В.К. Грицюк, В.А. Золотарьов

Харківський національний університет радіоелектроніки, Харків

ПОРІВНЯННЯ СТІЙКОСТІ СТЕГАНОГРАФІЧНИХ МЕТОДІВ КОХО-ЖАО ТА DWT[10] ДО РІЗНИХ ТИПІВ СПОТВОРЕННЯ ПРОГРАМНИМИ ЗАСОБАМИ

Наведено результати практичних досліджень щодо використання алгоритмів вбудовування для приховування інформації в цифрових відео файлах, отримані за допомогою спеціально розробленої програми на мові Java. Оцінена різниця між початковим відео з вбудованими даними та спотвореним відео за показником індексу структурної подібності індексу структурної подібності SSIM, який вважається більш точним ніж параметр пікового відношення сигналу до шуму (PSNR), та завжди лежить у діапазоні від -1 до 1 . Проаналізовані результати, отримані на трьох етапах досліджень, оцінки відео з різними методами вбудовування; з різними методами завадостійкого кодування; з різними моделями каналів зв'язку. Оцінка стійкості до завад в залежності від вибору стеганографічного метода проводилася методами Кохо-Жао і DWT, використовувалися два пороги вбудовування, без завадостійких кодів та без імітації каналів зв'язку. Вплив використання різних методів завадостійкого кодування на стійкість відео проводився за допомогою кодів Хеммінга, БЧХ, РС. Оцінка стійкості до завад в залежності від каналів зв'язку проводилася для 4-х моделей, на які можна розкласти реальний канал зв'язку: каналу з простим шумом, каналу з чорно-білим шумом, каналу з адитивним білим гауссівським шумом та каналу з дискретним каналом зі стиранням. Дослідним шляхом було з'ясовано, що різниця в стійкості до завад для різних стеганографічних методів несуттєва; збільшення порогу вбудовування інформації приводить до зростання стійкості; ускладнення алгоритму кодування підвищує стійкість як до атак, так і для завад; виявлено, що найгіршим для передачі відео є дискретний канал зі стиранням.

Ключові слова: стеганографія, відео, програмування, метод Кохо-Жао, метод DWT, завадостійкі алгоритми, моделі каналів зв'язку, алгоритми вбудовування.

Вступ

Розвиток засобів цифрової обчислювальної техніки дав поштовх для розвитку комп'ютерної стеганографії, яка ґрунтується на вбудовуванні секретного повідомлення в цифрові дані, що, як прави-

ло, мають аналогову природу (аудіозаписи, зображення, відео).

Стегосистема – сукупність засобів і методів, які використовують для формування прихованого каналу передавання інформації. Загальну структуру стегосистеми наведено на рис. 1.

Рис. 1. Структура стегосистеми

Повідомлення вбудовується в контейнер за допомогою ключа стегокодером, формуючи стегоконтейнер, або стего. Стего на приймальній стороні надходить на стегодетектор, який витягає приховане повідомлення.

Зазвичай у якості контейнера використовують нерухомі цифрові зображення, а для захисту інтелектуальної власності контейнера використовують цифрові водяні знаки (ЦВЗ). ЦВЗ – це зазвичай невеликий обсяг інформації (наприклад, ім'я автора,

торгова марка, дата публікації, цифровий ідентифікатор об'єкта), яку вбудовують в контейнер для її подальшого виявлення, зокрема для підтвердження авторства у разі несанкціонованого копіювання.

Вбудовують ЦВЗ у нерухоме зображення різними методами, з яких можна виділити дві великі групи: приховування інформації в просторовій та частотній областях зображення.

Найпоширенішим методом приховування інформації в часовій (просторовій) області є метод

заміни найменшого значущого біта (LSB), що полягає в заміні надлишкової, малозначимої частини зображення бітами секретного повідомлення.

Стеганографічні методи приховування даних у просторовій області зображення є нестійкими до більшості з відомих видів спотворень. Наприклад, використання операції компресії із втратами (щодо зображення, це може бути JPEG-компресія) призводить до часткового або, що ймовірніше, повного знищення вбудованої в контейнер інформації. Стійкішими до різноманітних спотворень, зокрема й компресії, є методи, що використовують для приховування даних не просторову, а частотну область контейнера.

Найпоширенішими серед усіх ортогональних перетворень у стеганографії є вейвлет-перетворення, дискретно-косинусне перетворення та алгоритм Коха-Жао.

Для оцінки різниці між початковим відео з вбудованими даними та спотвореним відео можна використовувати параметр пікового відношення сигналу до шуму (PSNR) та індекс структурної подібності (SSIM).

SSIM вважається більш складним, і був створений для більш точного визначення різниці двох зображень або відео. Його особливість полягає в тому, що він завжди лежить у діапазоні від -1 до 1 . Якщо його значення дорівнює 1 , то ми маємо дві однакові картинки. Загальна формула має вигляд:

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}, \quad (1)$$

де μ_x – середнє значення пікселів першої картинки;

μ_y – середнє значення пікселів другої картинки;

σ_x^2 – середньоквадратичне відхилення для першої картинки;

σ_y^2 – середньоквадратичне відхилення для другої картинки;

σ_{xy} – коваріація.

Програма була доповнена двома моделями каналів зв'язку для кращого імітування реальної передачі повідомлення. Це модель каналу з адитивним білим гауссовським шумом та дискретний канал зі стиранням.

Для кращого імітування передачі відео необхідно дослідити вплив каналу передачі не відео з вбудованим повідомленням. Реальний канал зв'язку можна описати чотирма математичними моделями. Це модель каналу з простим шумом, чорно-білим шумом, адитивним білим гауссівським шумом та дискретний канал зі стиранням.

Для оцінки методів вбудовування була розроблена програма на мові Java, яка дозволяє оцінити різницю між початковим відео з вбудованими даними та спотвореним відео за показником SSIM. Дослідження складалося з трьох етапів: оцінка відео з різними методами вбудовування; з різними методами завадостійкого кодування; з різними моделями каналів зв'язку.

Виклад основного матеріалу

1 Оцінка стійкості до завад в залежності від вибору стеганографічного метода

Для оцінки першого етапу були обрані два стеганографічних метода, два пороги вбудовування, без завадостійких кодів та без імітації каналів зв'язку.

Всі вихідні результати наведені у табл. 1.

Для наочності дані наведені у вигляді стовпчиків діаграм (рис. 2).

Таблиця 1

Результати програми у вигляді показників SSIM

	Коха-Жао [10]	DWT [10]	Коха-Жао [30]	DWT [30]
Афінне перетворення	0,4141	0,37	0,3966	0,4
Стиснення у 3 рази	0,4908	0,4925	0,8025	0,8025
Стиснення у 6 разів	0,3883	0,3691	0,8025	0,8025
Стиснення у 9 разів	0,3491	0,3216	0,3816	0,3975
Перетворення в H.264	0,5023	0,4983	0,8025	0,8025
Перетворення в mpeg4	0,3858	0,3725	0,8025	0,8025
Перетворення в flv	0,3616	0,3633	0,8025	0,8025
Локальна атака на ЦВЗ	0,435	0,4208	0,8025	0,7983

Рис. 2. Стовпчикова діаграма показників SSIM в залежності від методу стеганографічного вбудовування

Як видно з рис. 2, зі збільшенням порога вбудовування зростає стійкість до декількох типів атак. Всі методи вбудовування майже в рівному ступені вразливі до стиснення в 9 разів та афінного перетворення.

Найгірші показники у DWT[10]. Цей метод відрізняється від Коха-Жао[10] на декілька сотих.

Найстійкішим методом вбудовування виявився DWT[30]. Дуже близьким до нього є Коха-Жао[30]. DWT[30] кращий в афінному перетворенні та стис-

ненні у 9 разів, втім Коха-Жао[30] краще у локальній атаці на ЦВЗ. Отже, можна стверджувати, що ці два методи рівні між собою.

2 Оцінка стійкості до завад в залежності від методу кодування

Наступним кроком стало дослідження впливу використання різних методів завадостійкого кодування на стійкість відео. В якості кодів були обрані код Хеммінга, код БЧХ та код РС.

Таблиця 2

Показники SSIM для коду Хеммінга

	Коха-Жао [10]	DWT [10]	Коха-Жао [30]	DWT [30]
Афінне перетворення	0,24	0,2341	0,2483	0,2291
Стиснення у 3 рази	0,2716	0,2691	0,41	0,4141
Стиснення у 6 разів	0,2216	0,22	0,4075	0,2533
Стиснення у 9 разів	0,1933	0,1833	0,2025	0,1958
Перетворення в H.264	0,2783	0,2625	0,4108	0,4141
Перетворення в tpeg4	0,2241	0,2091	0,3916	0,3808
Перетворення в flv	0,2158	0,1958	0,3933	0,3783
Локальна атака на ЦВЗ	0,2533	0,245	0,4025	0,3941

Таблиця 3

Показники SSIM для коду БЧХ

	Коха-Жао [10]	DWT [10]	Коха-Жао [30]	DWT [30]
Афінне перетворення	0,33	0,3116	0,33	0,3116
Стиснення у 3 рази	0,3458	0,3433	0,4633	0,465
Стиснення у 6 разів	0,3016	0,3108	0,4591	0,35
Стиснення у 9 разів	0,29	0,2991	0,2991	0,3033
Перетворення в H.264	0,3675	0,345	0,4616	0,4591
Перетворення в tpeg4	0,3058	0,3	0,4475	0,4383
Перетворення в flv	0,2983	0,2941	0,4466	0,4391
Локальна атака на ЦВЗ	0,3308	0,335	0,4466	0,4416

Показники SSIM для коду PC

	Коха-Жао [10]	DWT [10]	Коха-Жао [30]	DWT [30]
Афінне перетворення	0,4274	0,4014	0,442	0,4196
Стиснення у 3 рази	0,4033	0,4003	0,5118	0,5147
Стиснення у 6 разів	0,37	0,3821	0,5023	0,4362
Стиснення у 9 разів	0,3379	0,3411	0,3412	0,3671
Перетворення в Н.264	0,48	0,4682	0,5238	0,521
Перетворення в jpeg4	0,3793	0,372	0,4968	0,4909
Перетворення в flv	0,3586	0,339	0,5144	0,5087
Локальна атака на ЦВЗ	0,3974	0,4132	0,4793	0,471

Рис. 3. Стовпчикова діаграма показників SSIM для методу Коха-Жао[10]

Рис. 4. Стовпчикова діаграма показників SSIM для методу DWT[10]

Рис. 5. Стовпчикова діаграма показників SSIM для методу Коха-Жао[30]

Рис. 6. Стопчикова діаграма показників SSIM для методу DWT[30]

Після проведення декількох тестів було виявлено, що при використанні завадостійких кодів SSIM різко погіршується. Лише при використанні кодів Ріда-Соломона при порозі вбудовування 10 індекс стає таким самим як і без кодів, а при використанні порога вбудовування 30 SSIM показує більші результати.

Діаграми свідчать, що з ускладненням алгоритму кодування зростає стійкість до завад відео. Це пояснюється тим, що РС код працює з байтами інформації, на відміну від кодів Хеммінга та БЧХ, і тому він здатний виправити значну кількість помилок.

3 Оцінка стійкості до завад в залежності від каналу зв'язку

Мало знайти методи, стійкі до атак зловмисника. Треба знайти методи, які будуть добре себе показувати при передачі даних у реальних умовах, тобто по каналах зв'язку. Тому слід дослідити, як канал передачі впливає на відео з різними кодами та методами вбудовування. У якості каналів розглядаються 4 найпростіші моделі, на які можна розкласти реальний канал зв'язку. Також досліджуються канали з різною потужністю завади, щоб зрозуміти, як показник буде зменшуватись.

Таблиця 5

Показники SSIM відео з кодом Хеммінга для різних каналів передачі

	Коха-Жао [10]	DWT [10]	Коха-Жао [30]	DWT [30]
Канал з простим шумом[1]	0,26	0,26	0,4116	0,4125
Канал з простим шумом[8]	0,2608	0,26	0,2558	0,2625
Канал з АБГШ[1]	0,2566	0,2616	0,3583	0,3508
Канал з АБГШ[8]	0,2591	0,26	0,3658	0,3308
Канал з чорно-білим шумом[1]	0,2683	0,27	0,4075	0,4041
Канал з чорно-білим шумом[5]	0,2625	0,2625	0,3516	0,3341
Дискретний канал з стиранням[1]	0,1742	0,1783	0,3	0,2971
Дискретний канал з стиранням[4]	0,1707	0,1755	0,2788	0,2742

Таблиця 6

Показники SSIM відео з кодом БЧХ для різних каналів передачі

	Коха-Жао [10]	DWT [10]	Коха-Жао [30]	DWT [30]
Канал з простим шумом[1]	0,3458	0,3483	0,4675	0,4608
Канал з простим шумом[8]	0,3466	0,3475	0,3483	0,3467
Канал з АБГШ[1]	0,3541	0,3441	0,4283	0,4116
Канал з АБГШ[8]	0,3466	0,3475	0,435	0,4041
Канал з чорно-білим шумом[1]	0,345	0,3583	0,4533	0,4416
Канал з чорно-білим шумом[5]	0,3467	0,35	0,42	0,405
Дискретний канал з стиранням[1]	0,2601	0,2579	0,4451	0,4497
Дискретний канал з стиранням[4]	0,2257	0,224	0,404	0,4023

Таблиця 7

Показники SSIM відео з кодом РС для різних каналів передачі

	Коха-Жао [10]	DWT [10]	Коха-Жао [30]	DWT [30]
Канал з простим шумом[1]	1	1	1	1
Канал з простим шумом[8]	0,94	0,9356	1	1
Канал з АБГШ[1]	0,88	0,8827	1	1
Канал з АБГШ[8]	0,8796	0,8802	1	1
Канал з чорно-білим шумом[1]	0,9763	0,9758	1	1
Канал з чорно-білим шумом[5]	0,9421	0,9382	1	1
Дискретний канал з стиранням[1]	0,6348	0,631	0,774	0,7687
Дискретний канал з стиранням[4]	0,5772	0,5834	0,7261	0,73

Рис. 7. SSIM для відео з кодом Хеммінга для різних каналів передачі

Рис. 8. SSIM для відео з кодом БЧХ для різних каналів передачі

Рис. 9. SSIM для відео з кодом PC для різних каналів передачі

Як видно з стовпчикових діаграм, стійкіший код до завад у каналі є PC. А більшого впливу надає дискретний канал зі стиранням.

Висновки

В даній роботі було проведено дослідження та порівняльна характеристика методів вбудовування інформації, методів завадостійкого кодування та каналів зв'язку для відео контейнера. Також були отримані кількісні результати порівняння різних методів завадостійкого кодування прихованого повідомлення, що дає можливість підвищити загальну

стійкість систем прихованої передачі інформації на базі відео контейнера.

В ході дослідження були зроблені наступні висновки:

- Різниця в стійкості до завад для різних методів вбудовування невелика.
- Збільшення порога вбудовування інформації викликає зростання стійкості.
- Ускладнення алгоритму кодування підвищує стійкість відео як до атак, так і до завад у каналах зв'язку.
- Найгіршим каналом для передачі відео є дискретний канал зі стиранням.

Список літератури

1. Fridrich J. Steganography in digital media: principles, algorithms, and applications / J. Fridrich. – Cambridge university press, 2010. – 437 p.
2. Li M. Steganalysis of SS steganography: hidden data identification and extraction / M. Li, Q. Liu // Circuits, systems and signal processing. – 2015. – Vol. 34. – № 10. – P. 3305-3324.
3. Анализ принципов создания и работы стеганографических алгоритмов / А.В. Лейман, А.Г. Коробейников, С.С. Кувшинов, С.Ю. Блинов // Программные системы и вычислительные методы. – Москва: М: НБ-Медиа, 2012. – Вып. 1. – № 1. – Модели и методы управления информационной безопасностью. – С. 28-36. ISSN 2305-6061.
4. Urbanovich N. The use of steganographic techniques for protection of intellectual property rights / N. Urbanovich, V. Plaskovitsky // New Electrical and Electronic Technologies and their Industrial Implementation. – 2011. – P. 147-148.
5. Рябко Б.Я. Основы современной криптографии и стеганографии / Б.Я. Рябко, А.Н. Фионов. – М.: Горячая линия-Телеком, 2010. – 232 с.
6. Zielinska E. Trends in steganography / E. Zielinska, W Mazurczyk, K. Szczypiorski // Communications of the ACM. – 2014. – Vol. 57. – № 3. – P. 86-95.
7. Старченко А.П. Методы встраивания и идентификации скрытых водяных знаков / А.П. Старченко. – СПб., 2011. – 103 с.
8. Марков М.В. Модели дискретных каналов связи / М.В. Марков // Сервис в России и за рубежом. – 2011. – С. 143.
9. Ничипорук Н.Е. Оценка корректирующей способности кодов Рида-Соломона при передаче подводных изображений через зашумленный канал связи / Н.Е. Ничипорук, С.В. Сай // Вестник ТОГУ. – 2011. – С. 31-34.
10. Manveer K. Review of various steganalysis techniques / K. Manveer, K. Gagandeep // International journal of computer science and information technologies. – 2014. – Vol. 5. – P. 1744-1747.
11. Deerga Rao K. Channel coding techniques for wireless communications / Rao K. Deerga. – Springer, 2015. – 394 p.
12. Korzhik V. The capacity of a stegosystem for the noisy attack channel / V. Korzhik, G. Morales-Luna, K. Nebaeva // Journal of information hiding and multimedia signal processing. – 2012. – Vol. 3. – No. 2. – P. 205-211.

References

1. Fridrich, J. (2010), *Steganography in digital media: principles, algorithms, and applications*, Cambridge university press, 437 p.
2. Li, M. and Liu, Q. (2015), Steganalysis of SS steganography: hidden data identification and extraction, *Circuits, systems and signal processing*, Vol. 34, No. 10, pp. 3305-3324.
3. Leiman, A.V., Korobeinikov, A.G., Kuvshinov, S.S. and Blinov, S.Yu. (2012), "Analiz principov sozdania i raboti steganograficheskikh algoritmov" [Analysis of the principles for the creation and operation of steganographic algorithms], *Program systems and computational methods. Models and methods of information security management*, Vol. 1, No. 1, NB-Media, Moscow, pp. 28-36. ISSN 2305-6061.
4. Urbanovich, N. and Plaskovitsky, V. (2011), The use of steganographic techniques for protection of intellectual property rights, *New Electrical and Electronic Technologies and their Industrial Implementation*, pp. 147-148.
5. Ryabko, B.Ya. and Fionov, A.N. (2010), "Osnovi sovremenoy kriptografii i steganografii" [Fundamentals of modern cryptography and steganography], Hotline-Telecom, Moscow, 232 p.
6. Zielinska, E., Mazurczyk, W. and Szczypiorski, K. (2014), Trends in steganography, *Communications of the ACM*, Vol. 57, No. 3, pp. 86-95.
7. Starchenko, A.P. (2011), "Metodi vstraivania i identifikatsii skritih vodanih znakov" [Methods for embedding and identifying hidden watermarks], Saint Petersburg, 103 p.
8. Markov, M.V. (2011), "Modeli diskretnih kanalov svyazi" [Models of discrete communication channels], *Service in Russia and abroad*, pp. 143.
9. Nichiporuk, N.E. and Sai, S.V. (2011), "Ocenka korrektyrnoy sposobnosti kodov Reda-Solomona pri peredachi podvodnih izobrazhenii cherez zashymlenii kanal svyazi" [Evaluation of the corrective ability of Reed-Solomon codes when transmitting underwater images through a noisy communication channel], *Bulletin of TOGU*, pp. 31-34.
10. Manveer, K. and Gagandeep, K. (2014), Review of various steganalysis techniques, *International Journal of Computer Science and Information Technologies*, Vol. 5, pp. 1744-1747.
11. Deerga, Rao K. (2015), *Channel coding techniques for wireless communications*, Springer, 394 p.
12. Korzhik, V., Morales-Luna, G. and Nebaeva, K. (2012), The capacity of a stegosystem for the noisy attack channel, *Journal of Information Hiding and Multimedia Signal Processing*, Vol. 3, No. 2, pp. 205-211.

Надійшла до редколегії 09.01.2020

Схвалена до друку 11.02.2020

Відомості про авторів:

Грицюк Владислав Костянтинович
магістр
Харківського національного університету
радіоелектроніки,
Харків, Україна
<https://orcid.org/0000-0001-9342-1872>

Золотарьов Вадим Анатолійович
кандидат технічних наук доцент
Харківського національного університету
радіоелектроніки,
Харків, Україна
<https://orcid.org/0000-0002-6414-755X>

Information about the authors:

Vladyslav Hrytsiuk
Master
of Kharkiv National University
of Radio Electronics,
Kharkiv, Ukraine
<https://orcid.org/0000-0001-9342-1872>

Vadym Zolotaryov
PhD Associate Professor
of Kharkiv National University
of Radio Electronics,
Kharkiv, Ukraine
<https://orcid.org/0000-0002-6414-755X>

СРАВНЕНИЕ СТОЙКОСТИ СТЕГАНОГРАФИЧЕСКИХ МЕТОДОВ КОХО-ЖАХО И DWT[10] К РАЗНЫМ ТИПАМ ИСКАЖЕНИЙ ПРОГРАММНЫМИ СРЕДСТВАМИ

В.К. Грицюк, В.А. Золотарев

Приведены результаты практических исследований по использованию алгоритмов встраивания для сокрытия информации в цифровых видео файлах, полученные с помощью специально разработанной программы на языке Java. Оценена разница между начальным видео со встроенными данными и искаженным видео по показателю индекса структурного сходства индекса структурного сходства SSIM, который считается более точным, чем параметр пикового отношения сигнала к шуму (PSNR), и всегда лежит в диапазоне от -1 до 1. Проанализированы результаты, полученные на трех этапах исследований оценки видео с различными методами встраивания; с различными методами помехоустойчивого кодирования; с различными моделями каналов связи. Оценка устойчивости к помехам в зависимости от выбора стеганографического метода проводилась методами Кохо-Жахо и DWT, использовались два порога встраивания, без помехоустойчивых кодов и без имитации каналов связи. Влияние использования различных методов помехоустойчивого кодирования на устойчивость видео проводилось с помощью кодов Хемминга, БЧХ, РС. Оценка устойчиво-

сти к помехам в зависимости от каналов связи проводилась для 4-х моделей, на которые можно разложить реальный канал связи: канала с простым шумом, канала с черно-белым шумом, канала с аддитивным белым гауссовским шумом и канала с дискретным каналом со стиранием. Опытным путем было выяснено, что разница в устойчивости к помехам для различных стеганографических методов незначительна; увеличение порога встраивания информации приводит к росту устойчивости; усложнения алгоритма кодирования повышает устойчивость как к атакам, так и помехам; обнаружено, что худшим для передачи видео является дискретный канал со стиранием.

Ключевые слова: стеганография, видео, программирование, метод Кохо-Жахо, метод DWT, помехоустойчивые алгоритмы, модели каналов связи, алгоритмы встраивания.

COMPARISON OF THE RESISTANCE OF STEGANOGRAPHIC METHODS OF KOHO-JOA AND DWT [10] TO DIFFERENT TYPES OF CONSTRUCTION BY SOFTWARE TOOLS

V. Hrytsiuk, V. Zolotaryov

The results of practical studies on the use of embedment algorithms for hiding information in digital video files obtained using a specially developed program in Java are presented. The difference between the initial video with embedded data and the distorted video is estimated by the index of structural similarity index of the structural similarity index SSIM, which is considered more accurate than the peak signal-to-noise ratio (PSNR), and always lies in the range from -1 to 1. Videos evaluation results obtained at three stages of research: with various embedding methods; with various error-correcting coding methods; with various models of communication channels analyzed. Evaluation of noise immunity depending on the choice of the steganographic method was carried out by the methods of Koh-Zhao and DWT, two integration thresholds were used, without noise-resistant codes and without simulating communication channels. The influence of using various error-correcting coding methods on video stability was carried out using Hamming, BCH, and RS codes. Evaluation of noise immunity depending on the communication channels was carried out for 4 models into which the real communication channel can be decomposed: a channel with simple noise, a channel with black and white noise, a channel with additive white Gaussian noise, and a channel with a discrete channel with erasure. It was experimentally found that the difference in noise immunity for various steganographic methods is not significant; increasing the threshold for embedding information leads to an increase instability; complications of the encoding algorithm increases resistance to both attacks and interference; found that the worst for video transmission is a discrete channel with erasure.

Keywords: steganography, video, programming, Koh-Zhao method, DWT method, noise-tolerant algorithms, communication channel models, embedding algorithms.