ULUSLARARASI 3B YAZICI TEKNOLOJİLERİ
VE DİJİTAL ENDÜSTRİ DERGİSİ

INTERNATIONAL JOURNAL OF 3D PRINTING TECHNOLOGIES AND DIGITAL INDUSTRY

ISSN:2602-3350 (Online)

URL: https://dergipark.org.tr/ij3dptdi

ПРИНЦИПЫ ВЫБОРА КОНТЕЙНЕРОВ ДЛЯ СТЕГАНОГРАФИЧЕСКИХ СИСТЕМ

PRINCIPLES OF CHOOSING CONTAINERS FOR STEGANOGRAPHIC SYSTEMS

Yazarlar (Authors): Esmira Mustafayeva *

Bu makaleye şu şekilde atıfta bulunabilirsiniz (To cite to this article): *Mustafayeva E. "Principles Of Choosing Containers For Steganographic Systems" Int. J. of 3D Printing Tech. Dig. Ind., 4(3): 264-229, (2020).*

DOI:10.46519/ij3dptdi.799590

Derleme Makale/ Review Article

Erişim Linki: (To link to this article): https://dergipark.org.tr/en/pub/ij3dptdi/archive

ПРИНЦИПЫ ВЫБОРА КОНТЕЙНЕРОВ ДЛЯ СТЕГАНОГРАФИЧЕСКИХ СИСТЕМ

Esmira Mustafayeva [a]*

[a] Институт Систем Управления Национальной Академии Наук Азербайджана

[*] *Автор-корреспондент:* mustafayevaesmira73@gmail.com

(**Received:** 24.09.2020; **Revised:** 15.10.2020; **Accepted:** 04.11.2020)

АННОТАЦИЯ

В статье рассмотрены общие принципы выбора контейнеров для создания совершенных стеганографических систем, а также характеристики, типы, объем, размер, формат, стойкость контейнеров к атакам. Описан процесс внесения информации в контейнер, проведен анализ устойчивости стеганограмм при пассивным и активным атакам. Было отмечено отличительные аспекты форматов современных графических контейнеров, преимущество и недастатки используемых интернет протоколов TCP, IP, VoIP и SCTP в качестве контейнера. Для определения влияния контейнеров на стеганографическую стойкость рассмотрен теоретико-информационную модель стеганографической системы с пассивным нарушителем. Изложена зависимость стойкости стеганографических систем от технологии внедрения скрытых сообщений в контейнер, проанализировано вероятностное распределение контейнеров и стеганограмм. Было показано, что стойкость стеганографических систем зависит от вероятностного распределения контейнеров и стеганограмм и только при их равенство стеганографическая система является совершенно стойкой.

Ключевые слова: стеганографическая система, сокрытие информации, контейнер, стеганограмма, конфиденциальная информация, нарушитель, атака.

PRINCIPLES OF CHOOSING CONTAINERS FOR STEGANOGRAPHIC SYSTEMS

ABSTRACT

In this study, the general principles of choosing containers to create perfect steganographic systems, as well as the characteristics, types, volume, size, format, stability of containers against attacks are considered. The process of entering information into a container is described, and the stability of steganograms with respect to passive and active attacks is analyzed. The distinguishing aspects of the formats of modern graphic containers, the advantage and disadvantages of the Internet protocols TCP, IP, VoIP and SCTP which are used as containers are discussed. To determine the effect of containers on steganographic stability, a theoretical information model of steganographic system with a passive intruder has been suggested. The dependence of the stability of steganographic systems on the technology of introducing hidden messages into a container is explained and the probability distributions of containers and steganograms are analyzed. It was shown that the stability of steganographic systems depends on the probability distributions of containers and steganograms, and only in the case they are identically distributed, the steganographic system is completely stable.

Keywords: steganographic system, information hiding, container, steganogram, confidential information, intruder, attack.

1. ВВЕДЕНИЕ

Чтобы защитить информации от несанкционированного доступа с древних времен, люди стали разрабатывать и внедрять методов и средств сокрытия информации от посторонних лиц. Среди таких методов и средств особое место занимали методы стеганографического скрытия информации. Процесс стеганографического сокрытия информации осуществляется различными способами, резко отличающиеся друг от друга. Однако эти методы имеют и общие свойства. Так как, скрываемое сообщение специальным образом внедряется некоторый не привлекающий внимание объект, а затем этот объект отправляется по открытому каналу в адрес назначения или хранится для дальнейшего использования.

Применение таких методов в первую очередь требует решение вопроса о стойкости стеганографических систем. Стойкость стеганографической системы, то есть устойчивость передаваемой по секретному каналу стеганограммы к обнаружению противником, в значительной степени зависит от правильного выбора контейнера, в котором будет сокрыта конфиденциальная информации. Следовательно, формат, назначение, источник и принципы выбора контейнеров играют важную роль в создании устойчивых стеганографических систем.

2. КОНТЕЙНЕРЫ В СТЕГАНОГРАФИЧЕСКИХ СИСТЕМАХ И ИХ ТИПЫ

Под контейнером понимается объект открытого характера, используемый для сокрытия конфиденциальной информации. В качестве контейнера может выступить любой материальный объект, носитель информации, информационный ресурс, текст, изображение, файл и т. д. Для внедрения информацию в контейнер в зависимости от его формата разрабатываются более стойкие стеганографические методы или из существующих методов выбираются более подходящие. Эффективность методов сокрытия информации зависит от назначения, структуры и типа контейнеров. Стеганографические методы разрабатываются на основе характеристик форматов и структур контейнеров. Так как, в структуре контейнера должно существовать избыточность, допускающая внедрять дополнительное сообщение большого объема или контейнер должен позволять осуществлении определенные изменения в ее содержании, которые не могут быть легко обнаружены.

Естественно, скрыть конфиденциальную информацию в другой открытой информации с большим объемом проще и надежнее. Поэтому современные стеганографические методы, как правило, основываются на принципах сокрытия конфиденциальной информации в другой намного объемной информации совершенно другого содержания и смысла.
Отметим, что многие специалисты считают более подходящим назвать объект с внедренной конфиденциальной информацией «носителем», однако во многих научных источниках такие объекты называются «контейнером». По причине популярности термин «контейнер» был принять как всеобщий термин [1].

В зависимости от принципов внедрения конфиденциальной информации, контейнеры делятся на две категории: потоковые и фиксированные контейнеры [2,3]. Потоковые контейнеры состоят из последовательности непрерывно поступающих битов. Так как, конфиденциальная информация внедряется в контейнер по поступлению в реальном времени, то объем контейнера, необходимого для передачи полной информации, заранее неизвестен кодеру. А в большой контейнер можно разместить нескольких сообщений. Интервалы между добавленными (или измененными) битами определяются генератором регулярно распределенных псевдослучайных последовательностей.

При этом основная трудность заключается в осуществлении синхронизации между отправителем и получателем, а также в определении при этом начала и конца последовательности. Если в данных контейнера существуют биты синхронизации, заголовки пакетов и т. д., то конфиденциальная информация может следовать после них. Сложность организации синхронизации имеет большое значение с точки зрения обеспечения секретности передачи. В качестве примера потоковых контейнеров можно указать узла стегоприставки, подсоединенного к обычному телефону. Под прикрытием обычного телефонного разговора, с помощью такого

телефонного узла может быть отправлен другой разговор, конфиденциальная информация и т.д. При этом не зная секретного ключа невозможно определить не только содержание скрытой передачи, а также самого факта передачи.
Понятно, что размеры и особенности фиксированных контейнеров заранее известны, а это позволяет скрывать в них данные соответствующим (оптимальным) образом. В дальнейшем, под контейнером будем подразумевать фиксированный контейнер. Контейнеры могут быть избранными, случайными или навязанными. Избранный контейнер зависит от характера встраиваемой информации или от ее назначения. Случайные контейнеры широко и свободно используется в повседневной деятельности, включая компьютерных технологиях, Интернет и т. д. В большинстве случаев, в практике используются такие контейнеры. Навязанный контейнер это такой контейнер, который навязывается отправителю в случае, когда злоумышленник (нарушитель) подозревает о возможности скрытого обмена конфиденциальной информацией между сторонами.

3. ПРОЦЕСС ВНЕДРЕНИЯ КОНФИДЕНЦИАЛЬНЫХ ИНФОРМАЦИЙ В КОНТЕЙНЕР

Для того, чтобы более надежно скрыть конфиденциальную информацию в контейнере его объем должен быть намного больше, чем объем скрываемой информации. В обратном случае, когда объем скрываемая сообщения превышает объем контейнера, выдвигается существенные требование к контейнеру. Для этого перед внесением конфиденциальную информацию в контейнер, необходимо осуществить ее сжатие, чтобы существенно уменьшить объем. Кроме того, для более надежной защиты содержания конфиденциальной информации в случае обнаружения ее в контейнере, рекомендуется заранее зашифровать ее с помощью некоторого криптографического алгоритма [3,4].

В процессе передачи объем, размер, формат и другие характеристики графических, аудио, видео и т.д. контейнеров могут модифицироваться. С целью устранения такого недостатка применяются методы обеспечения целостности передаваемого контейнера (в том числе встроенной информации) путем использования кодов исправления ошибок (помехоустойчивого кодирования). Следует отметить, что для надежной защиты скрываемой информации начальная обработка часто выполняется с использованием специального ключа.

Процесс внесения информации в контейнер выполняется с помощью стеганокодера путем изменения формата или незначительной модификации содержания, а это определяется используемым стеганографическим методом. После внедрения информации, модифицированный контейнер отправляется получателю через открытый канал связи [2,3]. Понятно, что во время передачи по каналам связи стеганограмма может подвергаться пассивным или активным атакам со стороны нарушителя. При пассивной атаке нарушитель для выявления факта существования скрытой информации перехватывает всевозможные контейнеры, отправляемые по каналам связи, далее сначала по отдельности, а потом в комплексе анализирует их. После правильного определения факта существования скрытой информации нарушитель старается извлечь ее из контейнера. При этом нарушитель должен дополнительно взломать шифр, если скрываемая информация заранее зашифрована. Если пассивный нарушитель не может определить факт существования скрытой информации, то естественно невозможно и ее извлечение.

Таким образом, при пассивной атаке контейнер не подвергается изменению. А при активной атаке нарушитель либо модифицирует, либо уничтожает контейнер. Активно атакующий нарушитель может изменять контейнер, передаваемый по каналу связи, таким образом, что ни отправитель и ни получатель не подозревали об этом. При этом нарушитель или уничтожает скрываемую информацию, или внося в нее существенные изменения, создает поддельную стеганограмму. При этом, чтобы модифицировать или уничтожать скрываемую информацию он должен сначала анализировать контейнеры, передаваемые по каналу связи [3].

4. МЕТОДЫ ВЫБОРА КОНТЕЙНЕРОВ В КОМПЬЮТЕРНОЙ СТЕГАНОГРАФИИ

Очевидно, что контейнер, не вызывающий сомнений в процессе передачи, считается лучшим контейнером. Поэтому при выборе форматов графических изображений, представленных в качестве контейнера, недостаточно требовать только стойкости стеганографических систем к атакам. В то же время этот формат должен быть достаточно распространенным и широко используемым в практике. В последнее время наиболее распространенным форматом является растровый формат JPEG. Почти все современные цифровые фотоаппараты и видеокамеры изображения сохраняют в этом формате. Формат большинства встречаемых в Интернете графических изображений также является JPEG. Исходя из сказанных, можно делать вывод о том, что использование графических изображений формата JPEG является более подходящим.
Вообще, важно отметить следующие отличительные аспекты форматов современных графических контейнеров с точки зрения построения стеганографических систем [1]:

- существование данных в сжатом форме;
- данные не подвергаются потерям при сжатии;
- использование форматов палитры цветов.

Если формат хранения растровых изображений использует сжатие данных, то разработка стеганографических систем становится значительно сложным. Во-первых, сложность анализа формата увеличивается, а во-вторых, внесение сообщения в данные изображения приводит к нежелательному ухудшению эффективности сжатия. Когда формат графического изображения использует сжатия с потерями данных, тогда классические методы сокрытия информации в графических изображениях становится малоэффективными. Другими словами, такая потеря может привести к уничтожению скрываемой информации. Использование хранения формата графических изображений в цветовых палитрах затрудняет применение классических методов сокрытия.

Как отмечено, стеганографические методы сокрытия информации в пространственной области изображения являются неустойчивыми к большинству видов искажений. Например, использование процедур сжатия с потерями могут привести к частичному или полному уничтожению скрываемой информации. Более стойкими к искажениям, в том числе к сжатию являются методы, использующие для сокрытия информации частотную область контейнера [3].
В качестве контейнера также успешно используются протоколы TCP, IP, VoIP и SCTP. В протоколах TCP/IP в качестве контейнера используются сетевые пакеты, а информация скрывается неиспользуемых полях заголовка этих пакетов. Преимущество данного метода заключается в том, что стеганограмма от отправителя к получателю передается без изменения. Кроме того, метод удобно в реализации. Недостатком метода является то, что передаваемые данные содержатся в открытом виде и могут быть легко обнаружена наблюдателем [5-7].

Пакеты VoIP, обеспечивающий голосовую связь и видеосвязь через Интернет, используются как контейнер для сокрытия сообщения. Метод TranSteg (Transcoding Steganography) сжимает полезные нагрузки сетевого пакета за счёт перекодирования. Сжатие данных используется, чтобы освободить место для стеганограммы. Метод позволяет получить скрытый канал с более или менее хорошей стеганографической пропускной способностью. В качестве недостатка данного метода можно указать трудность реализации, а также потеря качества передаваемой речевой информации при сжатии.

Среди вышеупомянутых методов стеганографический метод SCTP, основанный на использование протокола SCTP (Stream Control Transmission Protocol) представляет большой интерес. Такие стеганографические методы применяются в режиме мультипоточности и использования множественных интерфейсов. Стеганографические методы SCTP, основаны на возможности изменения содержимого SCTP-пакетов, последовательности передачи SCTP-пакетов, а также комбинации этих (гибридный) методов. Кроме того, эти методы позволяют возможности для стеганографических приложений использовать изменения параметров передачи, а также адресов отправителя и получателя [8].

5. РОЛЬ КОНТЕЙНЕРОВ В СТОЙКОСТИ СТЕГАНОГРАФИЧЕСКИХ СИСТЕМ

Для определения влияния контейнеров на стеганографическую стойкость рассмотрим теоретико-информационную модель стеганографической системы с пассивным нарушителем [2,9].

Нарушитель наблюдая сообщения, передаваемые между отправителям и получателям, не знает, что это пустой контейнер $-C$ или стеганограмма S содержащую скрытую сообщению. Отправитель может находится в активным или пассивным режиме. Если отправитель находится в активном режиме, он преобразует контейнер внесением в него скрываемого сообщения M используя секретный ключ K. При этом предполагается построение стеганографической системы, в которой отправитель сам может генерировать подходящий контейнер для сокрытия сообщения M. Получатель получая стеганограмму S, должен извлечь из нее сообщение M, используя ключ K. Если в соответствии с терминами теория информации обозначить через $H(M)$ - энтропию сообщения M, через $H(M/SK)$ - энтропию сообщения M при известных стеганограмм S и секретного ключа K, а через $H(S/CMK)$ – энтропию стеганограмму S при известных контейнером C, сообщения M и секретного ключа K, тогда стеганографическая система должно обеспечить следующее соотношение $H(S/CMK)=0$, $H(M/SK)=0$ при $H(M)>0$.

Для анализа стеганографических систем очень важно определение вероятностного распределения контейнеры и стеганограммы. Именно с помощью этих вероятностных распределений можно исследовать стойкость стеганографических систем. Так как, стойкость стеганографических систем можно определить, выбрав одно из двух гипотез H_C и H_S. При этом, первая гипотеза определяет энтропию при известном вероятностном распределении контейнеров C, обозначаемая через P_C, а вторая гипотеза энтропию при известном вероятностном распределении стеганогрмм S, обозначаемая через P_S. Мера различия этих гипотез является относительная энтропия $D(P_C \parallel P_S)$. Она может быть использована для оценки стойкости стеганографический системы при пассивном нарушителе. Если удовлетворяется соотношения $D(P_C \parallel P_S) \le \varepsilon$, то стеганографическая система называется ε - стойкий против пассивного нарушителя [2,9]. Если вероятностные распределения контейнера и стеганограммы одинаковы, то относительная энтропия равна нулю ($D(P_C \parallel P_S)=0, \varepsilon=0$), и такая стеганографическая система считается совершенной [10]. Для таких стеганографических систем вероятность обнаружения факта передачи скрываемого сообщения не меняется в зависимости от того, наблюдает ли нарушитель информационный обмен между отправителем и получателем или не наблюдает. Точнее, пассивный нарушитель, обладающий достаточно большими ресурсами и владеющий любыми методами стегоанализа, не сможет обнаружить факта использования совершенной стеганографической системы.

6. ЗАКЛЮЧЕНИЕ

Исследована зависимость надежности стеганографической системы от свойств контейнеров, принципов их выбора и технологии внедрения конфиденциальной информации в контейнер. Было отмечено, что стойкость стеганографических систем зависит от вероятностного распределения контейнеров и стеганограмм и только при их равенство стеганографическая система является совершенно стойкой.

ЛИТЕРАТУРА

1. Аграновский, А.В. и Балакин, А.В. и Грибунин, В.Г. и Сапожников, С.А., Стеганография, цифровые водяные знаки и стеганоанализ, М.: Вузовская книга, 220 с., 2009.

2. Грибунин, В.Г. и Оков, И.Н. и Туринцев, И.В., Цифровая стеганография, М.: Солон-Пресс, 272 с., 2002.

3. Конахович, Г.Ф. и Пузыренко, А.Ю., Компьютерная стеганография. Теория и практика, К.: МК-Пресс, 288 с., 2006.

4. Bender, W. and Gruhl, D. and Morimoto, N. and Lu, A., Techniques for Data Hiding, IBM Systems Journal, Vol. 35, Pages 313–336, 1996.

5. Enrique, C. and Roberto, G. and Ryouske, W., Data Hiding in Identification and Offset IP fields, California University at Irwing, Computer Science and Engineering 204B University of California, Irvine, CA 92717 USA. http://www.sciweavers.org/read/data-hiding-in-identification-and-offset-ip-fields-124683

6. Пескова, О.Ю. и Халабурда, Г.Ю., Применение сетевой стеганографии для защиты данных, передаваемых по открытым каналам Интернет, Известия ЮФУ. Технические науки, Вып. 12, С. 348-354, 2012.

7. Касумов В.А. и Гусейнова, Г.Возможности создания передачи каналы скрытой информации в протоколах интернет, Journal of Qafqaz University, Mathematics and Computer Science, Vol. 3, No. 1, P. 50-56, 2015.

8. Stewart, R., Ed. Stream Control Transmission Protocol. RFC 4960. Request for Comments: 4960, http://tools.ietf.org/html/rfc4960, 2007.

9. Cachin, C., An Information-Theoretic Model for Steganography, Proceeding of 2nd Int. Workshop on Information Hiding, Vol. 1525, Pages 306-3018, 1998.

10. Чисар, И. и Кернер, Я. Теория информации: Теоремы кодирования для дискретных систем без памяти, Пер. с англ., М.: Мир, 400 с., 1985.