Инвариантный алгоритм сокрытия информации для электротехнических систем

В. Н. Козловский[1], М. В. Шакурский[2]
Самарский государственный технический университет
kozlovskiy-76@mail.ru[1], M.Shakurskiy@gmail.com[2]

А. Ю. Газизулина[3], Н. И. Диденко[4]
Санкт-Петербургский политехнический университет Петра Великого
albinagazizulina@gmail.com[3], didenko.nikolay@mail.ru [4]

С. Б. Крыльцов
Санкт-Петербургский горный университет
kryltcov@outlook.com

Аннотация. **Защита информации играет ключевую роль в современных телекоммуникационных системах. Наиболее распространённым средством обеспечения конфиденциальной передачи информации на сегодняшний день является криптографическое кодирование. На сегодняшний день существует достаточное количество алгоритмов, способных обеспечить высокий уровень защиты информации от прочтения. Однако, злоумышленник может легко разрушить передаваемую информацию, так как её передача осуществляется, как правило, по открытым каналам. В этой ситуации эффективным средством обеспечения защищённой передачи информации является стеганографическое кодирование, так как оно обеспечивает скрытую передачу информации. Сокрытие информации может производится как в осмысленном информационном контейнере, так и в случайном. Использование последнего в значительной степени осложняет процесс декодирования полезной информации принимающей стороной. Одним из эффективных решений задачи декодирования является разработка инвариантных алгоритмов, позволяющих производить процесс декодирования скрытой информации без знания сигнала контейнера. В данной статье рассматривается инвариантный стеганографический алгоритм, построенный на основе контрольного отношения.**

Ключевые слова: стеганография; инвариантное преобразование; маскировка сигнала; случайный сигнал; стеганографический контейнер; декодирование сигнала

I. Введение

Синтез стеганографических систем, в общем случае, преследует своей целью сокрытие секретной информации в контейнере, представляющем собой информацию не несущую интереса для злоумышленника [1]. Существует большое количество разнообразных стеганографических алгоритмов. Оценка стеганографических алгоритмов, является сложной задачей. Это обуславливается количеством разнообразных алгоритмов с одной стороны и неоднозначностью задачи сокрытия с другой. Если вести речь только о незаметности встраивания информации в контейнер, то можно выделить следующие критерии эффективности стеганографических систем:

1. Визуальная незаметность.
2. Статистическая незаметность.
3. Частотная незаметность.

Под визуальной незаметностью подразумевается отсутствие каких-либо артефактов, искажений или шумов, возникающих в результате встраивания информации, которые могут быть замечены системой восприятия человека (зрение или слух, в зависимости от типа контейнера). Первые стеганографические системы опирались только на первый критерий, при этом были крайне уязвимы для других типов атак, в частности статистических. Статистическая незаметность определяется распределением плотности вероятности и математическим ожиданием. Факт встраиванием сигнала в контейнер может быть зафиксирован статистическими методами. В частности, если часть передаваемого сигнала известна, может быть применён корреляционный анализ. Последний критерий подразумевает анализ полосы частот, занимаемой контейнером. При встраивании информации она может исказиться, что позволит сделать вывод о возможности наличия скрытого сигнала в сигнале контейнера.

Злоумышленник, помимо прочтения скрытого сообщения, может попытаться разрушить его, даже не будучи уверен в наличии скрытого сообщения. В этом случае ведётся речь об устойчивости алгоритма к атакам на разрушение скрытого сообщения. Это может быть обнуление наименьших значащих бит, геометрическая трансформация, перекодирование данных из одного формата в другой и пр.

В классической стеганографии подразумевается, что контейнер является осмысленным. Иными словами, контейнер представляет собой какую-либо неслучайную информацию, которая визуально воспринимается как сообщение (речь, изображение и др.) В этом случае

малейшая модификация контейнера может оказаться визуально заметной.

Задача обнаружения скрытой информации осложняется, если контейнер случаен [2–7]. В данном случае контейнером может быть как шумовой сигнал в канале, так и шум в области младших бит изображения или звука. В этом случае статистический анализ шума, а именно он может свидетельствовать о наличии скрытого сообщения, не даст должного результата, а процесс наложения шума со скрытым сигналом может быть реализован с учётом известных стеганографических алгоритмов, учитывающих сжатие контейнера.

В представленной работе рассмотрен инвариантный алгоритм маскировки информации на основе метода контрольной разности.

II. Инвариантность стеганографического алгоритма

Скрытый сигнал декодируется принимающей стороной на основе заранее определённых ключей. При этом контейнер может быть как известным, так и случайным. В случае аддитивного наложения скрываемого сигнала на сигнал контейнера (например, в методе наименьших значащих бит) достаточно знание ключа. Однако в ряде алгоритмов реализовать декодирование при неизвестном контейнере сложно. При использовании случайного маскирующего сигнала задача декодирования может быть решена либо с помощью синхронизированного с передающей стороной генератора случайного сигнала либо с помощью инвариантных алгоритмов – алгоритмов, декодирование в которых возможно без знания маскирующего сигнала [8–10]. Построение таких алгоритмов возможно при наличии достаточной информационной избыточности.

Примем общую форму маскировки полезного сигнала следующего вида:

$$y = au + b\xi + cu\xi \tag{1}$$

где y – сигнал заполненного контейнера; u – маскируемый сигнал; ξ – маскирующий сигнал; a, b, c – коэффициенты преобразования.

Указанное преобразование содержит сумму маскируемого сигнала, с амплитудным коэффициентом a, маскирующего сигнала с амплитудным коэффициентом b и произведения маскирующего и маскируемого сигнала с амплитудным коэффициентом c. Оговоримся, что выражение (1) может быть и другим. В данном случае выбор обусловлен наличием в выражении как аддитивной, так и мультипликативной составляющих маскировки, что делает алгоритм нелинейным, и осложняет обнаружение скрытого сигнала.

Обеспечение в системе сокрытия информации инвариантности к маскирующему сигналу подразумевает, что в качестве маскирующего сигнала может выступать сигнал любой амплитуды, при условии отсутствия потерь в канале передачи информации с одной стороны, и возможность декодирования полезного сигнала принимающей стороной, при условии, что ей не известен маскирующий сигнал. В случае двухкомпонентной системы сокрытия информации максимальное количество неизвестных в передаваемом сигнале равно двум. Рассмотрим способы формирования инвариантных систем сокрытия информации, если за основную модель встраивания взята модель вида (1).

III. Математическая модель

Двухкомпонентная система сокрытия информации, построенная по модели (1) в соответствии с рис. 1.2 имеет следующий вид:

$$\begin{aligned} y_1 &= a_1u_1 + b_1\xi + c_1u_1\xi \\ y_2 &= a_2u_2 + b_2\xi + c_2u_2\xi \end{aligned} \tag{2}$$

где u_1 и u_2 – встраиваемые сигналы, определяемые сигналом u.

Определим необходимое соотношение сигналов u_1 и u_2 с помощью подстановки значения ξ из второго уравнения (2) в первое. Выразим ξ:

$$\xi = \frac{y_2 - a_2u_2}{b_2 + c_2u_2} \tag{3}$$

Подставим (3) в первое уравнение (2) и получим:

$$y_1 = \frac{a_1u_1(b_2 + c_2u_2) + b_1(y_2 - a_2u_2) + c_1u_1(y_2 - a_2u_2)}{b_2 + c_2u_2} \tag{4}$$

Перепишем (4) относительно u_1 и u_2:

$$u_1u_2(a_1c_2 - a_2c_1) + u_1(a_1b_2 + c_1y_2) - u_2(a_2b_1 + c_2y_1) + b_1y_2 - b_2y_1 = 0 \tag{5}$$

Выражение (5) содержит две неизвестных u_1 и u_2 Выбирая соотношение $u_2 = f(u_1)$ на основе условия контрольного отношения получим:

$$\begin{aligned} u_1 &= u \\ u_2 &= u_1 / K \end{aligned} \tag{6}$$

Получим математическую модель (2, 5 и 6) инвариантного двухканального алгоритма сокрытия информации.

Заменим (6) на (5):

$$\begin{aligned} &u_1(u_1 / K)(a_1c_2 - a_2c_1) + u_1(a_1b_2 + c_1y_2) - \\ &(u_1 / K)(a_2b_1 + c_2y_1) + b_1y_2 - b_2y_1 = 0 \end{aligned} \tag{7}$$

Раскроем скобки и запишем полученное выражение относительно u_1:

$$u_1^2\left(\frac{a_1c_2 - a_2c_1}{K}\right) + u_1\left(a_1b_2 + c_1y_2 - \frac{a_2b_1 + c_2y_1}{K}\right) + b_1y_2 - b_2y_1 = 0 \tag{8}$$

Упростим запись выражения (8) объединив константы:

$$u_1^2 C_1 + u_1\left(\frac{c_1 y_2 K - c_2 y_1}{K} + C_2\right) + \left(b_1 y_2 - b_2 y_1\right) = 0 \quad (9)$$

где

$$C_1 = \frac{a_1 c_2 - a_2 c_1}{K}$$
$$C_2 = \frac{a_1 b_2 K - a_2 b_1}{K} \quad (10)$$

Решая уравнение (9) получим следующие корни:

$$u_1 = -\left(2C_1 K\right)^{-1}\left(C_2 K + c_1 y_2 K - c_2 y_1 \pm \sqrt{C_2 K\left(C_2 K + 2K c_1 y_2 - 2c_2 y_1\right) + K^2 c_1^2 y_2^2 + 4C_1 K^2\left(b_2 y_1 - b_1 y_2\right) - 2K c_1 c_2 y_1 y_2 + c_2^2 y_1^2}\right) \quad (11)$$

Уравнение (11) имеет два корня, только один из которых соответствует скрытому сигналу. Если принять условие:

$$a_1 c_2 = a_2 c_1 \quad (12)$$

То выражение (5) примет следующий вид:

$$u_1\left(a_1 b_2 + c_1 y_2\right) - \left(u_1 / K\right)\left(a_2 b_1 + c_2 y_1\right) + b_1 y_2 - b_2 y_1 = 0 \quad (13)$$

Запишем относительно:

$$u_1 = \frac{K\left(b_2 y_1 - b_1 y_2\right)}{K a_1 b_2 - a_2 b_1 + K c_1 y_2 - c_2 y_1} \quad (14)$$

Аналогичным образом получим выражение декодирования относительно u_2:

$$\left(u_2 K\right)\left(a_1 b_2 + c_1 y_2\right) - u_2\left(a_2 b_1 + c_2 y_1\right) + b_1 y_2 - b_2 y_1 = 0 \quad (15)$$

Перепишем относительно u_2

$$u_2 = \frac{b_2 y_1 - b_1 y_2}{K a_1 b_2 - a_2 b_1 + K c_1 y_2 - c_2 y_1} \quad (16)$$

Полученные выражения (14) и (15) позволяют реализовать более простые алгоритмы декодирования и избавится от двузначности, возникающей при решении квадратных уравнений (8) и (9).

IV. Заключение

Полученные в данной статье выражения описывают инвариантный алгоритм сокрытия информации, использующий контрольное отношение. Основным достоинством алгоритма, использующим контрольное отношение, по отношению к алгоритмам, использующим контрольную сумму и контрольную разность, является независимость полос частот занимаемых передаваемыми сигналами от характера контрольного значения.

Исследование математической модели показало, что применение условия (12) позволяет получить инвариантный алгоритм однозначного восстановления информации, скрытой при помощи алгоритма (2).

Численные исследования математических моделей показали, что чувствительность алгоритма к вариации коэффициентов может достигать высоких значений за счёт наличия области разрыва в алгоритме восстановления сигнала.

Список литературы

[1] Fridrich J. (2010) Steganography in digital media. Principles, Algorithms and applications. 437 p.

[2] Cuomo K. M. (1993) Circuit implementation of synchronized chaos with applications to communications. Physical Review Letters. Vol. 71 No. 1, pp. 65-68.

[3] Cuomo K. M. (1994) Communication using synchronized chaotic systems. US Patent No 291555 from 01.03.1994.

[4] Kocarev L. (1992) Experimental demonstration of secure communications via chaotic synchronization. International Journal of Bifurcation and Chaos. Vol. 2, Issue 3, pp. 709-713.

[5] Dedieu H. (1993) Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing. IEEE Transactions on Circuits and Systems-II: Analog and Digital Signal Processing. Vol. 40, No. 10, pp. 634-642.

[6] Parlitz U. (1996) Estimating model parameters from time series by autosynchronization. Physycal Review Letters. Vol. 76, No. 8, pp. 1232-1235.

[7] Dmitriev A.S., Panas A.I., Starkov S.O. (1995) Experiments on speach and music signals transmission using chaos. International Journal of Bifurcation and Chaos. Vol. 5, Issue 4. (http://dx.doi.org/10.1142/S0218127495000910).

[8] Shakurskiy M.V., Shakurskiy V.K., Volovach V.I. (2014) Two-channel real-time steganographic system. Proceedings of IEEE East-West Design & Test Symposium (EWDTS'2014) pp. 309-311.

[9] Shakurskiy M.V., Shakurskiy V.K., Volovach V.I. (2015) Computer model of steganographic system based on contraction mapping with stream audio container. Proceedings of IEEE East-West Design & Test Symposium (EWDTS'2015), pp. 306-309.

[10] Shakurskiy V.K., Shakurskiy M.V. (2014) Contraction mapping in invariant transformers and steganographic systems. Transl. – Samara: SSC RAS p. 159.

[11] Konoplev, A.S., & Busygin, A.G. (2015). Steganographic methods of communications in distributed computing networks. Paper presented at the ACM International Conference Proceeding Series, , 08-10-Sep-2015. doi:10.1145/2799979.2800024

[12] Bozhokin, S.V., Zharko, S.V., Larionov, N.V., Litvinov, A.N., & Sokolov, I.M. (2017). Wavelet correlations of nonstationary signals. Technical Physics, 62(6), 837-845. doi:10.1134/S1063784217060068

[13] Stankevich, L., & Sonkin, K. (2016). Human-robot interaction using brain-computer interface based on EEG signal decoding. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 9812, 99-106. doi:10.1007/978-3-319-43955-6_13

[14] Sonkin, K., Stankevich, L., Khomenko, Y., Nagornova, Z., Shemyakina, N., Koval, A., & Perets, D. (2016). Neurological classifier committee based on artificial neural networks and support vector machine for single-trial EEG signal decoding. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 9719, 100-107. doi: 10.1007/978-3-319-40663-3_12

[15] Klochkov, Y., Odinokov, S., Klochkova, E., Ostapenko, M., & Volgina, A. (2016). Development of certification model. Paper presented at the 2016 5th International Conference on Reliability, Infocom Technologies and Optimization, ICRITO 2016: Trends and Future Directions, 120-122. doi:10.1109/ICRITO.2016.7784937

[16] Klochkov, Y., Papic, L., & Butkevich, R. (2017). Development of the standardization system in an organization. International Journal of Reliability, Quality and Safety Engineering, 24(6), Article number 1740004. doi:10.1142/S0218539317400046

[17] Klochkov, Y., Klochkova, E., Antipova, O., Kiyatkina, E., Vasilieva, I., & Knyazkina, E. (2016). Model of database design in the conditions of limited resources. Paper presented at the 2016 5th International Conference on Reliability, Infocom Technologies and Optimization, ICRITO 2016: Trends and Future Directions, 64-66. doi:10.1109/ICRITO.2016.778492

[18] Yury, K., Lera, G., Elena, K., Irina, V., & Sergey, D. (2016). Consideration of uncertainties and risks in the building process of multifunctional harbor transshipment complex. International Journal of Reliability, Quality and Safety Engineering, 23(6), Article number 1640011. doi:10.1142/S0218539316400118

[19] Klochkov, Y., Gazizulina, A., & Golovin, N. (2016). Assessment of organization development speed based on the analysis of standards efficiency. Paper presented at the Proceedings - 2nd International Symposium on Stochastic Models in Reliability Engineering, Life Science, and Operations Management, SMRLO 2016, 530-532. doi:10.1109/SMRLO.2016.93

[20] Atroshenko, S.A., Korolyov, I.A., & Didenko, N. (2016). Evaluation of physico-mechanical properties of high-chromium tool steels modified with harrington method. Materials Physics and Mechanics, 26(1), 26-29.

[21] Romashkina, G.F., Didenko, N.I., & Skripnuk, D.F. (2017). Socioeconomic modernization of russia and its arctic regions. Studies on Russian Economic Development, 28(1), 22-30. doi:10.1134/S1075700717010105

[22] Didenko, N., Kunze, K., & Skripnuk, D. (2015). Russian export strategy and social sector: Consequences of resource-oriented exports on population of russia. Mediterranean Journal of Social Sciences, 6(5S2), 473-481. doi:10.5901/mjss.2015.v6n5s2p473