Метод сокрытия информации в графоподобных структурах социальной сети

И. В. Нечта
Сибирский государственный университет телекоммуникаций и информатики,
Новосибирск, Россия
Контактный e-mail: ivannechta@gmail.com

Предложен новый метод передачи скрытых сообщений в социальных сетях на примере сети "Вконтакте", позволяющий через структуру графа друзей пользователя внедрять секретные сообщения. Получены количественные оценки объема внедряемого сообщения в графы различного размера. Показана необходимость добавления избыточности во внедряемое сообщение. Представленный метод позволяет использовать другие графоподобные структуры социальной сети для внедрения скрытых сообщений.

Ключевые слова: стеганография, безопасность в социальных сетях, структурная стеганография.

Введение

Одним из направлений науки, связанных с обеспечением информационной безопасности, является стеганография. Классическая задача стеганографии сформулирована в работе Симмонса [1] следующим образом. Пусть имеются два участника обмена сообщениями: Алиса и Боб. Их задача заключается в создании потайного канала связи для передачи секретных сообщений. Имеется сторонний наблюдатель Ева, задача которой состоит в выявлении самого факта существования тайного канала связи.

Вначале Алиса встраивает секретное сообщение в безобидный на первый взгляд объект данных — так называемый контейнер. Затем заполненный контейнер передается Бобу по открытому каналу связи. Сам факт передачи сообщений по открытому каналу связи не является подозрительным для Евы. Считается, что сообщение предварительно зашифровано ключом, который доступен только Алисе и Бобу, о котором они договариваются заранее. Исходя из принципа Кирхгофа [2], Ева может знать о том, каким методом внедрения могли пользоваться Алиса и Боб, но, даже подвергнув перехваченный контейнер анализу, она не сможет однозначно утверждать наличие факта внедрения. Таким образом, скрытность передачи обеспечивается особенностями метода внедрения и секретным ключом шифрования, недоступным Еве.

В стеганографии также существует обратная задача. В приведенном примере Ева занимается выявлением факта передачи секретного сообщения, т. е. стегоанализом. При проведении стегоанализа Ева может использовать статистические различия между заполненным контейнером (с секретным сообщением) и пустым. Эффективность методов стегоанализа определяется ошибками. Ошибка первого рода — случай, когда заполненный контейнер воспринимается как пустой, ошибка второго рода — случай, когда

пустой контейнер воспринимается как заполненный. Часто для оценки эффективности метода используется среднее арифметическое указанных ошибок.

Методы стеганографии позволяют встраивать скрытую информацию в различные цифровые контейнеры. Например, метод LSB-внедрения предусматривает запись секретного сообщения в последний значащий бит в цвете пикселя изображения. Известны методы [3], модифицирующие дискретные косинусные коэффициенты изображения при внедрении в файлы JPG-формата. Внедрение в текстовый контейнер (например, методом использования синонимов [4]) изменяет в предложениях слова на эквивалентные им синонимы в соответствии со скрываемым сообщением. Существует ряд методов [5–8], скрывающих секретное сообщение в сгенерированном естественноподобном тексте. В настоящий момент актуальной задачей является создание как новых методов внедрения в различные типы контейнеров (файловые системы, сетевой трафик, программные приложения и т. д.), так и точных методов стегоанализа.

Внедряемое сообщение может использоваться для различных целей. Так как цифровые отпечатки пальцев предназначены для идентификации пользователя цифрового объекта данных, в каждую продаваемую копию программы автор может встраивать секретное сообщение, которое идентифицирует покупателя лицензии. При обнаружении пиратской копии программы автор без труда извлекает секретное сообщение и устанавливает лицо, создавшее нелицензионную копию продукта.

Для защиты объектов авторского права также используются цифровые водяные знаки. Существуют устойчивые (робастные) водяные знаки, которые активно применяются для доказательства авторских прав на цифровой объект данных. Например, автор обнаруживает, что его изображение используется сторонним лицом без соответствующего на то разрешения. В этом случае водяной знак может быть извлечен и использован в качестве доказательства авторства в судебном порядке. Очевидно, что такой водяной знак должен обладать некоторой степенью устойчивости, чтобы его удаление или искажение посторонним лицом представляло значительные трудности. Используются также хрупкие водяные знаки, которые разрушаются при малейших или определенных (условно хрупкие) изменениях контейнера. Такие водяные знаки широко применяются для контроля целостности цифрового объекта.

Стегоанализ применяется для установления скрытых каналов передачи данных, например выявления утечки коммерческой информации. Существуют также задачи противодействия различным сообществам [9], члены которых могут тайно обмениваться информацией в социальных сетях или чатах под видом обычного общения.

Известные в настоящий момент методы стеганографии, которые активно применяются в социальных сетях [10], предполагают использование классической текстовой стеганографии для встраивания информации в сообщения, передаваемые между пользователями, или других методов внедрения в различные типы данных, например в опубликованные фотографии пользователя. В работах [11–13] решаются задачи выявления определенных лиц в анонимных социальных сетях.

В данной работе описан новый метод, позволяющий организовать передачу секретных сообщений в социальных сетях. Предлагается использовать функцию “Добавление друзей” для внедрения скрытых данных. В качестве примера рассматривается популярная сеть “Вконтакте”. Результаты проведенного эксперимента показали, что указанный метод стеганографии позволяет встраивать большой объем информации в различные структуры социальной сети, представляемые в виде графа.

1. Описание метода

Предлагается использовать графы, имеющиеся в социальной сети, для внедрения сообщения. Например, функция добавления в друзья позволяет установить связь между контактами пользователей социальной сети. Контакт пользователя, определяемый идентификатором, соответствует узлам графа, а его связи с друзьями в сети — ребрам. Стоит отметить, что подобный граф является неориентированным, что в данном случае уменьшает объем внедрения. Очевидно, что для построения графа можно использовать и другие функции социальной сети, например установление отметки "Like" на фотографиях. Для удобства проведения эксперимента выбрана сеть "Вконтакте" и рассмотрен случай с добавлением друзей.

Для внедрения сообщения Алиса выполняет следующие шаги:

1) шифрование секретного сообщения;
2) добавление избыточности в сообщение;
3) регистрация новых аккаунтов;
4) установление связей (построение графа).

Шифрование и добавление избыточности производится по заранее согласованным с Бобом алгоритмам. Предполагается, что ключи шифрования переданы заранее. Добавление избыточности необходимо для достижения неразличимости статистических свойств зашифрованного сообщения и сообщения, взятого из пустого контейнера. Необходимость избыточности экспериментально показана в следующем разделе.

Регистрация новых аккаунтов и установление связей производятся в соответствии с внедряемым сообщением. Количество необходимых аккаунтов определяется в ходе эксперимента. В случае, когда под Алисой выступает некоторое сообщество, возможна передача доступа к аккаунтам некоторому координатору, который по своему усмотрению будет ими управлять. Сеть "Вконтакте" позволяет регистрировать новый аккаунт через подтверждающий СМС-код, причем допускается регистрация нескольких аккаунтов на один телефонный номер. Такая схема регистрации позволяет автоматически создавать множество новых аккаунтов при помощи специального программного обеспечения. Добавление друзей "Вконтакте" также можно осуществлять программно, при помощи сервиса API. Таким образом, создание графа (задача Алисы) может выполнять один человек.

Рассмотрим процесс внедрения информации в граф. Исходный граф состоит из двух подграфов: основного G и ключевого K. Пусть имеется основной неориентированный подграф $G(V, E, \varphi)$, где V — множество вершин подграфа, E — множество ребер, а φ — функция смежности, определяющая наличие ребра между вершинами V_a и V_b подграфа G:

$$\varphi(a,b) = \begin{cases} 1, & E_{a,b} \in E, \\ 0, & E_{a,b} \notin E. \end{cases} \tag{1}$$

Пронумеруем все возможные упорядоченные пары вершин подграфа (V_a, V_b), где $a < b$. Количество таких пар составит

$$N = \frac{|V| \cdot (|V| - 1)}{2}.$$

Таким образом, внедренное сообщение $M = \{m_1, m_2, ..., m_N\}$, содержащее N бит, определяется функцией смежности $m_i = \varphi_i$ для соответствующей i-й пары вершин.

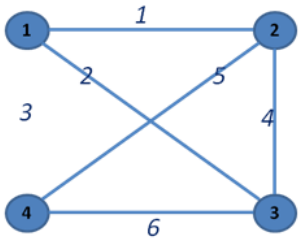

Рис. 1. Пример внедрения сообщения в подграф G

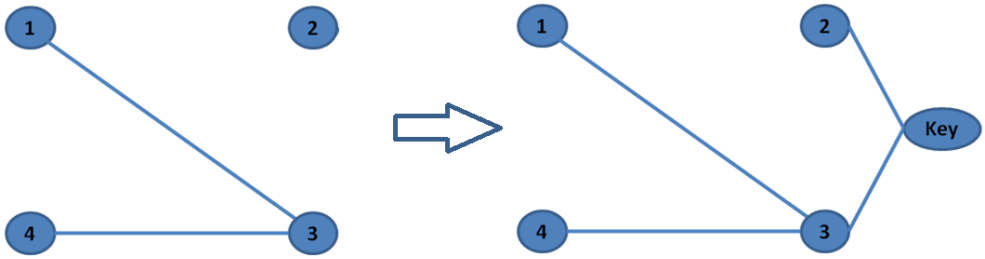

Рис. 2. Пример использования ключевой вершины Key для передачи графа

В программной реализации, выполненной в ходе данного исследования, нумеруются все ребра первого узла, затем ребра второго узла и т. д. На рис. 1 представлен подграф G, в котором нет ребра между вершинами *1* и *4* (что соответствует ребру *3*), в таком случае передаваемым сообщением является последовательность 110111.

В общем случае ключевой подграф K состоит из одной вершины и не менее чем из одного ребра. Данный подграф применяется для решения таких задач, как:

- передача исходного графа от Алисы к Бобу;
- привязка к графу всех его вершин, в том числе изолированных.

Алиса и Боб предварительно договариваются не только о ключе шифрования сообщения (как в классической схеме Симмонса), но и о ключевом аккаунте, с помощью которого Боб будет выходить на остальные узлы графа. То есть в список друзей ключевого аккаунта входят все несвязанные аккаунты и хотя бы один произвольный аккаунт из связанной группы, чтобы через него выйти на остальных друзей. Исходный граф (с ключевым подграфом) всегда имеет один компонент связности. Предполагается, что граф не имеет связей с другими аккаунтами социальной сети, не относящимися к передаче секретного сообщения.

После получения графа Бобом ключевой подграф отбрасывается и в дальнейшем не используется. На рис. 2 показан основной подграф из четырех узлов, причем вершина *2* изолирована. С помощью добавленного ключевого узла (Key) и ребер Боб сможет найти все четыре вершины, составляющие основной подграф.

Таким образом, Боб сможет найти в социальной сети искомый граф по ключевому аккаунту и за счет связности графа учесть все его вершины.

2. Проведение экспериментального анализа

В рамках данного исследования необходимо предлагаемым методом установить количественную оценку объема внедрения. Объем, равный $(n(n-1))/2$, где n — количество вершин основного подграфа, является верхним пределом и не может быть достигнут

из-за различий статистических свойств внедряемого сообщения и сообщения, взятого из пустого контейнера.

Одно из требований, предъявляемых к современным шифрам, — статистическая неразличимость зашифрованной и истинно случайной последовательностей. В работе [14] показано, что внедряемое сообщение (которое предварительно зашифровано) нарушает статистическую структуру контейнера, повышая его энтропию. В ряде работ, например в [15], предлагалось использовать добавление избыточности для "выравнивания" статистических свойств. С одной стороны, это повышает устойчивость к статистическому стегоанализу, но, с другой стороны, объем внедрения в контейнер уменьшается. Далее мы рассмотрим статистические свойства сообщения, взятого из пустого контейнера, и рассчитаем объем внедрения без учета избыточности.

В ходе работы создано программное обеспечение, позволяющее извлекать сообщения из графов друзей социальной сети "Вконтакте". Для эксперимента был взят произвольный аккаунт. Количество друзей как первого поколения (друзья исходного аккаунта), так и второго поколения (друзья друзей исходного аккаунта) ограничивалось некоторым числом Limit $\in [2; 9]$. Ограничение вводилось затем, чтобы уменьшить размер анализируемого графа, в противном случае граф мог содержать миллионы пользователей, так как социальные связи весьма обширны. Доступ к базе данных "Вконтакте" осуществлялся через API (GET-запросы), результат возвращался в XML-формате и затем анализировался.

Пусть H — энтропия по Шеннону [16], являющаяся мерой неопределенности сообщения и численно равная количеству информации на символ сообщения. Ограничимся простым анализом энтропии сообщения, состоящего из символов алфавита $A = \{0, 1\}$. Не исключено, что анализируемые сообщения содержат в себе другие закономерности, отличающие их от зашифрованного сообщения (в котором биты 0 и 1 равновероятны и между их появлением отсутствуют какие-либо закономерности).

$$H = -(p_0 \cdot \log_2 p_0 + p_1 \cdot \log_2 p_1). \tag{2}$$

Здесь p_0 и p_1 — вероятности появления 0 и 1 бит в сообщении соответственно. Введем обозначения: V — число узлов графа (без ключевого), L — длина извлеченного из графа сообщения.

Из таблицы видно, что извлеченное сообщение существенно отличается от внедряемого зашифрованного сообщения (у которого $H \to 1$). В таблице указана энтропия на один бит сообщения. Из работ Шеннона известно, что энтропия численно равна количеству информации, содержащейся в сообщении. Соответственно, количество бит

Результаты анализа сообщения графа, извлеченного из социальной сети

Limit	V	L, бит	H	L_{sec}, бит
2	6	15	0.97	14
3	11	55	0.76	41
4	17	136	0.58	79
5	25	300	0.46	137
6	39	741	0.31	232
7	50	1225	0.27	328
8	66	2145	0.21	454
9	83	3403	0.18	599

информации, которые можно безопасно передать с помощью L битов, будем вычислять по формуле

$$L_{sec} = \lfloor H \cdot L \rfloor. \tag{3}$$

В таблице представлены полученные результаты извлечения и анализа сообщения из графа сети “Вконтакте” (т. е. сообщения из пустого контейнера). Здесь объем внедрения показан в колонке L, безопасный объем внедрения — в колонке L_{sec}.

Заключение

Предложен новый метод внедрения скрытых сообщений в графоподобные структуры социальных сетей. Рассмотрен пример встраивания скрытых сообщений при помощи функции добавления друзей сети “Вконтакте”. Оценивается безопасность внедрения относительно известного подхода к стегоанализу, когда выявляются различия в распределении вероятностей бит извлеченного из контейнера сообщения до и после его заполнения. В ходе экспериментальных исследований получены количественные оценки безопасного объема внедрения. Показана необходимость добавления избыточности во внедряемое сообщение.

Недостатком предложенного метода следует считать шаг регистрации новых аккаунтов. В социальных сетях в целях безопасности могут использоваться ограничения на автоматическую регистрацию новых аккаунтов. В рассмотренном примере сеть “Вконтакте” не использует ограничения на регистрацию. Однако данная проблема потенциально может замедлить процесс внедрения сообщений.

Список литературы / References

[1] **Simmons, G.J.** The prisoners problem and the subliminal channel. Advances in Cryptology. Boston, 1984. P. 51–67.

[2] **Kerckhoffs, A.** La cryptographie militaire // J. des Sciences Militaires. 1893. Vol. 9. P. 5–83.

[3] **Rabie, T., Kamel, I.** High-capacity steganography: a global-adaptive-region discrete cosine transform approach // Multimedia Tools and Applications. 2017. Vol. 76, No. 5. P. 6473–6493.

[4] **Winstein, K.** Tyrannosaurus lex 1999. Available at: http://web.mit.edu/keithw/tlex/ (accessed 14.01.2018).

[5] **James, C.** Steganography: Past, Present, Future. Available at: http://www.sans.org/reading_room/whitepapers/steganography/steganography_past_present_future_552 (accessed 11.12.2016).

[6] **Bennett, K.** Linguistic steganography: Survey, analysis, and robustness concerns for hiding information in text. Available at: http://www.cerias.purdue.edu/apps/reports_and_papers/view/2697 (accessed 15.03.2018).

[7] **Topkara, M.** Natural language watermarking // Proc. of SPIE Intern. Conf. on Security, Steganography, and Watermarking of Multimedia Contents. Bellingham, WA USA: SPIE, 2005. P. 441–452.

[8] **Chapman, M., Davida, G.** Hiding the hidden: A software system for concealing cipher text in innocuous text // Proc. of the Intern. Conf. on Inform. and Communications Security: Lecture Notes in Comput. Sci. 1997. Vol. 1334. P. 333–345.

[9] **Engel, P.** ISIS has figured out ways to get around restrictions on one of the main apps it uses for propaganda. Available at: http://www.businessinsider.com/isis-telegram-channels-2015-11 (accessed 11.12.2016).

[10] **Guha, S., Tang, K., Francis, P.** NOYB: Privacy in online social networks // Proc. of the First Works. on Online Social Networks. San Diego, CA, USA, November 08–12, 2008. P. 49–54.

[11] **Nilizadeh, S., Kapadia, A., Ahn, Y.Y.** Community-enhanced de-anonymization of online social networks // Proc. of the 2014 ACM SIGSAC Conf. on Computer and Communications Security. Scottsdale, AZ, USA, November 03–07, 2014. P. 537–548.

[12] **Sharad, K.** True friends let you down: Benchmarking social graph anonymization schemes // Proc. of the 2016 ACM Works. on Artificial Intelligence and Security. Vienna, Austria, October 24–28, 2016. P. 93–104.

[13] **Diwakar, A.K., Singh, N.K., Tomar, D.S.** End user privacy preservation in social networks against neighborhood attack // Asia Security and Privacy (ISEASP), 2017. Surat, India: IEEE, 2017. P. 1–9.

[14] **Zhilkin, M., Melentsova, N., Ryabko, B.** Data compression based method of revealing hidden information in steganographic systems // Proc. of XI Intern. Symp. on Probl. of Redundancy in Information and Control Systems, Saint-Petersburg, 2007. P. 42–44.

[15] **Нечта И.В.** Метод внедрения скрытых сообщений в исполняемые файлы // Вестник СибГУТИ. 2011. № 2. С. 3–10.
Nechta, I.V. Method of secret messages embedding into executable files // Vestnik SibSUTI. 2011. Vol. 2. P. 3–10. (In Russ.)

[16] **Shannon, C.E.** A mathematical theory of communication // Bell System Technical J. 1948. Vol. 27(3). P. 379–423.

Поступила в редакцию 10 июня 2017 г.,
с доработки — 15 января 2018 г.

A method of hidden messages embedding in graphlike structures of a social network

Nechta, Ivan V.

Siberian State University of Telecommunications and Information Sciences, Novosibirsk, 630102, Russia,

Corresponding author: Nechta, Ivan V., e-mail: ivannechta@gmail.com

Purpose. This article addresses the construction of a new method for transmission of hidden messages in social networks.

Methodology. The research employs methods of information theory, probability theory and mathematical statistics The Shannon entropy is used as the statistics for the analysis of an embedded message.

Findings. The author proposed using the graphical structures of social networks as a container for the secret message transmission for the first time. As an example, the popular Vkontakte network is considered. The main idea of the method involves using the structure of the user's friends graph to embed a secret message. Based on the available vertices (friends' accounts), a complete graph is constructed, and its edges

are enumerated. Each edge of the graph corresponds to one bit of the message being embedded: the bit is "1", if the edge is present in the graph (one account in friends of the other), the bit is "0" if the edge is missing.

To transfer the graph from one person to another, a key vertex is used. The specified vertex is connected by an edge with each connected component of the graph, which allows the graph to be transmitted using a single node and take into account all the vertices (including isolated ones). When retrieving a message, the key vertex and the edges connected to it are not considered.

Conclusions. During the experimental research, it was shown that messages extracted from an empty container differ from the encrypted message by the probability distribution of bits. The necessity of adding redundancy to transmitted secret messages is shown with the purpose of "leveling" the statistical properties of an empty and filled container. The results of the experiment have showed that this method of steganography allows embedding a large amount of information into various social network structures represented in the form of a graph. It was noted in the paper that potentially "narrow" place of the algorithm is registration of new accounts. The restrictions imposed by the administration of some social networks for security purposes do not always allow automatic registration of new accounts, which makes the process of message embedding more difficult.

Keywords: steganography, security in social networks, structural steganography.

Received 10 June 2017
Received in revised form 15 January 2018