant transform image coding. Proc. Computer Processing in communications. New York: Polytechnic Press, 1969. P. 63-84. **10.** *Sindeev M., Konushin A., Rother C.* Alpha-flow for video matting. Technical Report. 2012. P. 41–46. **11.** *Wallace G. K.* The JPEG Still Picture Compression Standard. Communication in ACM. 1991. V34. №4. P. 31-34. **12.** *Stankiewicz O., Wegner K., Karwowski D. , Stankowski J., Klimaszewski K. and Grajek T.* Encoding mode selection in HEVC with the use of noise reduction // 2017 International Conference on Systems, Signals and Image Processing (IWSSIP). Poznan, 2017. P. 1-6. **13.** *Wang S., Zhang X., Liu X., Zhang J., Ma S. and Gao W.* Utility-Driven Adaptive Preprocessing for Screen Content Video Compression // IEEE Transactions on Multimedia. March 2017. Vol. 19, no. 3. P. 660-667. **14.** *Christophe E., Lager D., Mailhes C.* Quality criteria benchmark for hiperspectral imagery // IEEE Transactions on Geoscience and Remote Sensing. Sept 2005. Vol. 43, No 9. P. 2103–2114. **15.** *Wallace G.K.* Overview of the JPEG (ISO/CCITT) Still image compression: image processing algorithms and techniques // Processing of the SPIE. 1990. Vol. 1244. P. 220-233. **16.** *Barannik V., Barannik D., Bekirov A., Lekakh A.* A steganographic method based on the modification of regions of the image with different saturation // Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), 14th International Conference, 2018. P. 542-545. DOI: 10.1109/TCSET.2018.8336260. **17.** *Barannik V., Alimpiev A., Bekirov A., Barannik D., Barannik N.* Detections of sustainable areas for steganographic embedding // IEEE East-West Design & Test Symposium (EWDTS). 2017. P. 555-558. DOI: 10.1109/EWDTS.2017.8110028. **18.** *Barannik V.V., Ryabukha Yu.N., Tverdokhleb V.V., Barannik D.V.* Methodological basis for constructing a method for compressing of transformants bit representation, based on non-equilibrium positional encoding // Proceedings of the 2nd IEEE International Conference on Advanced Information and Communication Technologies, AICT 2017. Lviv. P. 188-192. DOI: 10.1109/ AIACT.2017.8020096+/. **19.** *Zhuravlev A.P.* Phonetic significance [Text] / AP Zhuravlev. L.: LGU, 1974. **20.** *Belikova T.V.* Methods of Detection of Destructive Suggestive Information-Psychological Operations in the Information and Social Space [Text] / T.V. Belikova // Radioelektronika i informatika. 2016. N 3. P. 62-68. **21.** *Баранник В.В.* Основы теории структурно-комбинаторного стеганографического кодирования: монография / В.В. Баранник, Д.В. Баранник, А.Э Бекиров. Х.: Издательство «Лидер», 2017. 256 с. **22.** *Barannik D., Bekirov A., Frolov O., Suprun O.* The new method of secure data transmission on the indirect steganography basis // IEEE East-West Design & Test Symposium (EWDTS). 2016. P. 1-4. DOI: 10.1109/EWDTS.2016.7807754.

Транслітерированний список літератури:

1. *Gribunin VG, Okov IN, Turincev IV*, Cifrovaja steganografija. M .: Solon-Press, 2018. 248 s.

2. *Grundmann M., Kwatra V., Han M., Essa I.* Efficient hierarchical graph based video segmentation. IEEE CVPR. 2010. P. 85-91.

3. *Melnik A.C.* Information systems and networks. Bulletin [Text] / M.M. Goloborodko. №. 673. Lviv: NU "Lviv Polytechnic". 2010. P. 365-374.

4. *Gonzalez R.* Digital image processing [Text] / R. Gonzalez, R. Woods. K.: Tekhnosfera, 2018. 1104 p.

5. *Konakhovich G.F.* Computer steganography. Theory and practice [Text] / G.F. Konakhovich, A.Yu. Puzyrenko. Kiev: To Press, 2016. 288 p.

6. *Miano J.* Formats and image compression algorithms in action [Text]. K.: Triumph, 2013. 336 p.

7. *Ablamejko S.V., Lagunovskij D.M.* Obrabotka izobrazhenij: tehnologija, metody, primenenie. Minsk: Amalfeja, 2000. 303 s.

8. *Miano J.* Compressed image file formats: JPEG, PNG, GIF, XBM, BMP / by John Miano. 1999. 264 p.

9. *Pratt W. K.*, *Chen W. H., Welch L. R.* Slant transform image coding. Proc. Computer Processing in communications. New York: Polytechnic Press, 1969. P. 63-84.

10. *Sindeev M., Konushin A., Rother C.* Alpha-flow for video matting. Technical Report. 2012. P. 41–46.

11. *Wallace G. K.* The JPEG Still Picture Compression Standard. Communication in ACM. 1991. V34. №4. P. 31-34.

12. *O. Stankiewicz, K. Wegner, D. Karwowski, J. Stankowski, K. Klimaszewski and T. Grajek,* "Encoding mode selection in HEVC with the use of noise reduction," 2017 International Conference on Systems, Signals and Image Processing (IWSSIP). Poznan. 2017. P. 1-6.

13. *S. Wang, X. Zhang, X. Liu, J. Zhang, S. Ma and W. Gao*, "Utility-Driven Adaptive Preprocessing for Screen Content Video Compression," in IEEE Transactions on Multimedia, vol. 19, no. 3, pp. 660-667, March 2017.

14. *Christophe E., Lager D., Mailhes C.* Quality criteria benchmark for hiperspectral imagery. IEEE Transactions on Geoscience and Remote Sensing. Sept 2005. Vol. 43. No 9. P. 2103–2114.

15. *Wallace G.K.* Overview of the JPEG (ISO/CCITT) Still image compression: image processing algorithms and techniques. Processing of the SPIE. 1990. Vol. 1244. P. 220-233.

16. *Barannik V., Barannik D., Bekirov A., Lekakh A.* A steganographic method based on the modification of regions of the image with different saturation // Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), 14th International Conference, 2018. P. 542-545. DOI: 10.1109/TCSET.2018.8336260.

17. *Barannik V., Alimpiev A., Bekirov A., Barannik D., Barannik N.* Detections of sustainable areas for steganographic embedding // East-West Design & Test Symposium (EWDTS). IEEE, 2017. P. 555-558. DOI: 10.1109/EWDTS.2017.8110028.

18. *Barannik V.V., Ryabukha Yu.N., Tverdokhleb V.V., Baranmk D.V.* Methodological basis for constructing a method for compressing of transformants bit representation, based on non-equilibrium positional encoding. 2nd IEEE International Conference on Advanced Information and Communication Technologies, AICT 2017, Proceedings, Lviv, 2017, pp. 188 - 192. DOI: 10.1109 / AIACT.2017.8020096+/.

19. *Zhuravlev AP* Phonetic significance [Text] / AP Zhuravlev. L.: LGU, 1974.

20. *Belikova T.V.* Methods of Detection of Destructive Suggestive Information-Psychological Operations in the Information and Social Space [Text] / T.V. Belikova // Radioelektronika i informatika. 2016. N 3. P. 62-68.

21. *Barannik V.V.* Fundamentals of the theory of structurally combinatorial steganographic coding: monograph / V.V. Barannik, D.V. Barannik, A.E. Bekirov. X.: Publisher "Leader", 2017. 256 p.

22. *Barannik D., Bekirov A., Frolov O., Suprun O.* The new method of secure data transmission on the indirect steganography basis // IEEE East-West Design & Test Symposium (EWDTS). 2016. P. 1-4. DOI: 10.1109/EWDTS.2016.7807754.

Надійшла до редколегії 11.11.2019

Рецензент: д-р техн. наук, проф. Безрук В.М.

Бараннік Наталія В'ячеславівна, завідувач бібліотеки Національного університету цивільного захисту України. Наукові інтереси: методи підвищення інформаційної безпеки. Адреса: Україна, 61023, Харків, вул. Сумська, 77/79, e-mail: Barannik_V_V@ukr.net

Бабенко Юрій Михайлович, аспірант кафедри кіберзахисту та захисту інформації факультету інформаційних технологій Київського національного університету ім. Тараса Шевченка. Наукові інтереси: методи підвищення інформаційної безпеки. Адреса: Україна, 01601, Київ, вул. Володимирська, 64/13, e-mail: babenkomahalych@gmail.com.

Пархоменко Максим Вікторович, викладач Харківського національного університету Повітряних Сил ім. І. Кожедуба. Наукові інтереси: методи підвищення інформаційної безпеки. Адреса: Україна, 61023, Харків, вул. Сумська, 77/79, e-mail: maxpar76@gmail.com.

Жуйков Дмитрий Борисович, доцент кафедри Харківського національного університету Повітряних Сил ім. І. Кожедуба. Наукові інтереси: методи підвищення інформаційної безпеки. Адреса: Україна, 61023, Харків, вул. Сумська, 77/79, e-mail: vvbar.off@gmail.com

Єрошенко Валерій Петрович, канд. техн. наук, викладач кафедри Харківського національного університету Повітряних Сил ім. І. Кожедуба. Адреса: Україна, 61023, Харків, вул. Сумська, 77/79, e-mail: e-mail: wpEroshenko59@gmail.com

Піскун Ярослав Андрійович, студент ХНУРЕ. Адреса: Україна, 61166, Харків, пр. Науки, 14.

Barannik Natalia Vyacheslavivna, library manager of the National university of civil defence of Ukraine. Ukraine, Kharkiv, Sumska Str., 77/79.

Babenko Yurii, PhD, Department of cyber security and information hijacking of Faculty of Information Technology of Taras Shevchenko National University of Kyiv. Scientific interests: methods of improving information security. Address: Ukraine, 01601, Kyiv, Vladimirskaya Str, 64/13, e-mail: babenkomahalych@gmail.com.

Maksym Parkhomenko, Combat of ASC department, Ivan Kozhedub Kharkiv National Air Force University. Address: Ukraine, 61023, Kharkiv, Sumskaya Str., 77/79, e-mail: maxpar76@gmail.com.

Dmytro Zhuikov, PhD, Docent, Kharkiv National Air Force University Kharkiv named after Ivan Kozhedub Address: Ukraine, Kharkiv, Sumska str., 77/79, e-mail: vvbar.off@gmail.com

Yroshenko Valerii, Candidate of Technical Science, Teacher, Kharkiv National Air Force University Kharkiv named after Ivan Kozhedub. Kharkiv National Air Force University Kharkiv named after Ivan Kozhedub Address: Ukraine, Kharkiv, Sumska str., 77/79, e-mail: wpEroshenko59@gmail.com

Piskun Yaroslav, student, Kharkov National University of Radio Electronics. Address: Ukraine, 61166, Kharkiv, Nauky Ave, 14.