Практическое сравнение возможностей некоторых стеганографических алгоритмов

И. А. Кривошеев, М. А. Линник

Хабаровский Федеральный исследовательский центр Дальневосточного отделения РАН, Хабаровск, Россия

Аннотация. В статье рассматриваются результаты работы наиболее распространенных алгоритмов стеганографии. Численным моделированием показана возможность противостоять атакам стегоанализа на различных этапах, связанных с объемом встраивания информации. Показано, что наиболее приемлемым можно считать адаптивные алгоритмы стеганографии.

Ключевые слова: стеганография, адаптивная стеганография, стегоанализ, RS-стегоанализ, Хи-квадрат стегоанализ, стегоанализ битовых срезов.

DOI 10.14357/20718632230410 **EDN** TUNEPY

Введение

На сегодняшний день постоянно увеличивающийся объем хранимой, передаваемой и обрабатываемой информации формирует потребность в развитии и постоянной модернизации мер по защите информации и безопасной передачи данных. Развитие этой области позволит обеспечить конфиденциальность и сохранность информации на должном уровне. Стоит отметить, что также постоянно совершенствуются методы по перехвату и дешифровыванию данных, поэтому вопрос разработки мер противодействия является весьма актуальным.

В настоящей статье предлагается рассмотреть использование стеганографии в качестве решения одной из проблем безопасной передачи информации. Отличительной особенностью использования стеганографии является то, что данные внедряются в используемый для передачи объект (стегоконтейнер) таким образом, чтобы он не вызывал подозрений. В качестве носителей сообщения могут выступать текст, изображение, звук или видео.

В последнее время в качестве стегоконтейнеров очень активно рассматриваются цветные изображения. Преимущество данного класса контейнеров заключается в том, что, во-первых, они могут быть носителями большого объема информации, а во-вторых, для компенсации искажений, возникающих в результате встраивания и извлечения, необходимы незначительные вычислительные затраты относительно других типов [1].

В статье рассматриваются наиболее известные алгоритмы, способные работать в этом классе задач с приемлемыми характеристиками.

1. Постановка задачи

При разработке эффективной стегосистемы учитывается ряд факторов [2, 3], которые могли бы повлиять на конфиденциальность системы в целом.

Одним из них является возможность использования особенностей зрительной системы человека для выявления факта передачи данных.

Под этим подразумевается следующее: человеческий глаз более точно воспринимает возникновения искажений в самых высоких областях интенсивности цвета [3]. Данное обстоятельство нужно учитывать при проектировании защищенного алгоритма.

Другим фактором является поиск оптимальной пропускной способности – это достижение баланса между высоким объемом передачи информации и увеличение предела встраивания, после которого искажения будут заметны при применении стегоанализа.

Кроме того, следует отметить, что встраивание посторонней информации в исходный контейнер оставит следы, которые улавливаются группой алгоритмов стегоанализа. По этой причине алгоритмы должны иметь механизмы, позволяющие устранять последствия нарушения корреляционных связей между элементами контейнера, которые возникают в результате встраивания информации.

В качестве области встраивания информации в статье рассматривается внедрение сообщений в пространственную область. Именно такой подход затрудняет работу стегоанализа из-за того, что алгоритмы этого раздела позволяют встраивать наибольший объем информации. Кроме того, все производимые операции по встраиванию и извлечению данных являются зачастую обратимыми [4].

В качестве ключевого параметра, на котором основываются рассматриваемые алгоритмы, используется интенсивность цвета изображения в формате RGB, что означает разделение значения каждого пикселя на три цветовые компоненты: красную, синюю и зеленую. Информация встраивается за счет их модификации по определенным правилам.

2. Обзор стеганографических алгоритмов

Рассмотрим группу алгоритмов, работа которых основана на встраивании информации в пространственную область изображения.

Одним из самых известных алгоритмов в этой области является алгоритм замены младшего бита (LSB) [1, 4]. Его ключевым достоинством является возможность встраивания большого объема данных: встраивание от одного до четырех младших битов трех цветовых компонент цвета пикселя не будет заметно при визуальном наблюдении. Главный недостаток алгоритма – крайне низкая стеганографическая стойкость, из-за того, что он уязвим для обнаружения с помощью специальных инструментов.

Алгоритм Куттера-Джордана-Боссена [5] акцентируется на устойчивости к искажениям. Его работа основывается на использовании особенностей зрительной системы человека. Человеческое зрение менее восприимчиво к изменениям в синей компоненте цвета, поэтому именно данная составляющая используется для встраивания.

Особенностью алгоритма является то, что операция встраивания и извлечения не являются взаимно обратимыми. Таким образом, восстановление сообщения воспроизводится не со стопроцентной точностью, а выполняется с некоторой погрешностью.

Основным преимуществом алгоритма является, как уже было отмечено ранее, защита секретного сообщения от воздействия искажений контейнера. Однако это достигается за счет ряда существенных недостатков. Это, во-первых, выполнение извлечения вслепую, поэтому требуется дублирование информации, что добавляет дополнительные ограничения на объем встраивания информации. Во-вторых, исходный контейнер существенно модифицируется, поэтому снижается общая устойчивость стегосистемы. К тому же, стоит обратить внимание, что встраивание информации с помощью этого алгоритма происходит без учета структуры используемого контейнера.

Основное преимущество рассмотренной выше группы алгоритмов состоит в том, что для вычисления они требуют меньшую вычислительную мощность. Однако, существенным недостатком является то, что встраивание происходит без учета особенностей контейнера. Отсутствует анализ общей структуры изображения для выявления наиболее текстурированных или шумовых областей. Поэтому влияние искажений при встраивании данных будет существеннее, из-за чего снизится защищенность всей стегосистемы в целом.

В настоящее время особое внимание уделяется использованию алгоритмов адаптивной стеганографии. Это высокоэффективная группа

алгоритмов, которая позволяет скрывать сообщение в стегоконтейнере таким образом, чтобы минимизировать искажения и обеспечивать защиту от ряда стеганографических атак.

Наиболее интересные работы были нацелены именно на учет сглаживания следов встраивания и рассеивания битов сообщения по всему контейнеру. HUGO (Highly Undetectable steGO) [6] – сводит к минимуму влияние посторонней информации, которая достигается при использовании решетчатых кодов по алгоритму Витерби. Каждому пикселю присваивается определенный вес. Значение пикселя изменяется с вероятностью обратно пропорциональной его влиянию, которое определяется с помощью вычисленного значения веса.

Работа алгоритма WOW (Wavelet Obtained Weights) [7] основана на модификации окрестности пикселя, в который происходит встраивание данных с целью снизить изменение корреляционных связей и таким образом замаскировать сам факт встраивания. Основной акцент делается на минимизации искажений.

Рассмотренные алгоритмы являются высокоэффективными, но основной их недостаток – это необходимость в больших вычислительных мощностях, что накладывает ограничения на скорость выполнения и общую пропускную способность.

Авторами данной статьи в [8, 9] был предложен новый алгоритм для встраивания стеганографической информации (Dynamic), который учитывает приведенные выше недостатки. Во время его работы анализируется общая структура изображения и взаимное расположение пикселей.

Такой подход позволяет учитывать особенности распределения цвета в контейнере. Для внедрения сообщения используются наиболее пригодные области, тем самым достигается уменьшение искажения корреляционных связей между пикселями и минимизируется воздействие на общий уровень конфиденциальности стегосистемы.

3. Численное моделирование и эксперименты

Практическое использование этих методов с точки зрения выбора объема встраивания информации и защиты от различных алгоритмов стегоанализа было оценено при помощи численного моделирования. Для сравнения используются алгоритмы, представленные в пункте 2. Подобранная группа состоит из наиболее распространенных стегоалгоритмов и отражает кардинально разные подходы: передача как можно большего объема информации или акцент на защите данных от обнаружения.

На начальном этапе были сформированы две группы по 200 изображений в формате bmp с разрешением 512 x 512, которые предлагается использовать в качестве стегоконтейнеров. Преимуществом формата bmp является простота и возможность точного восстановления сообщения [1].

Эксперименты проводились для двух ситуаций встраивания данных. Первая – это встраивание больших объемов информации. Для этого случая максимальный допустимый объем равен общему количеству пикселей выбранного изображения-контейнера.

Следует отметить, что понятия объем встраивания и общий объем изображения не являются эквивалентными. Объем изображения – это количество памяти, которое он занимает на устройстве. Для алгоритма [8] максимальный допустимый объем встраивания вычисляется по следующей формуле:

$$V = 3(h-(b-1))(w-(b-1)) - \sum z$$

где b – длина блока; w, h – ширина и высота изображения в пикселях; $\sum z$ – сумма запрещенных для встраивания пикселей.

Для алгоритма Куттера-Джордана-Боссена он равен разрешению изображения, деленному на 4 для того, чтобы учесть затраты на дублирование информации. Для остальных алгоритмов из рассматриваемой группы максимальный допустимый объем – это общее число пикселей контейнера.

Вторая ситуация встраивания данных – это внедрение сообщений малого размера. Такая ситуация может возникнуть, если, например, в изображение требуется добавить цифровой водяной знак.

Особенностью этого эксперимента является ввод дополнительных ограничений на объем встраивания информации. Максимальный допустимый объем для алгоритмов вычисляется относительно алгоритма Куттера-Джордана-Боссена.

Для извлечения сообщения, встроенного при помощи этого алгоритма, требуется дополнительное дублирование битов сообщения, поэтому значение максимального возможного объема для этих алгоритмов существенно ниже относительно других рассмотренных алгоритмов.

Выбранные эксперименты в полной мере охватывают основные цели применения стеганографии – это передача как можно большего объема секретной информации при условии, что факт передачи остается скрыт для злоумышленника или стегоаналитика (1 ситуация) и внедрение малого объема данных, который требуется для формирования цифровых водяных знаков (2 ситуация).

На Рис. 1 показано соотношение максимально допустимого объема встраивания информации для рассматриваемых алгоритмов для выбранных 200 контейнеров. На оси абсцисс показаны номера пустых контейнеров изображений, использовавшихся в эксперименте. На оси ординат показаны значения максимального объем информации (в битах), отсортированного по возрастанию, которые можно встроить в контейнер.

На графике видно, что наибольший объем информации можно встроить в изображение с помощью алгоритма LSB, при условии, что задействованы все три цветовые компоненты. Если используется только одна цветовая компонента, то это значение эквивалентно максимальному допустимому объему для HUGO и WOW.

Также стоит отметить, что предельное значение объема для Dynamic [8] не является постоянной величиной. Причина этого заключается в том, что работа алгоритма основана на анализе структуры изображения и встраивание происходит в наиболее текстурированные области для того, чтобы привнести меньшую величину искажений, и тем самым обеспечить сохранность конфиденциальности данных. Поэтому значение максимального допустимого объема вычисляется для каждого изображения индивидуально.

Для проведения визуальной оценки сравним Dynamic и LSB при помощи анализа битовых срезов [10]. Суть этого алгоритма состоит в формировании нового изображения - на основе исходного, - которое построено на младших битах. Если в контейнере находится посторонняя информация, то она будет визуально заметна.

В качестве анализируемых изображений был выбран вариант, который содержит ярко выраженную однородную текстуру, и поэтому наличие посторонней информации проявляется заметнее.

Результат визуального стегоанализа в этом случае, где встраивалось 30% от максимально допустимого объема, представлен на Рис. 2, а. На Рис. 2, б и 2, в представлены результаты визуального стегоанализа для LSB и Dynamic.

Стоит обратить внимание (Рис. 2, б), что с помощью анализа битовых срезов можно точно определить расположение информации, встроенной с помощью LSB. А при использовании

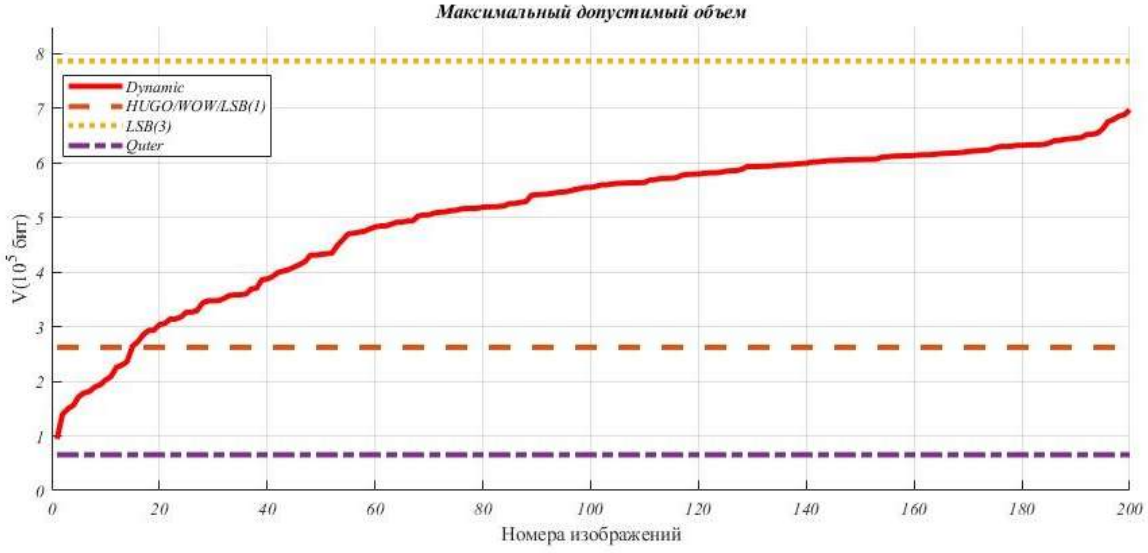
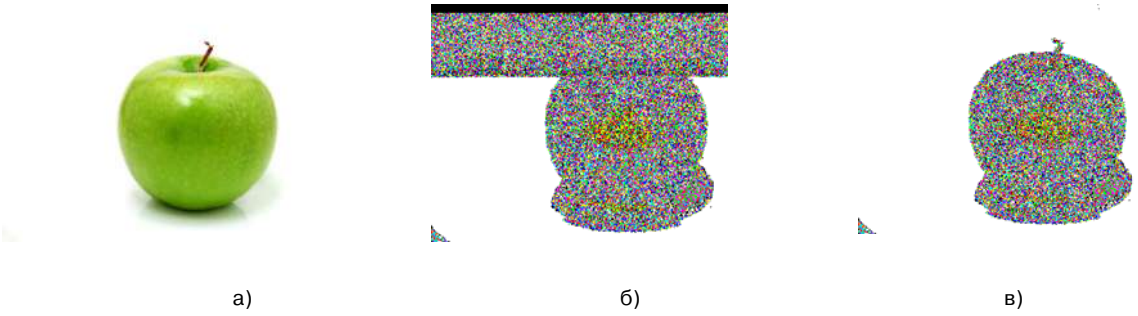


Рис. 1. Значения максимального объема у стегоконтейнеров для рассматриваемых алгоритмов



а) б) в)

Рис. 2. Анализ битовых срезов

а) стегоконтейнер со встроенной информацией, б) результаты стегоанализа для LSB, в) результаты стегоанализа для Dynamic

Dynamic (Рис. 2, в) сообщение рассеивается по контейнеру и не фиксируется с помощью данного метода стегоанализа. Поэтому можно говорить о том, что данный метод позволяет защитить контейнер от стеганографической атаки методом битовых срезов.

Для статистического стегоанализа были привлечены методы на основе критерия Хи-квадрат [11] и RS-стегоанализ [12]. Работа этих алгоритмов основывается на проверке контейнера на нарушение естественных корреляционных зависимостей между пикселями.

Для проведения сравнения алгоритмов в изображения были встроены 10%, 30% и 50% информации от максимально допустимого объема. Он вычислялся индивидуально для двух видов экспериментов. В первом случае максимальный допустимый объем равен разрешению изображения, а во втором максимальный объем вычисляется относительно Куттера-Джордана-Боссена (равен разрешению изображения, деленному на 4).

Суть RS-стегоанализа состоит в проверке сформированных групп пикселей и, если разница количества пикселей в них велика, то делается вывод, что в контейнере находится посторонняя информация.

На Рис. 3 представлены результаты RS-стегоанализа для рассматриваемых алгоритмов.

Обратим внимание, что на графиках значения RS-стегоанализа для алгоритма Dynamic приблизительно равны результатам WOW и HUGO. Но при этом значения RS-стегоанализа у него ниже, что свидетельствует о бóльшем уровне скрытности.

На Рис. 4 представлены графики RS-стегоанализа для второго эксперимента по встраиванию малых объемов информации.

Несмотря на то, что при встраивании малых объемов информации на работу RS-стегоанализа накладываются ограничения в погрешности, Dynamic, HUGO и WOW показывают себя лучше других рассмотренных алгоритмов в этой категории.

Метод стегоанализа на основе критерия Хи-квадрат опирается на гипотезу, согласно которой одновременная вероятность появления близких цветов в пустом (исходном) контейнере незначительна. На Рис. 5 приведены результаты первого эксперимента стегоанализа на основе критерия Хи-квадрат для случаев встраивания большого объема информации.

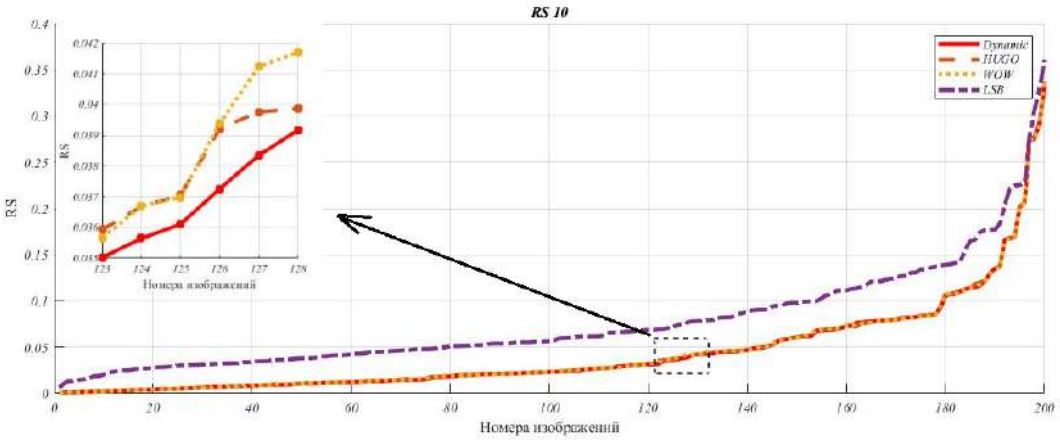
Наиболее высокие результаты по сохранению конфиденциальности этой группы показывают алгоритмы HUGO, WOW и Dynamic.

На Рис. 6 представлены графики второго эксперимента по встраиванию малых объемов информации.

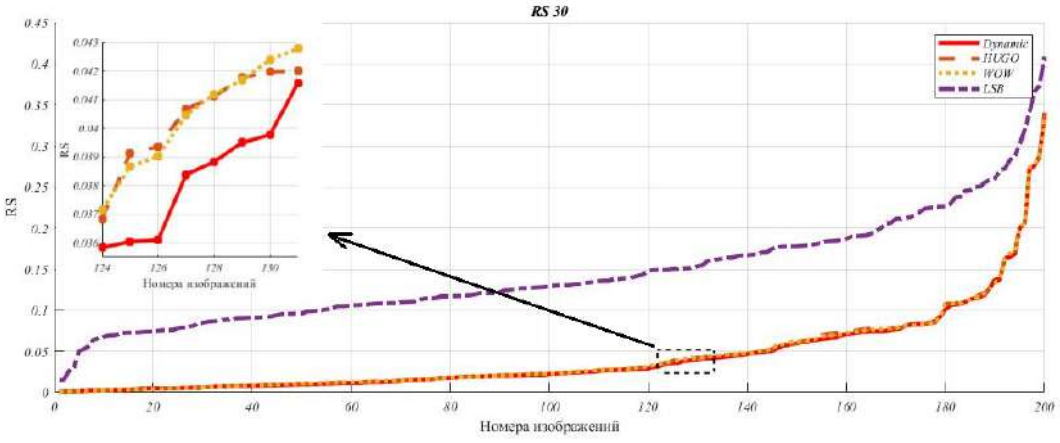
Из графиков видно, что наибольшую защищенность в этом эксперименте имеет алгоритм Куттера-Джордана-Боссена.

4. Обсуждение результатов

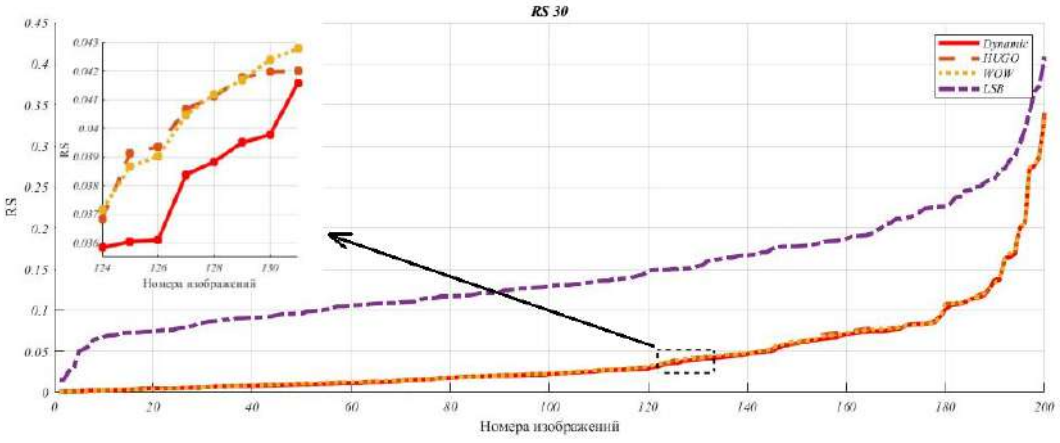
Согласно результатам проведенных экспериментов, было продемонстрировано, что алгоритмы HUGO, WOW и Dynamic поддерживают высокий уровень конфиденциальности информации при защите от RS стегоанализа. В этом случае можно сказать, что повышается вероятность того, что стегоконтейнер, содержащий передаваемое сообщение, не будет дискредитирован.



а)

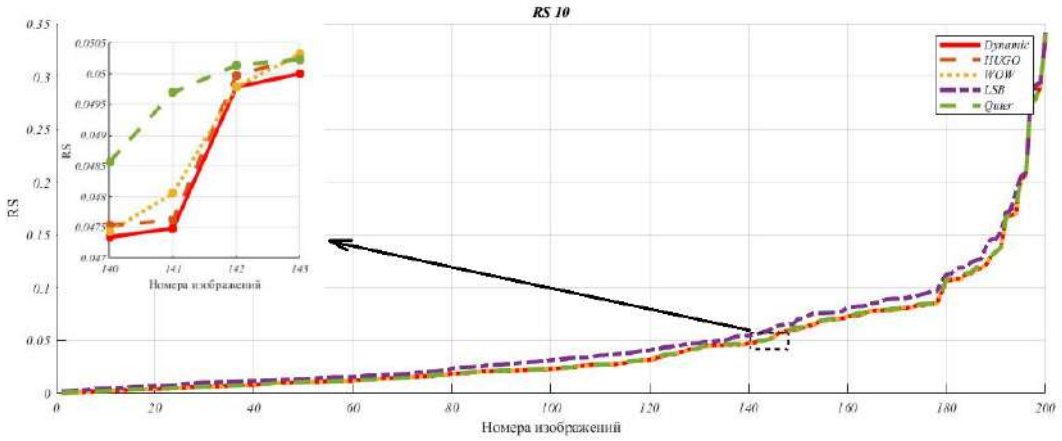


б)

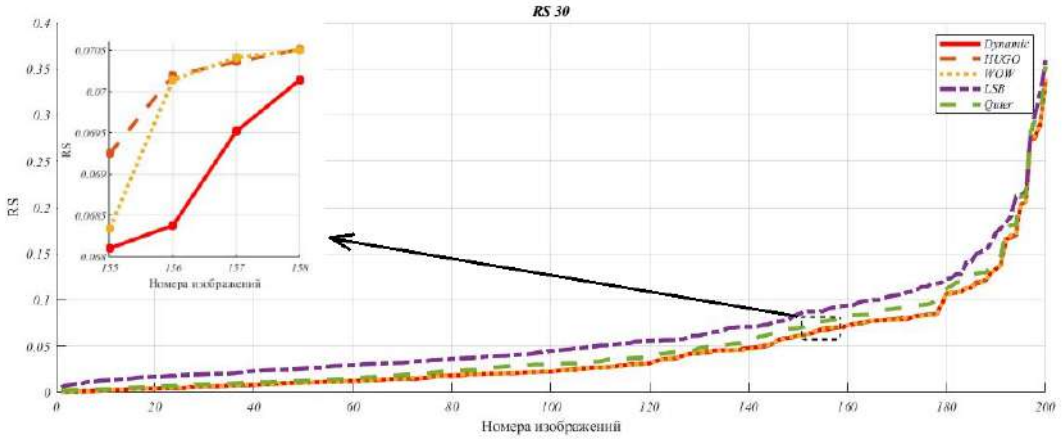


в)

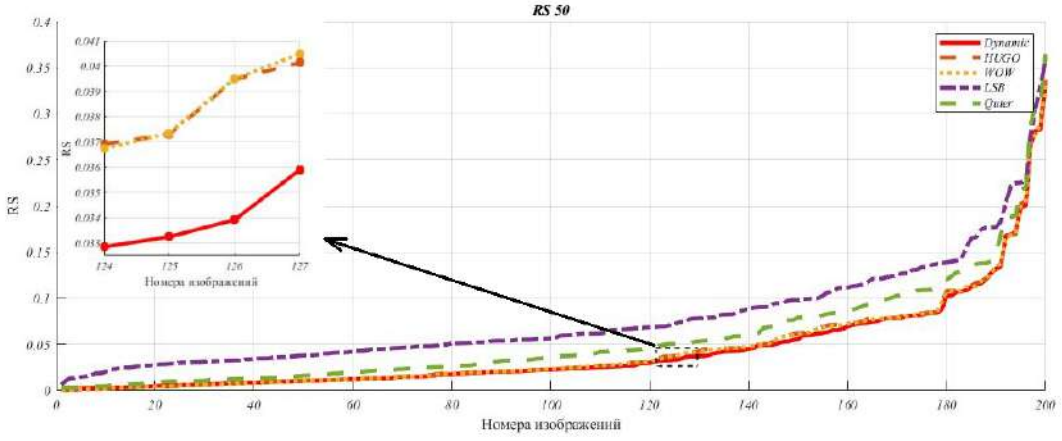
Рис. 3. Результаты численного моделирования первого эксперимента RS-стегоанализом для рассматриваемых алгоритмов при заполнении а) 10%, б) 30%, в) 50% объема контейнера



а)

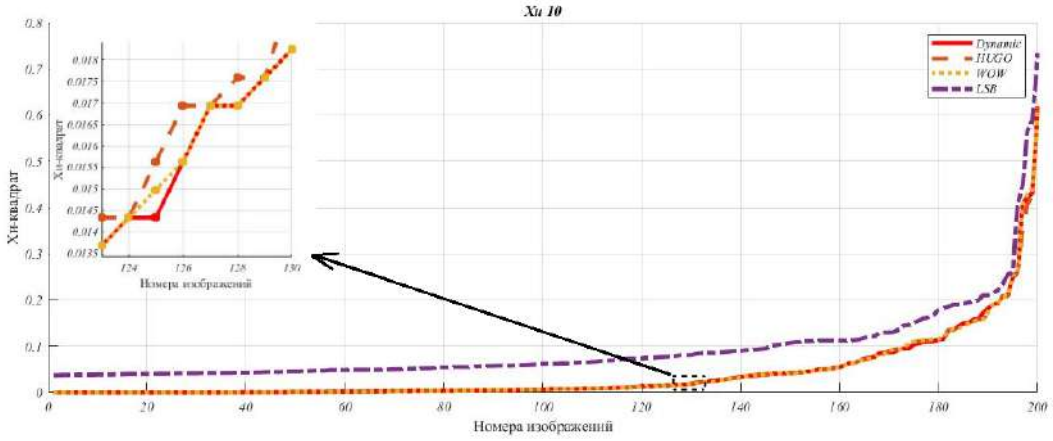


б)

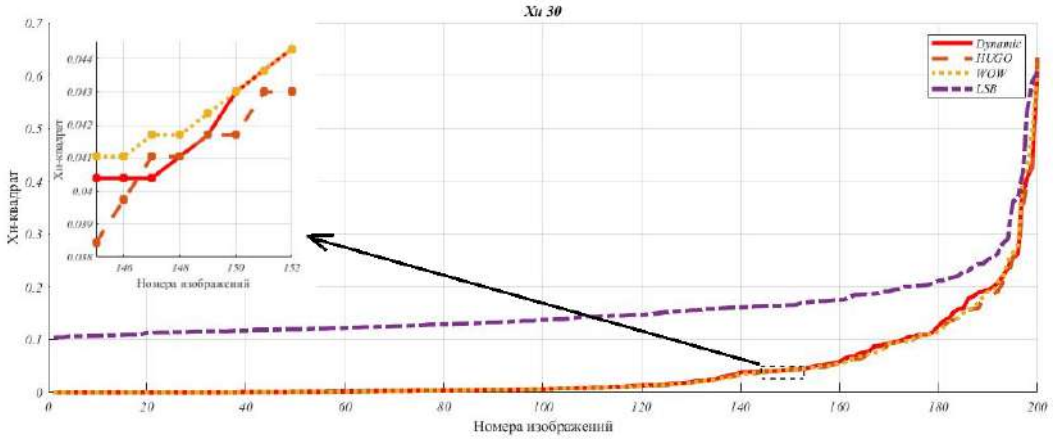


в)

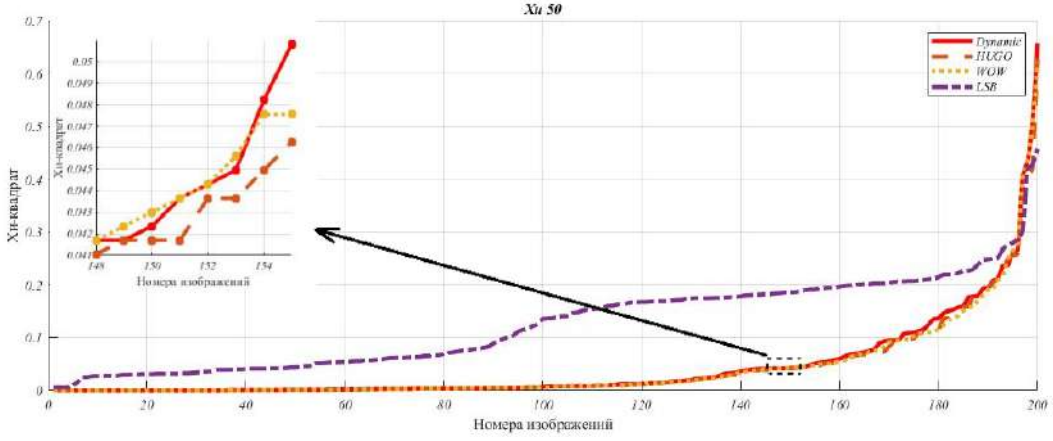
Рис. 4. Результаты численного моделирования второго эксперимента RS-стегоанализом для рассматриваемых алгоритмов при заполнении а) 10%, б) 30%, в) 50% объема контейнера



а)

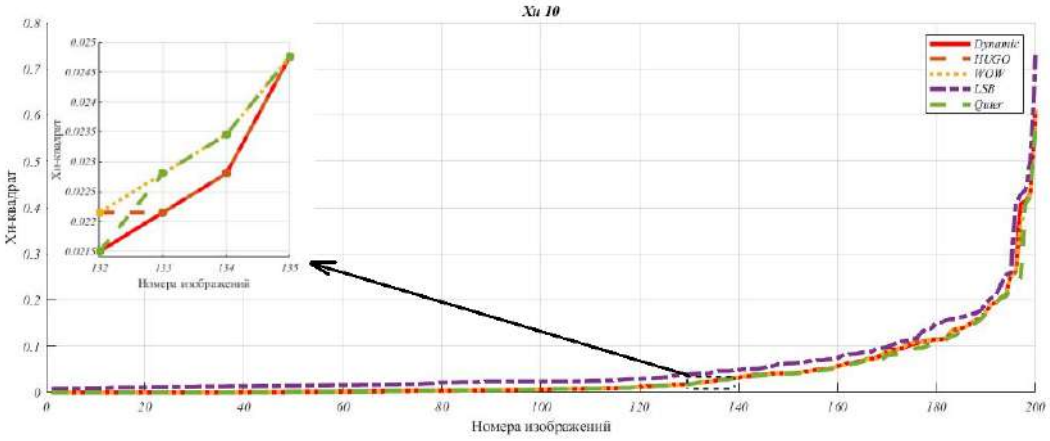


б)

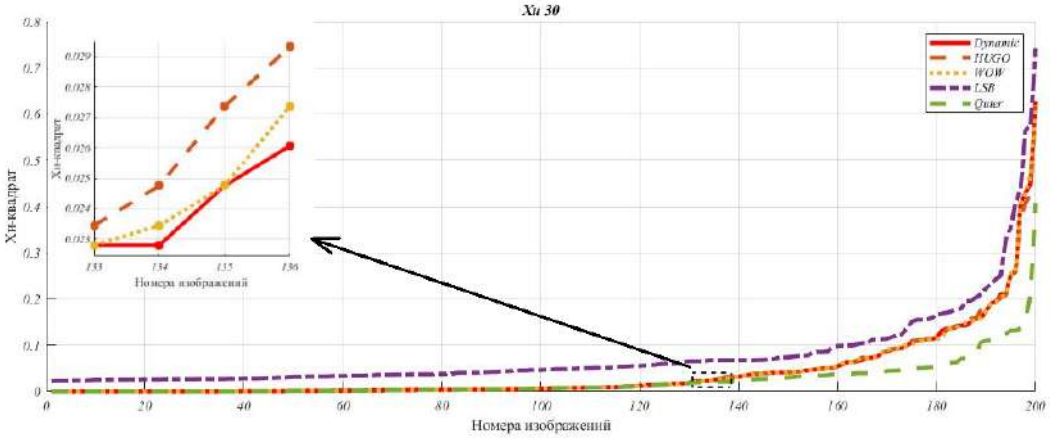


в)

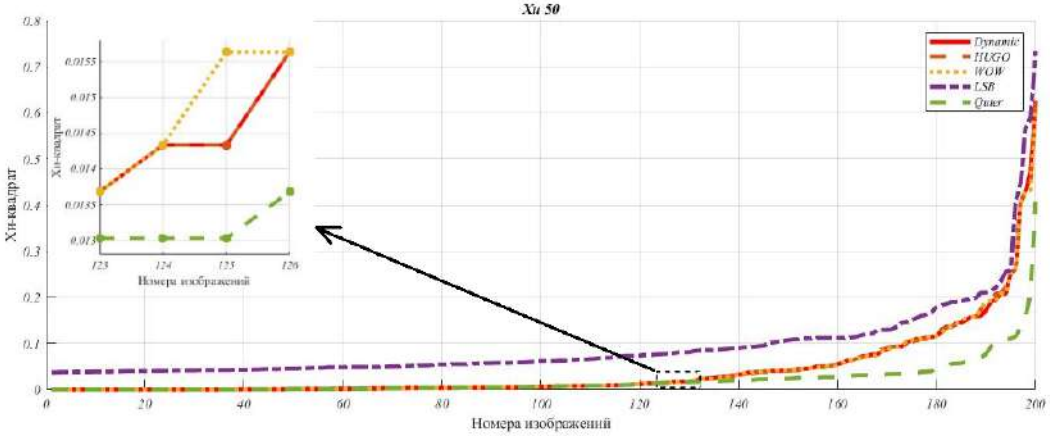
Рис. 5. Результаты численного моделирования первого эксперимента для Хи-квадрат стегоанализа рассматриваемых алгоритмов при заполнении а) 10%, б) 30%, в) 50% объема контейнера



а)



б)



в)

Рис 6. Результаты численного моделирования второго эксперимента для Хи-квадрат стегоанализа рассматриваемых алгоритмов при заполнении а) 10%, б) 30%, в) 50% объема контейнера

Алгоритм Куттера-Джордана-Боссена продемонстрировал большую защищенность от стегоанализа на основе критерия Хи-квадрат. Однако согласно показателям, полученным в ходе эксперимента по использованию RS-стегоанализа, при повышении объема встраиваемых данных его уровень конфиденциальности ниже HUGO, WOW и Dynamic и приближается к LSB.

Алгоритм LSB имеет низкую защищенность от стеганографических атак во всех экспериментах, но он при этом прост в реализации.

Можно выдвинуть предположение, что Dynamic имеет ряд выгодных преимуществ над известными аналогами. Он поддерживает возможность встраивания большого объема информации и одновременно обеспечивает высокую защищенность от стеганографических атак. Если изображение содержит большие площади однородных областей, то требуется введения порога, который позволит предотвратить запись информации в нежелательные пиксели, что в свою очередь может негативно сказываться на общей защищенности стегосистемы.

Если важно передать большие объемы информации, и при этом уровень защищенности не важен, то можно воспользоваться LSB и схожими с ними алгоритмами, где встраивание происходит без учета характеристик стегоконтейнера.

В случае, когда при встраивании данных особое внимание уделяется устойчивости к искажениям, и при этом встраивается достаточно малый объем информации, то для этой цели может быть использован алгоритм Куттера-Джордана-Боссена. Однако следует помнить, что восстановление данных выполняется с некоторой погрешностью, поэтому данный алгоритм целесообразен, если восстанавливаемые данные – это цвет пикселей изображения.

Если требуется поддержание одновременно высокого уровня защищенности и относительно большого объема встраивания данных, то выгодным решением будет использование группы алгоритмов адаптивного встраивания (HUGO, WOW) и Dymamic.

Заключение

В статье приведены результаты работы основных известных алгоритмов на группе изображений формата bmp для встраивания больших и малых объемов информации.

Представленные в статье результаты анализа алгоритмов могут быть использованы в качестве оценочных параметров для выбора наиболее подходящего алгоритма стеганографического встраивания в зависимости от того критерия, который будет определяющим для рассматриваемой ситуации.

Подводя итоги можно сказать, что два алгоритма – Dynamic и WOW - имеют преимущества над LSB и алгоритмом Куттера-Джордана-Боссена ввиду того, что встраивание происходит на основе анализа всей структуры изображения с целью выявить наиболее подходящие для этого области.

Алгоритм HUGO также сохраняет высокую конфиденциальность данных, но при этом требует большего времени для проведения встраивания.

Dynamic показывает достаточно высокие результаты защищенности и помимо этого адаптируется к используемому контейнеру с целью выявить наиболее подходящие области для встраивания.

В заключение стоит присмотреться к алгоритмам адаптивного встраивания данных, так как они, на наш взгляд, достаточно близки к понятию стеганографического сокрытия информации, а также в какой-то степени более устойчивы к различным методам стегоанализа, что выгодно отличает их от других алгоритмов.

Литература

1. Шелухин О.И. Канаев И.Д. Стеганография. Алгоритмы и программная реализация. М.: Горячая линия. 2017. 592 с.
2. Коханович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. К.: МК-Пресс. 2006. 288 с.
3. Грибунин В.Г., Оков И.Н. Цифровая стеганография. М.: Солон-пресс. 2002. 272 с.
4. Fridrich, J., Long, M. Steganalysis of LSB encoding in color images / J. Fridrich, M. Long // Multimedia and Expo. 2000 IEEE International Conference. 2000. Vol. 3. pp. 1279-1282.
5. Kutter M., Jordan F., Bossen F. Digital Signature Of Color Images Using Amplitude Modulation / M. Kutter, F. Jordan, F. Bossen // Proc. of the SPIE Storage and Retrieval for Image and Video Databases V. 1997. Vol. 3022. pp. 518-526.
6. Pevny T., Filler T., Bas P. Using High-Dimensional Image Models to Perform Highly Undetectable Steganography / T. Pevný, T. Filler, P. Bas // Information Hiding. 2010. pp. 161-177.
7. Holub V., Fridrich J. Designing Steganographic Distortion Using Directional Filters // Proc. 4th IEEE Intern. Workshop on Inform. Forensics and Security (WIFS). 2012. pp. 234-239.

8. Кривошеев И.А., Линник М.А., Динамический способ стеганографического встраивания информации на основе LSB // Информационные технологии и вычислительные системы. 2022. № 3. С. 24-34.
9. Кривошеев И.А., Линник М.А., Способ встраивания конфиденциальной информации в цветное изображение // Патент РФ на изобретение № 2749880 от 18.06.2021. Бюл. № 17.
10. Pfitzmann A., Westfeld A. Attacks on Steganographic Systems. Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools and Some Lessons Learned. IH 1999. LNCS, 1768: pp. 61-76.
11. Westfield A., Pfitzmann A. Attacks on Steganographic Systems Breaking the Steganography Utilities EzStego, Jsteg, Steganosand S-Tools and Some Lessons Learned // Dresden University of Technology, Department of Computer Science, Information Hiding, Third International Workshop, IH'99 Dresden Germany, September. 1999. pp. 61-76.
12. Fridrich J., Goljan M., Du R. Reliable Detection of LSB Steganography in Color and Grayscale Images // State Univ. of New York, Binghamton, NY, USA. 2001. pp. 27-30.

Кривошеев Игорь Александрович. Хабаровский Федеральный исследовательский центр Дальневосточного отделения РАН, Хабаровск, Россия. Главный научный сотрудник, доктор технических наук. Область научных интересов: информационная безопасность и защита информации, численное моделирование, обработка изображений. E-mail: igork@as.khb.ru

Линник Максим Анатольевич. Хабаровский Федеральный исследовательский центр Дальневосточного отделения РАН, Хабаровск, Россия. Младший научный сотрудник. Область научных интересов: информационная безопасность, численное моделирование, обработка изображений. E-mail: linnik.max1995@mail.ru.

A practical Comparison of the Capabilities of Some Steganographic Methods

I. A. Krivosheev, M. A. Linnik

Khabarovsk Federal Research Center of the Far Eastern Branch of the Russian Academy of Sciences, Khabarovsk, Russia

Abstract. The article discusses the results of the most common methods of steganography. With the help of numerical simulation, the ability to resist steganalysis attacks at various stages related to the amount of information embedding was demonstrated. It was shown that adaptive methods of steganography can be considered the most acceptable.

Keywords: steganography, adaptive steganography, stegoanalysis, RS-steganalysis, Chi-square stegoanalysis, bit-slice analysis.

DOI 10.14357/20718632230410 **EDN** TUNEPY

References

1. Shelukhin, O. I., Kanaev, I.D. 2017. Steganografija. Algoritmy I programmnaja realizacija [Steganography. Algorithms and software implementation] Moskow: Hot line. 592 p.
2. Kokhanovich, GF, Puzyrenko, A.Y. 2006. Komp'juternaja steganografija. Teorija i praktika [Computer steganography. Theory and practice.]. K.: MK-Press. 288 p.
3. Gribunin, V.G., Okov, I.N. 2002. Cifrovaja steganografija [Digital steganography] Moskow: Solon-press. 272 p.
4. Fridrich, J., Long, M. Steganalysis of LSB encoding in color images / J. Fridrich, M. Long // Multimedia and Expo. 2000 IEEE International Conference. 2000. Vol. 3. pp. 1279-1282.
5. Kutter M., Jordan F., Bossen F. Digital Signature Of Color Images Using Amplitude Modulation / M. Kutter, F. Jordan, F. Bossen // Proc. of the SPIE Storage and Retrieval for Image and Video Databases V. 1997. Vol. 3022. pp. 518-526.
6. Pevny T., Filler T., Bas P. Using High-Dimensional Image Models to Perform Highly Undetectable Steganography / T. Pevný, T. Filler, P. Bas // Information Hiding. 2010. pp. 161-177.
7. Holub V., Fridrich J. Designing Steganographic Distortion Using Directional Filters // Proc. 4th IEEE Intern. Workshop on Inform. Forensics and Security (WIFS). 2012. pp. 234-239.
8. Krivosheev I.A., Linnik M.A. 2022. Dinamicheskij sposob steganograficheskogo vstraivaniya informacii na osnove LSB [Dynamic algorithm of steganographic information embedding based on LSB]. Informacionnye tekhnologii i vychislitel'nye sistemy [Journal of Information Technologies and Computing Systems]. 2: 24-34.
9. Krivosheev I.A., Linnik M.A. 2021. Sposob vstraivaniya konfidencial'noj informacii v cvetnoe izobrazhenie [Method for embedding confidential information in a color image]. Patent RF No. 2749880.

10. Pfitzmann A., Westfeld A. Attacks on Steganographic Systems. Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools and Some Lessons Learned. IH 1999. LNCS, 1768: pp. 61-76.
11. Westfield A., Pfitzmann A. Attacks on Steganographic Systems Breaking the Steganography Utilities EzStego, Jsteg, Steganosand S-Tools and Some Lessons Learned // Dresden University of Technology, Department of Computer Science, Information Hiding, Third International Workshop, IH'99 Dresden Germany, September. 1999. pp. 61-76.
12. Fridrich J., Goljan M., Du R. Reliable Detection of LSB Steganography in Color and Grayscale Images // State Univ. of New York, Binghamton, NY, USA. 2001. pp. 27-30.

Krivosheev Igor A. Doctor of Science in technology, leading scientist, Khabarovsk Federal Research Center of the Far Eastern Branch of the Russian Academy of Sciences, Turgeneva street, 51, Khabarovsk, 680000 Russia, e-mail: igork@as.khb.ru.

Linnik Maxim A. Junior scientist, Khabarovsk Federal Research Center of the Far Eastern Branch of the Russian Academy of Sciences, Turgeneva street, 51, Khabarovsk, 680000 Russia, e-mail: linnik.max1995@mail.ru