Душкин Роман Викторович
Директор по науке и технологиям Агентства Искусственного Интеллекта

Яхонтов Светозар Игоревич
Директор по развитию компаний StarForce и Safe'n'Sec, эксперт по информационной безопасности.

Андронов Михаил Григорьевич
Инженер-программист ООО «ВойсЛинк».

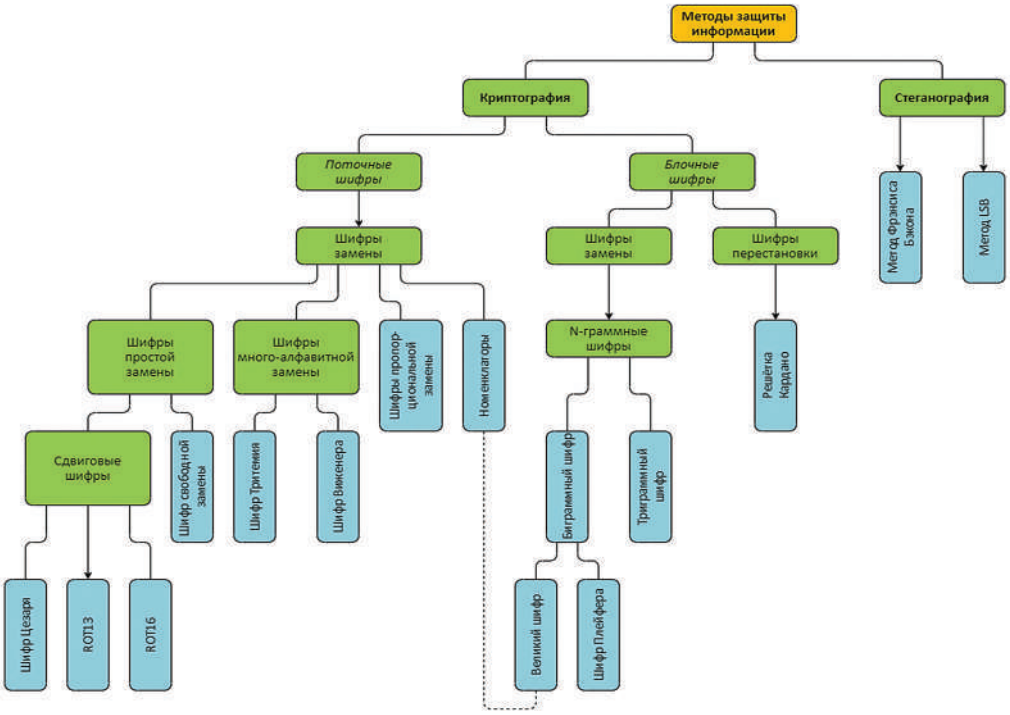
Стеганография LSB

Статья продолжает авторский цикл по криптографии. На этот раз в фокусе внимания авторов располагается ещё один метод стеганографии, который применяется при сокрытии информации в файлах изображений – другими словами, этот метод связан с современными информационно-коммуникационными технологиями и может применяться только на компьютерах. В статье приводится описание метода LSB, даны примеры атак на него, а также даётся ссылка на программу для выделения стеганограммы из изображения. Эта программа может быть использована читателем в качестве отправной точки для самостоятельных исследований.

В предыдущей статье мы рассмотрели стеганографию методом Фрэнсиса Бэкона как метод сокрытия тайного сообщения в произвольном тексте. Уникальное свойство стеганографии как способа передачи тайных посланий через посредника, «у всех на виду», не вызывая подозрений, востребовано сегодня не меньше, чем во времена гусиного пера и письма от руки. Информация и, в особенности, секреты, всегда имела цену. И умение сохранить секрет в современном мире, переда-

вая информацию через любые открытые каналы и публичные источники, пользуясь их доступностью и возможностью мгновенно доставить послание множеству получателей, позволяет добиться большого успеха в политике и бизнесе.

Как обычно, актуализируем нашу диаграмму методов криптографии и стеганографии:



К несомненным плюсам стеганографии в произвольном тексте можно отнести простоту метода. Ведь создать и прочитать скрытое сообщение можно без использования счётных машин и специальных справочников. Однако, минусом такого метода является относительно низкая взломостойкость и заметность стеганограммы для знающего о стеганографии человека. Ведь даже если «Профессор лопух», то «аппаратура при нём!», а экзамены сдать как-то надо.

Как можно было бы скрыть от внимательных глаз сам факт передачи тайного послания?

Правильно! Надо воспользоваться недостатками человеческого зрения. Человеческий глаз лучше различает оттенки зелёного. Это результат эволюции. В дикой природе среди зелёных трав и листьев важно с как можно большего расстояния и как можно раньше заметить хищника или добычу. Примечательно, что многие животные не видят, в нашем представлении восприятия, зелёный цвет. Они воспринимают его как множество оттенков серого. И таких оттенков серого различают больше, чем человек различает оттенков зелёного. Это, в том числе, дает живот-

ным преимущества ночного зрения. Хуже всего человеческий глаз различает оттенки синего цвета. Но это не значит, что надо писать стеганограммы тёмно-синим шрифтом или чернилами. Мы будем пользоваться этим знанием несколько иначе.

Мы сможем скрывать целые тома текста в обычных картинках, которые в неисчислимых количествах публикуется каждый день в социальных сетях и на публичных интернет-ресурсах.

Метод шифрования

В случае картинок и фотографий контейнером (стегоконтейнером) для тайного сообщения (стеганограммы) является файл изображения. Можно рассмотреть структуру такого контейнера на примере файла изображения в формате BMP (от английского Bitmap Picture – картинка представленная в виде «битовой карты» или набора последовательно записанных битов данных). Файл BMP условно можно разделить на 4 части:

- Заголовок файла
- Заголовок изображения
- Палитра
- Само изображение

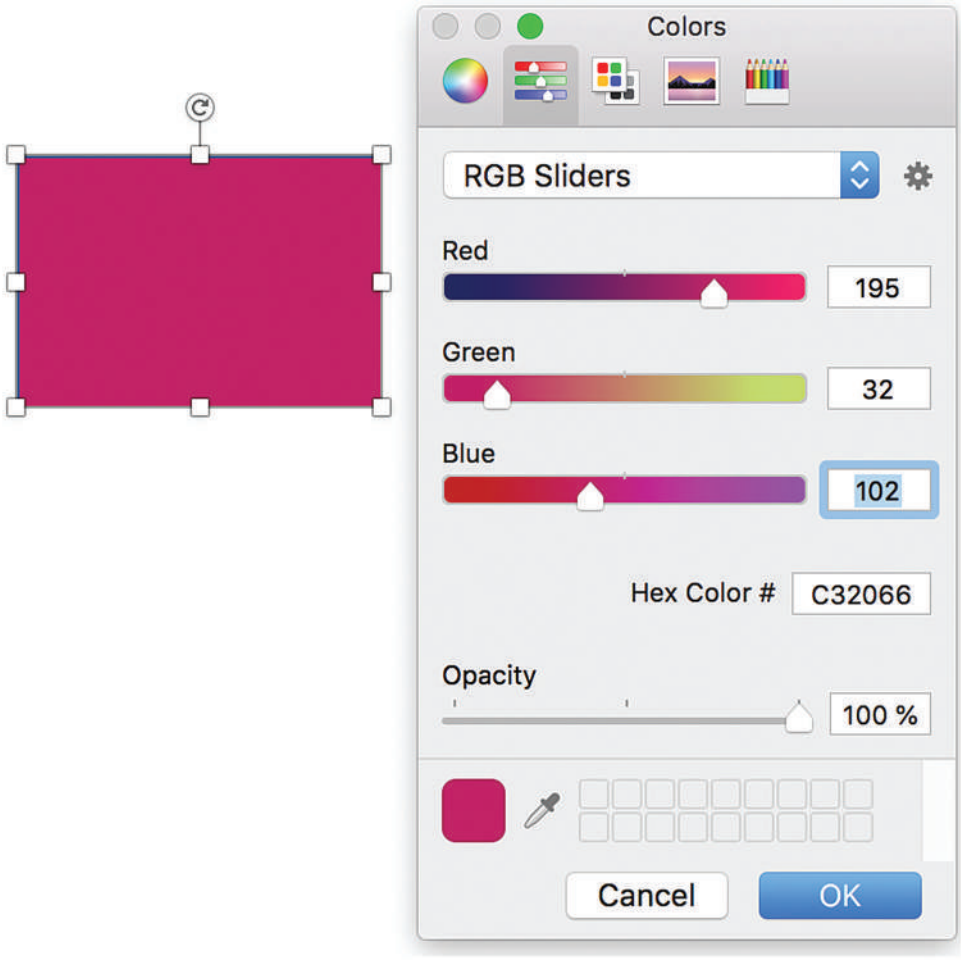
Первые два байта заголовка файла – это сигнатура BM по которой компьютерная программа определяет, что это именно BMP файл изображения. Далее в четырёх следующих байтах записан размер файла. Следующие четыре байта зарезервированы и должны содержать нули. В следующей четвёрке байтов записано смещение от начала файла до байтов, кодирующих изображение. В 24-битном BMP-файле каждый пиксель кодируется тремя байтами RGB (Red, Green, Blue).

В методе стеганографии LSB (от англ. *Least Significant Bit* – наименее значимый бит) биты кода секретного сообщения помещают вместо младших битов (последних, самых малозначимых, на схеме ниже выделено серым) в байтах, отвечающих за кодирование цвета. Изменение оттенка цвета пикселя при замене последнего бита палитры на «0» или «1» будет почти неуловимо человеческим глазом.

Представление байтов, отвечающих за кодирование цвета до внесения стеганограммы:

1	1	0	0	0	0	1	1	R = 195	
0	0	1	0	0	0	0	0	G = 32	
0	1	1	0	0	1	1	0	B = 102	

Возможно, читатель сталкивался с таким представлением палитры в распространённых графических редакторах и офисных программах.



Представление байтов, отвечающих за кодирование цвета после внесения стеганограммы в последние незначащие биты байтов отвечающих за кодирование цвета:

1	1	0	0	0	0	1	0	R’ = 194	
0	0	1	0	0	0	0	1	G’ = 33	
0	1	1	0	0	1	1	1	B’ = 103	

Соответственно, максимальная ёмкость 24-х битного BMP-файла, как стегоконтейнера, при использовании последних битов всех байтов, отвечающих за кодирование трёх цветов, составляет одну восьмую от объёма файла изображения. Например, в файл изображения размером 1080 на

1080 пикселей (это максимальный размер картинки для публикации в популярной социальной сети Instagram) можно поместить стеганограмму всего текста этого выпуска этого журнала. Расчёты таковы:

$$1080 \times 1080 \times 3 \times 1/8 = 437400.$$

Столько байтов текстовой информации можно поместить в картинку в Instagram, а именно 437 400 символов. Эта статья содержит около 30 000 символов.

При чём здесь синий цвет, упомянутый в статье выше? Если для стеганограммы использовать только последние биты байтов, отвечающих за передачу палитры синего цвета (Blue), то это снизит ёмкость файла изображения, как стеганоконтейнера, в три раза, но заметить человеческим глазом наличие стеганограммы в таком изображении даже сопоставив рядом оригинал без стеганограммы будет практически невозможно. Как мы теперь знаем, человеческий глаз хуже всего различает оттенки синего цвета.

Методы атаки

Использование стеганографии в целях тайнописи обусловлено наличием посредника между участниками секретной переписки, где посредник является заинтересованным лицом в компрометации (раскрытии, нарушении секретности) секретного сообщения. Поэтому такой посредник называется «нарушителем». Можно выделить три типа нарушителя, которым должна противостоять стеганограмма:

- *Пассивный нарушитель*. Он может обнаружить факт наличия стеганограммы в контейнере и, возможно, читать сообщения. Обнаружение стеганограммы в контейнере является наиболее трудоёмкой задачей, а защита от обнаружения считается основной задачей стеганографии.
- *Активный нарушитель*. Он может удалить или разрушить стеганограмму в контейнере.
- *Злоумышленный нарушитель*. Он способен создавать ложные стеганограммы в контейнере.

Компрометация факта наличия стеганограммы в контейнере

- *Субъективная атака (в данном случае «субъективный» – основанный на ощущениях, чувствах)*. Нарушитель внимательно рассматривает изображение, пытаясь определить «на глаз», имеется ли в изображении скрытое сообщение. Такая атака может быть проведена только против незащищённых стеганограмм. Дополнительные возможности нарушителю могут дать наличие в картинке областей с однотонной заливкой. В этом случае даже если стеганограмма была внесена в контейнер в последние биты байтов, отвечающих за синий цвет, и изменение фона соседних пикселей нельзя определить «на глаз», то простое сравнение последних битов в соседних пикселях позволит выявить наличие шума, являющегося признаком наличия стеганограммы. Поэтому следует избегать использования в качестве контейнеров изображений с однотонными участками.

- *Атака на основе известного пустого контейнера.* В этом случае нарушителю достаточно провести простое сравнение пустого и заполненного контейнеров, после чего выделить шум, наличие которого скомпрометирует факт наличия стеганограммы. Очевидно, что методом противодействия такой атаке будет однократное использование в качестве пустого контейнера уникальных недоступных нарушителю изображений.
- *Атака на основе известного заполненного контейнера.* Если встраивание скрытой информации осуществлялось одним и тем же способом раз от раза в разные изображения, то наличие повторяющихся признаков внесения изменений в данные изображения даст возможность нарушителю как скомпрометировать факт наличия стеганограммы, так и упростит анализ других стеганографических сообщений. Смена способа внесения стеганограммы в контейнер, например последовательность чередования байтов, ответственных за цвет пиксела, в которые вносится изменённый последний бит, является действенным методом противодействия атаке такого типа.
- *Атака на основе известной математической модели контейнера или его части.* Нарушитель может определить отличие подозрительного шума в известной ему модели. Например, биты внутри изображения могут быть как-то скорелированы друг с другом, как в случае с участками изображения с плавным переходом тонов (градиентом цвета) – значения байтов пикселей ответственных за передачу цвета входящие в область плавного перехода тонов будут изменяться линейно, и отличие значений байт от пикселя к пикселю по нелинейной зависимости будет нарушением математической модели. Нарушение корреляции может быть признаком наличия скрытого сообщения. Поэтому при использовании стеганографии важно не нарушать статистики контейнера при внедрении сообщения.

Вышеперечисленные методы атаки не изменяют стеганографическое сообщение.

Воздействие на заполненный контейнер с целью разрушения стеганограммы

Изображение как контейнер может быть подвержено различным преобразованиям на пути к получателю:

- Преобразование файла изображения в другой формат, например сжатие JPEG, то есть преобразование файла изображения из формата .BMP в формат .JPEG.
- Сжатие изображения с потерями.
- Изменение разрядности цветовой шкалы с 8 до 7 бит.
- Применение очищающих изображение от шумов методов, использующих оценивание и вычитание шума – такие алгоритмы преобразования изображения используются для избавления от шумов матрицы на недоэкспонированных фотоснимках, снятых в условиях слабого освещения.
- Линейная и нелинейная фильтрация – методы преобразования изображения, сглаживающие переходы цветов на участках изображения.
- Выравнивание гистограммы – искусственное улучшение участ-

ков фотографии, снятой в сложных условиях освещения (например, при съёмке помещения с яркой засветкой через окно или при наличии ярких искусственных источников освещения).

- Изменение контрастности изображения.
- Ошибки при передаче файла изображения по каналу связи.
- Простая обрезка изображения.

Например, фотокамера современных мобильных телефонов может производить съёмку и обработку изображения алгоритмом HDR (High Dynamic Range – высокий динамический диапазон). Алгоритм HDR заключается в съёмке сразу нескольких изображений («одновременных попыток») с разной экспозицией (настройками уровня освещённости кадра), после чего итоговое изображение собирается из удачных (не засвеченных и не недоэкспонированных) участков изображения из «одновременных попыток». Итоговая картинка получается впечатляюще удачной («лучше настоящего») – облака не пересвечены, участки изображения в тени достаточно освещены. Такая обработка может разрушить стеганограмму. Потому, например, контроль за утечками информации при способе кражи информации посредством съёмки секретного документа с экрана компьютера на смартфон реализуется посредством иных типов стеганографии, не чувствительных к таким типам атак. Например, посредством разбиения выводимого изображения на мозаику элементов и незаметных глазу смещений элементов мозаики на величину и направление, параметры которых и являются данными стеганограммы. В качестве секретного сообщения в таких случаях используются идентификаторы компьютера или пользователя, которые и позволяют выявить, кто мог быть источником утечки.

Методы противодействия таким атакам предполагают повышение робастности стеганографического сообщения. В данном случае «робастность» – это устойчивость сохранять свойства целого в отделённой от целого части, достигается внесением избыточной информации в отдельный элемент изображения содержащей данные об информации в соседних элементах изображения – как повторяющийся мозаичный узор в картинке. Для этих целей могут быть использованы различные методы:

- Применение предварительной низкочастотной фильтрации на основе различных вариантов скользящего среднего – изображение, как контейнер, предварительно подготавливается к внесению стеганограммы таким образом, чтобы алгоритмы сглаживания переходов цвета не определяли необходимость преобразования цветов на участках изображения, где внесена стеганограмма.
- Применение математических моделей ключа встраивания сообщения, учитывающих возможные преобразования. Например, мозаичное разбиение изображения и применение алгоритма ключа, позволяющего восстановить стеганограмму по данным в соседних элементах мозаики.
- Другие методы из классической теории связи.

Заключение

В современном мире стеганографию в изображениях используют как в благих целях, так и злоумышленники. В первом случае это, например

- для защиты авторских прав на фотоснимки профессиональными фотографами – имя автора фотографии современные профессиональные цифровые фотоаппараты вносят стеганограммой в файл фотоснимка;
- для защиты конфиденциальной информации в организациях от утечек посредством фотографирования документов с экрана компьютера — данные об идентификаторе компьютера и пользователя вносятся в выводимое на экран изображение различными методами стеганографии.

Вот пример использования злоумышленниками.

- Известны случаи, когда зловредный код компьютерных вирусов доставлялся в сеть организации как стеганограмма в файлах изображений. Используя известные злоумышленникам уязвимости программного обеспечения, используемого в атакуемой организации, приводящие к исполнению зловредного кода при обработке изображения (прочтению файла изображения уязвимой программой), производилось заражение компьютеров организации и последующий перехват управления компьютерами сотрудников. Детектирование таких зловредов до сих пор является трудно-решаемой задачей из-за сложного математического обеспечения алгоритмов выявления наличия стеганограмм и большого количества изображений проходящих через периметр информационных систем организаций.

Знания в области современной стеганографии становятся всё более востребованными в индустрии информационной безопасности. Специалисты с таким знаниями крайне востребованы в ведущих российских и мировых компаниях занимающихся передовыми разработками в области защиты информации.

Упражнения

В качестве домашнего задания и самостоятельных упражнений рекомендуем выполнить следующее:

Расшифруйте следующее зашифрованное послание:

1. По ссылке https://yadi.sk/i/OcPnai4lvUggow скачайте файл изображения и сохраните его на жёсткий диск своего компьютера. Этот файл содержит скрытое методом стеганографии LSB секретное слово. Стеганограмма внесена в последние значимые биты байт ответственных за передачу синего цвета в пикселах находящихся в конце файла (с последнего к первому). На изображении эти пикселы расположены рядом справа налево от правого верхнего угла картинки. Секретное слово состоит из 12 букв кириллицей.

2. Установите на компьютер интерпретатор языка программирования Python. Скачать интерпретатор можно на официальном сайте www.python.org совершенно бес-

платно. Неважно, какую сборку вы установите, важно чтобы номер версии начинался на 3.

3. После установки интерпретатора Python на компьютер скачайте по ссылке https://yadi.sk/d/_z1R7Y5Y8wwPhA программу на языке Python, написанную для этого задания. Эта программа позволяет извлечь стеганограмму из вышеуказанного файла изображения. В программе уже учтено, что стеганограмма внесена в последние пикселы изображения с конца файла и находится в последних битах байтов ответственных за синий цвет.

4. Запустите интерпретатор командной строки на вашем компьютере. На компьютере с операционной системой Windows таким интерпретатором является программа **cmd.exe**.

5. В командной строке следует написать: python <путь до скрипта> -i <путь до картинки> -p <количество пикселей>.

6. Количество пикселей следует рассчитать исходя из описания задачи.

7. Результатом выполнения команды будет вывод в окне интерпретатора командной строки секретного слова этой статьи.

Калейдоскоп Калейдоскоп Калейдоскоп

Российские физики изучили условия, при которых не выполняется третий закон Ньютона

Иллюстрация нарушения третьего закона Ньютона

«Третий закон Ньютона, который все помнят из школьной программы, утверждает, что сила действия равняется силе противодействия. Однако для некоторых открытых и неравновесных дисперсных систем — частиц в среде — симметрия эффективной силы межчастичного взаимодействия может нарушаться, и возникает очень интересная физика: например, частицы самоорганизуются в сложные структуры, система аномально разогревается, появляются необычные неравновесные фазовые переходы», — комментирует Евгений Лисин.

Впервые такую систему с несимметричным взаимодействием частиц удалось получить в конце 90-х годов прошлого века в Германии. С тех пор, было проведено множество исследований. Однако, несмотря на богатую теоретическую базу, одной из важных нерешенных проблем оставалось прямое экспериментальное исследование. Точно измерить силу межчастичного взаимодействия и определить степень нарушения симметрии в зависимости от условий среды ранее не удавалось.

Решение этой проблемы стало возможным благодаря оригинальному спектральному методу измерения, который был разработан учеными МФТИ и ОИВТ РАН при поддержке Российского научного фонда. Метод учитывает случайные и диссипативные процессы в системе, не требует усложнения экспериментальной установки, предварительных измерений внешних полей и каких-либо предположений о типе изучаемого взаимодействия. Полная версия статьи: https://zanauku.mipt.ru