УДК 004.056.5
DOI: 10.26102/2310-6018/2023.43.4.003

Стойкость метода ассоциативной стегозащиты данных картографических сцен

И.С. Вершинин✉

Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ, Казань, Российская Федерация

Резюме. В статье приводится введенное ранее и необходимое для дальнейшего рассмотрения понятие двумерно-ассоциативного механизма маскирования, используемого для зашиты данных картографических сцен, представленных точечными объектами. Механизм маскирования положен в основу ассоциативной стеганографии. При этом объекты и координаты сцены представляются кодовыми словами в алфавите почтовых символов и подвергаются маскированию с дальнейшим формированием стегоконтейнеров. Набор масок является секретным ключом, используемым далее для распознавания сцены, представленной в защищенном виде совокупностью стегоконтейнеров. Оценивается стойкость метода к атаке с позиции знания информации о некоторых объектах и их координатах (ассоциации с картой местности). Рассматриваются два случая действия таких атак – собственно знание противником местоположения некоторого известного ему объекта, а также анализ сцены на предмет правдоподобности после распознавания на некотором ключе. Приводятся результаты экспериментальных исследований, позволяющие утверждать безусловную либо доказуемую (т. е. вычислительную, связанную с невозможностью полного перебора ключей) стойкость метода. Дополнительно проводится анализ стойкости для случая избыточного маскирования, вводимого для повышения помехоустойчивости хранимых или передаваемых данных, когда для защиты этих данных используется не один, а несколько наборов масок.

Ключевые слова: ассоциативная стеганография, стойкость, информационная безопасность, картографические сцены, анализ сцен.

Для цитирования: Вершинин И.С. Стойкость метода ассоциативной стегозащиты данных картографических сцен. *Моделирование, оптимизация и информационные технологии.* 2023;11(4). URL: https://moitvivt.ru/ru/journal/pdf?id=1438 DOI: 10.26102/2310-6018/2023.43.4.003

Resistance of the method for associative stegosecurity of cartographic scene data

I.S. Vershinin✉

Kazan National Research Technical University named after A.N. Tupolev-KAI, Kazan, the Russian Federation

Abstract. For further consideration, the article presents earlier introduced concept of a two-dimensional associative masking mechanism used to protect the data of cartographic scenes represented by point objects. The masking mechanism is the basis of associative steganography. In this case, the objects and coordinates of the scene are represented by code words using the alphabet of postal symbols and are masked with stegocontainers developed later. A set of masks is a secret key employed then to recognize a scene represented in a protected form by a set of stegocontainers. The method offence resistance is evaluated from the standpoint of the availability of information about some objects and their coordinates (associations with the terrain map). Two cases of such attacks are considered – the enemy's actual knowledge of the location of an object familiar to them as well as the analysis of the scene for plausibility after recognition using a key. The results of experimental studies are presented, which makes it possible to assert the unconditional or provable (i.e. computational associated with the impossibility of a

complete search for keys) resistance of the method. Additionally, a resistance analysis is carried out for the case of excessive masking introduced to increase the noise immunity of stored or transmitted data, when not one, but several sets of masks are used to protect this data.

Keywords: associative steganography, resistance, cartographic scenes, information security, scene analysis.

For citation: Vershinin I.S. Resistance of the method for associative stegosecurity of cartographic scene data. *Modeling, Optimization and Information Technology*. 2023;11(4). URL: https://moitvivt.ru/ru/journal/pdf?id=1438 DOI: 10.26102/2310-6018/2023.43.4.003 (In Russ.).

Введение

Идея двумерно-ассоциативного картографического шифра является итогом исследований механизмов ассоциативной обработки стилизованных бинарных изображений при действии помех [1-3].

Для анализа сцен [4] картографии (сокрытия данных) проводится кластеризация объектов сцен (их отнесение к тому или иному ранее сформированному кластеру либо формирование нового кластера с отнесением объекта-родителя к этому новому кластеру). Далее объекты представляются бинарными матрицами, над которыми проводятся процедуры маскирования и последующей рандомизации (см. ниже). Имя объекта, а также его координаты (x,y) кодируются, при этом разрядность кодов определяется количеством объектов и выбранной градацией координат. Кодовые символы представляются в бинарном виде в алфавите почтовых индексов.

На практике картографические данные могут быть представлены, например, в виде тематических слоев геоинформационных систем [5-6].

Процедуру кластеризации на примере точечных объектов иллюстрирует Рисунок 1. На начальном этапе случайным образом выбирается один из объектов карты, который становится «родителем» кластера. В качестве глобальных координат формируемого кластера выбираются координаты ближайшего к выбранному объекту (слева снизу) узла сетки. Координаты «родителя» кластера преобразуются из глобальных в локальные внутри кластера.

Далее процедура повторяется для всех остальных объектов карты. Если очередной выбранный объект находится за пределами сформированного кластера(-ов), формируется новый кластер. После выборки всех объектов карты кластеризация завершается. Защите подлежит набор кластеров как табличная информация, представленная в виде «коды объектов – коды координат».

После проведения над кодовыми представлениями объектов / координат процедуры маскирования генерируется случайный набор масок, выступающий в роли секретного ключа. Процедура маскирования проводится с использованием алгоритма маскирования [1]. Суть процедуры маскирования кодовых представлений объектов / координат (в алфавите почтовых символов) заключается в случайном нахождении так называемых дихотомальных битов и их последующем (в процессе рандомизации) сохранении. Знание позиций дихтомальных битов (масок) позволит провести однозначную идентификацию.

Пример работы алгоритма маскирования для почтовых символов размером 5×3 представлен на Рисунке 2. Точки обозначают сохраняемые биты (отмечаются единичными битами в формируемых матрицах масок).

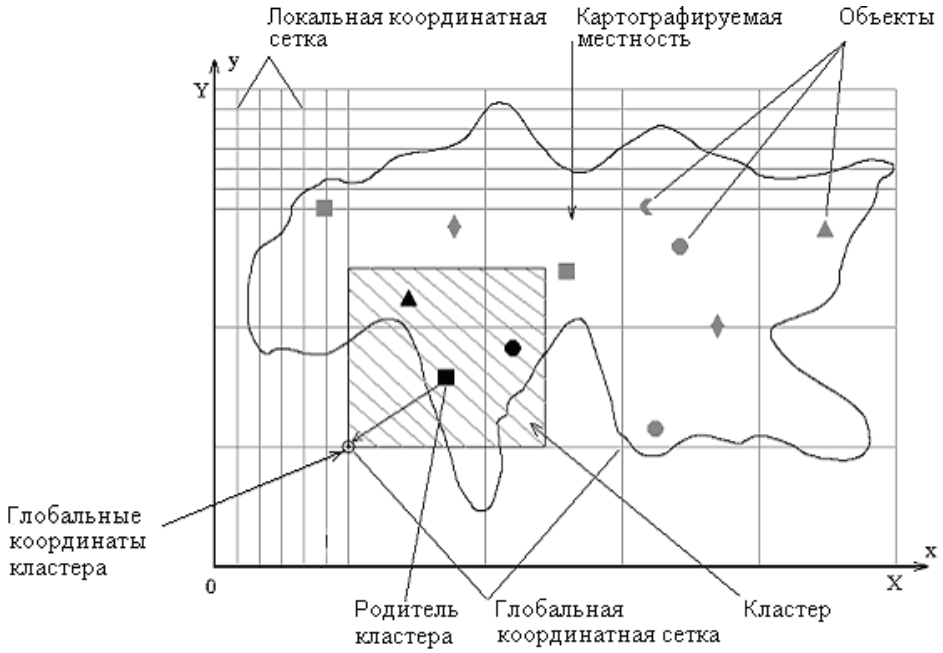

Рисунок 1 – Кластеризация объектов карты
Figure 1 – Clustering of map objects

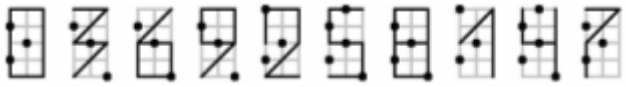

Рисунок. 2 – Пример работы алгоритма маскирования
Figure 2 – Masking algorithm sample

После формирования масок для кодовых представлений объектов / координат проводится процедура рандомизации с формированием стегоконтейнеров (Рисунок 3). На Рисунке 3 используется развернутое по контуру представление матриц кодовых символов (эталонов) и масок.

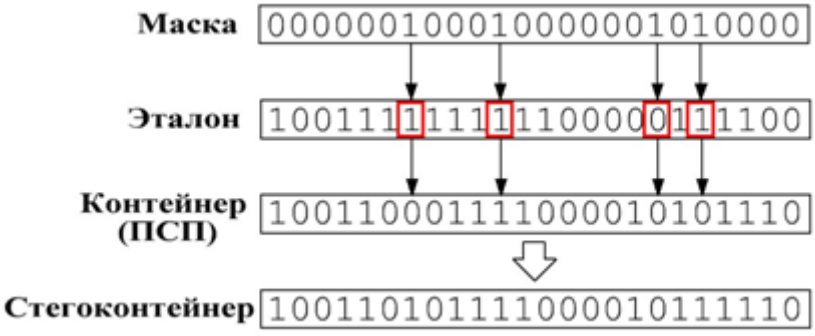

Рисунок 3 – Формирование стегоконтейнеров
Figure 3 – Formation of a stegocontainer

Выбор размеров бинарных матриц десятичных кодовых символов и генератора псевдослучайной последовательности (ПСП) для заполнения пустых контейнеров должен удовлетворять критерию полноты покрытия. Суть этого критерия состоит в обеспечении распознавания в каждом стегоконтейнере сообщения в целом полного множества кодов имен объектов и их координат, возможных для данной сцены, с первой случайной попытки формирования ГАММЫ при ограниченном переборе ключей.

Установлено, что данный критерий выполняется при выборе размеров бинарных матриц не менее 79×40 и генератора ПСП «Вихрь Мерсенна» [7]. Таким образом, при выполнении указанного критерия обеспечивается *безусловная стегостойкость* рассматриваемого метода [8].

Однако действие различного рода атак может привести к снижению уровня стойкости. Рассмотрение одной из таких атак – ассоциаций с картой местности – является целью данной статьи.

Решаются следующие задачи:

1. Оценка стойкости в случае знания противником местоположения некоторого известного ему объекта.
2. Оценка стойкости при проведении анализа сцены на предмет правдоподобности после распознавания на некотором ключе.

Ассоциации с картой местности

При переходе к рассмотрению реальных карт, объекты на которых подлежат защите с использованием данного метода стегозащиты, возможно снижение уровня стойкости с учетом известного характера местности либо обладанием некоторой (частичной) информации о расположении объектов на местности. Ограничимся рассмотрением следующих случаев:

1. Знание «противником» информации о некотором одном объекте на карте – расположение (координаты) и тип этого объекта.
2. Невозможность нахождения определенных типов объектов на карте с учетом характера местности

В первом случае проведем рассмотрение ситуации, наиболее благоприятной для противника. Такая ситуация возникает, если количество градаций локальных и глобальных координат совпадает и размер кластера равен размеру ячейки глобальной координатной сетки. Координаты (локальные и глобальные) кодируются в натуральном порядке. Исходя из этого, противник сможет определить глобальные координаты кластера, в котором располагается известный ему объект, а также локальные координаты этого объекта, а также их коды.

На Рисунке 4 местоположение объекта, известного противнику, представлено условным обозначением ⊠. Рассматривается простейший случай одноразрядного кодирования, когда число градаций локальных и глобальных координат одинаково и равно 10. Выше оси X цифрами 2, 4, 6, 8 обозначены градации локальных координат внутри кластера. Из-за равенства размера кластера шагу глобальной координатной сетки противник имеет точную информацию, в каком кластере находится известный объект. На Рисунке 4 этот кластер имеет глобальные координаты (0, 9), а известный объект в нем имеет локальные координаты (8, 0).

Тогда возможно применение «лобовой» атаки путем перебора ключей. Велика вероятность того, что распознавание на ложном ключе приведет к отсутствию в результатах распознавания искомого объекта. Тогда такой ключ исключается из рассмотрения. Следует отметить, что распознавание содержимого всех кластеров не требуется. Достаточно провести распознавание глобальных координат всех кластеров, и при наличии в результатах координат нужного кластера провести распознавание содержимого только этого кластера. Иначе ключ сразу признается ложным.

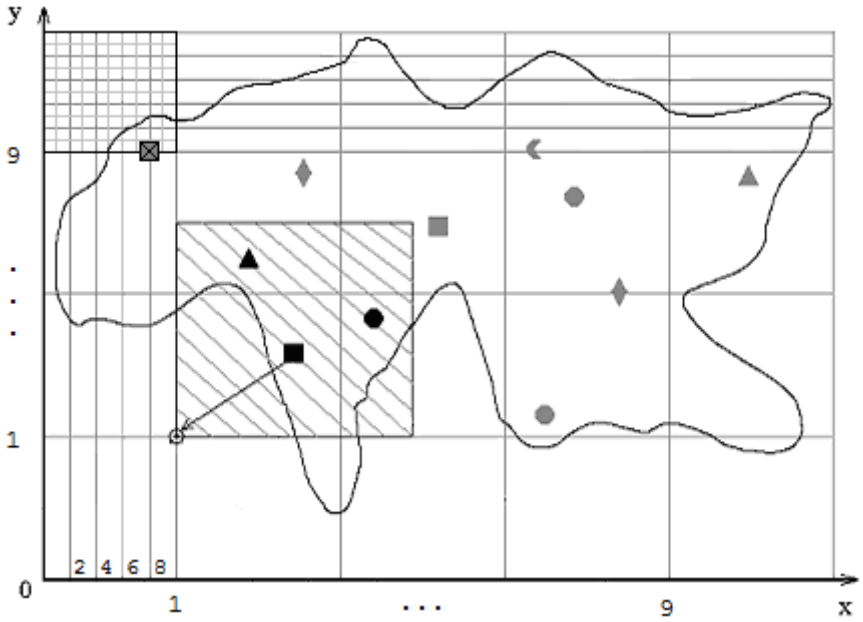

Рисунок 4 – Местоположение известного объекта
Figure 4 – Location of a known object

Для проверки данного утверждения был проведен эксперимент со следующим набором данных.

1. Карта содержит 10^2 кластеров.
2. В каждом кластере располагается 10^2 объектов.
3. Из указанного множества объектов карты осуществлялся случайный выбор известного противнику объекта.
4. Объекты представляются трехразрядными кодовыми словами, буквы (символы) которых представлены в алфавите почтовых символов (m×n = 39×20). Далее с использованием случайного набора масок (ключа) формируются стегоконтейнеры согласно рисунку 3.

При проведении ограниченного перебора ключей ($1{,}6\times10^6$), содержащего в том числе истинный ключ, ни на одном ключе множества, кроме истинного, не произошло выявление известного объекта. Другими словами, все остальные ключи этого множества – ложные.

Второй случай предполагает анализ результатов распознавания на каждом ключе с точки зрения правдоподобия. В случае выявления неправдоподобной картины (например, нахождение морской нефтяной вышки на суше) такой ключ полагается ложным. Для этого случая рассматривалось 6 вариантов, представленных в Таблице 1.

Таблица 1 – Варианты для проведения эксперимента
Table 1 – Options for conducting the experiment

№	Количество отсутствующих типов объектов на карте	Количество объектов на карте
1	1	100
2	1	1000
3	10	100
4	10	1000
5	100	100
6	100	1000

Для всех вариантов использовалось трехразрядное кодирование, то есть полное множество типов объектов равно 10^3. Из этого множества для каждого из вариантов случайно определялось соответствующее количество типов объектов, которых не может быть на карте. Из оставшегося множества типов объектов случайно формируется множество объектов карты. Количество объектов этого множества определяется количеством присутствующих на карте объектов для каждого варианта. Для этих объектов проводилась процедура маскирования и рандомизации с последующим распознаванием на множестве из 10^6 ключей и определением количества ложных ключей.

Результат для каждого из 6 вариантов представлен в Таблице 2. В Таблице приняты следующие обозначения: $K_{от}$ – количество отсутствующих типов объектов на карте, $K_{об}$ – количество объектов на карте, $K_{л}$ – число ложных ключей.

Таблица 2 – Число ложных ключей
Table 2 – Number of false keys

№	$K_{от}$	$K_{об}$	$K_{л}$
1	1	100	92115
2		1000	412204
3	10	100	605700
4		1000	997043
5	100	100	999944
6		1000	10^6

Из Таблицы 2 следует, что число ложных ключей тем больше, чем больше число типов объектов, которые не могут присутствовать на карте. Также увеличение количества ложных ключей происходит с увеличением количества объектов на карте.

Обсуждение

По результатам исследования *для первого случая* на основании частичного перебора ключей можно утверждать, что в случае полного перебора ключей будет выявлен истинный ключ. Следовательно, в данном случае имеем лишь доказуемую или вычислительную стойкость метода, связанную с недостижимостью полного перебора ключей в приемлемые сроки.

Рассмотренный случай предполагал наличие наиболее благоприятных для противника условий. Однако, если размер кластера не будет совпадать с размером ячейки глобальной координатной сетки, то при кластеризации в силу случайности известный противнику объект может попасть в различные кластеры. Тогда распознавание объектов необходимо будет проводить не в одном, а в нескольких кластерах, что повышает вероятность нахождения противником истинного объекта на ложном ключе.

Также выше предполагалось, что кодирование координат осуществляется в натуральном порядке. Однако в общем случае этот порядок может быть произвольным и неизвестным противнику. Тем не менее, следуя известному принципу Керкгоффса [9], согласно которому эффективная работа системы не должна основываться на факте её неизвестности для противника (противнику известно *всё*, кроме ключа) для обоих рассмотренных случаев можно утверждать лишь доказуемую стойкость.

По результатам исследования *для второго случая* (Таблица 2) можно сделать вывод о сохранении безусловной стойкости в случае небольших количества

отсутствующих типов объектов и «объема» карты, в противном случае – лишь о доказуемой (вычислительной) стойкости.

В дополнение определим уровень стойкости для случая внедрения избыточности на уровне ключей. Известно [10], что избыточность вводится для повышения помехоустойчивости передаваемой или хранимой информации. Особенность рассматриваемого подхода заключается в том, что формирование стегоконтейнеров и их последующее распознавание проводится не на одном наборе ключей, а на нескольких (3, 5, 7, …) по так называемому мажоритарному принципу. Для рассмотренных атак увеличение числа истинных ключей не приведет к отмене необходимости полного перебора ключей. Следовательно, стойкость на уровне доказуемой остается неизменной.

Заключение

В статье рассмотрен механизм двумерно-ассоциативного механизма маскирования, применяемый для защиты сцен картографии. Для двух случаев проведено исследование воздействия специфических картографических атак (ассоциаций с картой местности) на стойкость метода. В результате установлена доказуемая (в первом случае) либо безусловная (во втором случае) стойкость. Безусловная стойкость во втором случае сохраняется лишь в случае малого количества объектов. Иначе, как и для предыдущего случая, можно говорить о доказуемой стойкости.

Второе исследование аналогично поиску осмысленного текста для атаки перебором ключей в случае использования симметричных криптоалгоритмов [9]. Если в результате расшифрования зашифрованного сообщения на некотором ключе не будет получен осмысленный текст, то такой ключ полагается ложным.

Помимо картографии, актуальным видится применение ассоциативного стеганографического механизма защиты данных и области защиты интеллектуальной собственности: защита авторских прав, мониторинг нарушений, защита конфиденциальных документов, обеспечение анонимности и т.п. Использование ассоциативного стеганографического механизма защиты данных в защите интеллектуальной собственности открывает новые горизонты для обеспечения конфиденциальности, сохранности и контроля над распространением произведений интеллектуальной собственности.

СПИСОК ИСТОЧНИКОВ

1. Райхлин В.А., Вершинин И.С. Моделирование процессов двумерно-ассоциативного маскирования распределенных точечных объектов картографии. *Нелинейный мир*. 2010;8(5):288–296.
2. Райхлин В.А., Вершинин И.С., Гибадуллин Р.Ф. Обоснование принципов ассоциативной стеганографии. *Вестник КГТУ им. А.Н. Туполева*. 2015;2:110–119.
3. Raikhlin V.A., Vershinin I.S., Gibadullin R.F. The elements of associative steganography theory. *Moscow University Computational Mathematics and Cybernetics*. 2019;43(1):40–46. DOI: 10.3103/S0278641919010072.
4. Duda R.O., Hart P.E., Stork D.G. *Pattern classification and scene analysis*. New York, Wiley; 1973. 512 p.
5. Сяо Н. *Алгоритмы ГИС*. М.: ДМК Пресс; 2021. 328 с.
6. Бабенко Л.К., Басан А.С., Журкин И.Г., Макаревич О.Б. *Защита данных геоинформационных систем*. М.: Гелиос АРВ; 2010. 336 с.
7. Tian X., Benkrid K. Mersenne twister random number generation on FPGA, CPU and GPU. *2009 NASA/ESA Conference on Adaptive Hardware and Systems, San Francisco, CA, USA*. 2009. p. 460–464. DOI: 10.1109/AHS.2009.11.

8. Грибунин В.Г., Оков И.Н., Туринцев И.В. *Цифровая стеганография*. М.: СОЛОН-Пресс; 2002. 272 с.
9. Молдовян Н.А., Молдовян А.А., Еремеев М.А. *Криптография: от примитивов к синтезу алгоритмов*. СПб.: БХВ-Петербург; 2004. 448 с.
10. Морелос-Сарагоса Р. *Искусство помехоустойчивого кодирования*. М.: Техносфера; 2006. 320 с.

REFERENCES

1. Raikhlin V.A., Vershinin I.S. Modeling of processes of two-dimensional associative masking of distributed point objects of cartography. *Nelinejnyj mir = Non-linear world.* 2010;8(5):288–296. (In Russ.).
2. Raikhlin V.A., Vershinin I.S., Gibadullin R.F. Substantiation of the principles of associative steganography. *Vestnik KGTU im. A.N. Tupoleva = Bulletin KSTU named after A.N. Tupolev.* 2015;2:110–119. (In Russ.).
3. Raikhlin V.A., Vershinin I.S., Gibadullin R.F. The elements of associative steganography theory. *Moscow University Computational Mathematics and Cybernetics*. 2019;43(1):40–46. DOI: 10.3103/S0278641919010072.
4. Duda R.O., Hart P.E., Stork D.G. *Pattern classification and scene analysis*. New York, Wiley; 1973. 512 p.
5. Xiao N. *GIS algorithms.* Moscow, DMK Press; 2021. 328 p. (In Russ.).
6. Babenko L.K., Basan A.S., Zhurkin I.G., Makarevich O.B. *Data protection of geoinformation systems*. Moscow, Gelios ARV; 2010. 336 p. (In Russ.).
7. Tian X., Benkrid K. *Mersenne twister random number generation on FPGA, CPU and GPU. 2009 NASA/ESA Conference on Adaptive Hardware and Systems, San Francisco, CA, USA.* 2009. p. 460–464. DOI: 10.1109/AHS.2009.11.
8. Gribunin V.G., Okov I.N., Turincev I.V. *Digital steganography*. Moscow, SOLON-Press; 2002. 272 p. (In Russ.).
9. Moldovyan N.A., Moldovyan A.A., Eremeev M.A. *Cryptography: from Primitives to Algorithm Synthesis*. Saint Petersburg, BHV-Peterburg; 2004. 448 p. (In Russ.).
10. Morelos-Zaragoza R. *The Art of error correcting coding*. Moscow, Tekhnosfera; 2006. 320 p. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Вершинин Игорь Сергеевич, кандидат технических наук, доцент, заведующий кафедрой компьютерных систем, Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ, Казань, Российская Федерация.
e-mail: Vershinin_Igor@rambler.ru
ORCID: 0000-0001-5166-2862

Igor S. Vershinin, Candidate of Technical Sciences, Associate Professor, Head of Computer Systems Department, Kazan National Research Technical University named after A.N. Tupolev-KAI, Kazan, the Russian Federation.

Статья поступила в редакцию 08.09.2023; одобрена после рецензирования 27.09.2023; принята к публикации 05.10.2023.

The article was submitted 08.09.2023; approved after reviewing 27.09.2023; accepted for publication 05.10.2023.