УДК 004.056.5 DOI:10.31854/1813-324X-2020-6-1-70-76

Обнаружение видео стегосистем универсальным методом, основанным на использовании NIST-тестов

К.А. Ахрамеева[1], В.И. Коржик[1*], З.К. Нгуен[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация
[*]Адрес для переписки: val-korzhik@yandex.ru

Информация о статье
Поступила в редакцию 01.11.2019
Принята к публикации 27.01.2020

Ссылка для цитирования: Ахрамеева К.А., Коржик В.И., Нгуен З.К. Обнаружение видео стегосистем с использованием универсального метода, основанного на использовании NIST-тестов // Труды учебных заведений связи. 2020. Т. 6. № 1. С. 70–76. DOI:10.31854/1813-324X-2020-6-1-70-76

Аннотация: *В статье предлагается универсальный метод обнаружения видео стегосистем, предложенный недавно авторами и основанный на использовании NIST-тестов. Описывается алгоритм обнаружения и оценивается его эффективность в терминах вероятностей пропуска и ложного обнаружения. Рассматривается возможность улучшения стойкости к обнаружению таких стегосистем за счет уменьшения скорости вложения в них скрытной информации.*

Ключевые слова: *видео стегосистема, алгоритмы вложения и извлечения, NIST-тесты, скорость вложения информации, вероятности пропуска и ложного обнаружения.*

1. Введение

Стеганография – это технология скрытного погружения информации, которая, в отличие от криптографии, скрывает не только содержание конфиденциальной информации, но и сам факт ее присутствия в некоторых «невинных», на первый взгляд, покрывающих объектах (ПО). В настоящее время она широко применяется как в государственных структурах, так и в бизнес-сообществе. В качестве ПО могут использоваться: неподвижные и подвижные (видео) изображения, аудиосигналы, текстовые документы и др.

В литературе описано множество алгоритмов погружения и извлечения конфиденциальной информации. Наиболее известные из них: погружение в наименьшие значащие биты (НЗБ) цифровых ПО, использование широкополосных сигналов, системы с адаптивным квантованием и т. д. Наиболее полное описание стегосистем (СГ) представлено в монографии [1]. При практической реализации СГ к ним предъявляются следующие требования: устойчивость к обнаружению; малые искажения ПО; максимизация скорости вложения; устойчивость к удалению вложенной информации (при условии, что процедура ее удаления незначительно искажает ПО).

К сожалению, полное выполнение всех требований для «реальных» ПО (таких, как изображение, звук и печатный текст) оказывается невозможным. Так, обеспечение идеальной секретности (т. е. необнаруживаемости вложений наилучшими методами) оказывается возможным только для лингвистической СГ или для СГ в каналах с шумом [2]. Однако в первом случае скорость вложения мала и легко допускается удаление вложений информации без искажения ПО, а для второго – необходимым условием является возможность обнаружения только по каналам с шумом, которые присутствуют далеко не всегда. Помимо интереса к разработке собственно СГ, возникает большой интерес и к алгоритмам их обнаружения. Это объясняется требованиями информационной безопасности к цифровым ПО. Так, например, в DLP-системе (*от англ.* Data Leak Prevention), насколько авторам известно, вообще не предусмотрены методы обнаружения вложений, а это значит, что утечка из внутреннего во внешний информационный контур компаний легко может быть реализована с использованием СГ. Поэтому построение эффективных алгоритмов их обнаружения является весьма актуальной задачей, как в теоретическом, так и в практическом плане (некоторые алгоритмы обнаружения СГ описаны в [1]).

Сложность решения данной задачи определяется следующими обстоятельствами:

– алгоритмы вложения и извлечения конфиденциальной информации не всегда известны и часто они определяются секретным стегоключом;

– статистика ПО является достаточно сложной и трудно поддающейся описанию простыми моделями;

– конфиденциальные сообщения перед вложением обычно подвергаются шифрованию стойкими шифрами (такими, как ГОСТ, 3-DES, AES и др.) [3].

Последнее условие объясняется следующими обстоятельствами. Во-первых, шифрование обеспечивает дополнительную защиту конфиденциальной информации от чтения содержания, если все же стегоаналитику удается обнаружить присутствие СГ и найти стегоключ. Во-вторых, если вложенное сообщение не было предварительно зашифровано, то стегоаналитик может опробовать возможные алгоритмы извлечения, и если хоть один из них приведет к смысловому тексту, то это будет доказывать факт присутствия СГ. Поэтому далее будем полагать, что вкладываемое в ПО конфиденциальное сообщение всегда предварительно зашифровывается стойким шифром. Заметим, что данный факт является положительным для рассматриваемого метода стегоанализа (СГА).

В настоящее время наиболее популярны такие ПО, как неподвижные изображения или текстовые документы на каком-либо языке. Однако выбор в качестве ПО цифровых видеопотоков также представляет интерес, поскольку это позволяет вложить значительно бóльшие объемы «секретной» информации. Кроме того, такое направление менее исследовано, что и определило тематику настоящей статьи.

Данная работа структурирована следующим образом. В Разделе 2 описан в общем виде новый метод СГА, основанный на использовании NIST-тестов. Раздел 3 посвящен описанию метода вложения и извлечения информации в цифровой видеопоток формата MPEG-2, а также метод обнаружения такой СГ на основе NIST-тестов. Раздел 4 представляет результаты моделирования СГ, описанного в Разделе 3, а также его анализ методом, описанным в Разделе 2. Раздел 5 содержит описание эффективности обнаружения метода модификации СГ, обеспечивающего улучшение ее необнаруживаемости. В Заключении суммируются результаты работы, и предлагаются направления возможных дальнейших исследований.

2. Описание метода стегоанализа, основанного на использовании NIST-тестов

Данный метод СГА был впервые предложен и описан в работе [4]. Он базируется на следующем достаточно очевидном факте: *информация, извлекаемая по известному алгоритму из предполагаемой СГ, представляет собой криптограмму и поэтому, в случае шифрования сообщения перед вложением стойким шифром, последовательности извлекаемых бит должны удовлетворять известным NIST-тестам на псевдослучайность; если же вложение в ПО не выполнялось, то извлекаемые последовательности бит не будут (хотя бы частично) удовлетворять NIST-тестам.*

Что касается знания алгоритма извлечения из предполагаемой СГ, то некоторые СГ (например, с НЗБ) имеют открытый и общеизвестный алгоритм извлечения; другие, основанные, например, на матричных методах погружения [2], имеют *стегоключ*, который и определяет алгоритм извлечения (однако этот ключ можно найти простым перебором возможного множества стегоключей [5]).

В таблице 1 представлен список 15-ти NIST-тестов в соответствии со стандартом [6]. Алгоритмы, выполняющие тестирование двоичных последовательностей в соответствии со стандартом, доступны в Интернете.

ТАБЛИЦА 1. Названия NIST-тестов на псевдослучайность

TABLE 1. Titles of NIST Tests on Pseudo Randomness

№ п/п	Название теста
1	The frequency test
2	Frequency test within a block
3	The runs test
4	Tests for the longest-run-of-ones in a block
5	The binary matrix rank test
6	The discrete Fourier transform (spectral) test
7	The non-overlapping template matching test
8	The overlapping template matching test
9	Maurer's "Universal Statistical" test
10	The linear complexity test
11	The serial test
12	The approximate entropy test
13	The cumulative sums (cusums) test
14	The random excursion teat
15	The random excursions variant test

Алгоритм обнаружения на основе использованных NIST-тестов состоит из следующих трех шагов:

Шаг 1. Извлечь из предполагаемой СГ вложенную двоичную последовательность;

Шаг 2. Применить весь набор NIST-тестов к извлеченной последовательности;

Шаг 3. Принять решение о наличии СГ, если все тесты «проходят», и об ее отсутствии – в противном случае.

Возможны некоторые обобщения представленного выше алгоритма, когда задается порог на количество прошедших тестов для решения о присутствии СГ, а также использование *метода опорных векторов* (SVM, *от англ.* Support Vector Machine) с нелинейным ядром [1]. В последнем

случае производится предварительное обучение на достаточно большой выборке СГ с одинаковыми алгоритмами вложения.

Авторы назвали свой метод СГА *универсальным*, поскольку он годится для стегоанализа любых СГ, если известен (или допускает вычисление) алгоритм извлечения, и не требует знания алгоритма погружения и статистики ПО, в который погружается «секретная» информация. В отличие от заявленного метода, известные алгоритмы СГА требуют знания статистики ПО и статистики СГ после погружения по известному алгоритму, что представляет собой весьма сложную задачу. Метод СГА на основе использования NIST-тестов в некотором «метафорическом смысле» является *несимметричным* по сравнению с традиционными методами СГА: он обнаруживает не изменение статистики от ПО к СГ, а присутствие псевдослучайности для СГ по сравнению с «плохой» псевдослучайностью ПО.

3. Описание СГ для видеосигналов стандарта MPEG-2 и ее стегоанализа на основе использования NIST-тестов

Можно предложить достаточно алгоритмов погружения для ПО в виде MPEG-2 файла, однако наиболее типичным и часто используемым является метод на основе вложения в НЗБ DCT-коэффициентов. В этом случае алгоритм погружения выполняется следующими шагами:

Шаг 1. Зашифровать вкладываемое сообщение стойким шифром;

Шаг 2. Выделить из видеофайла I-кадры и выполнить для каждого I-кадра DCT-преобразования в областях размером 8×8 пикселей;

Шаг 3. Найти номер $\hat{\jmath}$ DCT-коэффициента для каждой 8×8 области взятой из каждого I-кадра:

$$\hat{\jmath} = \arg\min_{j}\min_{k}\left[\left(q_k + \frac{\Delta}{2}\right) - S_j\right]^2; \quad j = 1, \dots, N, \qquad k = 1, \dots, L, \tag{1}$$

где: q_k – k-ый уровень квантования DCT-коэффициентов; Δ – интервал квантования; S_j – j-ый DCT-коэффициент в каждой из 8×8 области; N – количество ненулевых DCT-коэффициентов S_j в каждой области; L – количество уровней квантования.

Шаг 4. Произвести вложение по одному информационному биту b в каждую из областей I-ых кадров видеофайла, изменяя (если необходимо) наименьший значащий бит $\hat{\jmath}$-го DCT-коэффициента в каждой 8×8 области так, чтобы выполнялось равенство:

$$b = \sum_{j} \text{НЗБ}(j) \bmod 2. \tag{2}$$

Наглядно процедура такого вложения означает следующее. В каждой из 8×8 областей всех I-кадров выбирается единственный DCT-коэффициент, который находится на минимальном квадратичном расстоянии до середины между какими-либо уровнями квантования. (Это делается для того, чтобы минимизировать изменения статистики видеосигнала после вложения). Затем в данный DCT-коэффициент производится вложение бита по правилу СГ с НЗБ [1, 2]. Важным преимуществом такого метода вложения является тот факт, что для извлечения вложенного бита из каждого I-кадра нет необходимости находить $\hat{\jmath}$-ый DCT-коэффициент. Достаточно лишь выполнить сложение по модулю 2 НЗБ всех ненулевых DCT-коэффициентов в каждой из 8×8 областей и принять решение о вложении бита $b = 0$ в данную область, если эта сумма равна 0, и о вложении бита $b = 1$ в противном случае.

Хотя, на первый взгляд, объем вложения кажется небольшим (один бит в каждой из 8×8 областей всех I-кадров), но для видеофайла стандарта MPEG-2 продолжительностью 3 минуты он оказывается в среднем равным $3{,}2 \cdot 10^6$ бит для видеокадров размером 720×576 пикселей, что вполне достаточно для многих практически реальных ситуаций.

Для обнаружения СГ в каком-либо видеофайле на основе использования NIST-тестов, который был ранее представлен в Разделе 2, выполняются следующие шаги:

Шаг 1. Выделяются I-кадры в видеофайле;

Шаг 2. Производятся вычисления DCT-коэффициентов для каждой из 8×8 областей во всех I-кадрах;

Шаг 3. Извлекаются вложенные биты предполагаемой криптограммы (по одному для каждой из 8×8 областей I-кадров);

Шаг 4. Извлеченные биты проверяются на псевдослучайность при помощи NIST-тестов.

При прохождении всех (или заданного количества тестов выше определенного порога) принимается решение о наличии СГ. В противном случае принимается решение об отсутствии вложения.

4. Экспериментальное исследование метода обнаружения видео СГ на основе использования NIST-тестов

В таблице 2 представлены результаты прохождения 15-ти NIST-тестов для 15 различных двоичных криптограмм, полученных при шифровании по ГОСТ-28147-89. Серым цветом отмечено прохождение теста для выбранной криптографии, белым цветом – не прохождение. Заметим, что в данном случае нет необходимости извлекать для этого информацию из видеофайла, поскольку при наличии СГ и известного правила извлечения всегда будут получены криптограммы того шифра, которым были зашифрованы вложенные сообщения.

В таблице 3 представлены результаты прохождения различных тестов (в %) для 1000 различных криптограмм, каждая из которых имеет длину 10^6 бит.

ТАБЛИЦА 2. Результат NIST-тестирования для 15-ти криптограмм шифра ГОСТ-28147-89

TABLE 2. Results of NIST Testing for 15 Encrypted Sequences by Cipher GOST-28147-89

NIST тест	Криптограмма														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
2	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
3	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
4	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
5	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
6	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
7	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
8	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
9	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
10	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
11	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
12	■	■	■	■	■	■	■	■	■	■	■	■	■	■	
13	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
14	■	■				■	■	■	■	■		■		■	
15	■	■				■	■	■		■		■	■	■	

ТАБЛИЦА 3. Частость (в %) прохождение NIST-тестов для 1000 криптограмм, зашифрованных шифром ГОСТ-28147-89

TABLE 3. Pass Rates (in Percent) of Passed NIST Tests Obtained for Statistic Constituting of 1000 Encrypted Sequences by Cipher GOST-28147-89

NIST-тест	1	2	3	4	5	6	7	8
Частость	98,9	99,5	99,1	98,4	99,4	99,2	99,8	98,8
NIST-тест	9	10	11	12	13	14	15	
Частость	98,8	99,2	98,4	99,0	98,6	69,7	70,0	

Результаты таблицы 3 показывают, что в 13-ти из 15-ти NIST-тестов частость их прохождения для криптограмм шифра ГОСТ оказывается более 98 %. Однако, для окончательного суждения об эффективности предлагаемого метода обнаружения, необходимо исследовать прохождение тестов при отсутствии вложения, т.е. для обычных видеофайлов стандарта MPEG-2.

В таблице 4 представлены результаты тестирования 15-ти двоичных последовательностей, извлеченных по правилу (2) из различных MPEG-2 файлов без вложения. В таблице 5 показана частость прохождения тестов (в %) при извлечении по правилу (2) из 1000 MPEG-2 файлов без вложения.

Сравнивая таблицы 2 и 4, а также таблицы 3 и 5, легко видеть, что они существенно отличаются. Это обстоятельство позволяет выбрать порог относительно количества NIST-тестов для принятия решения об обнаружении СГ. В таблице 6 представлены зависимости вероятностей пропуска СГ P_m и ложного обнаружения P_{fa} от величины выбранного порога.

ТАБЛИЦА 4. Результаты тестирования для последовательностей, извлеченных по правилу (2)

TABLE 4. Results of NIST Testing for Sequences Extracting from MPEG-2 files without Embedding Based on the Formula 2

NIST тест	Криптограмма														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	■	■	■	■	■	■	■			■	■		■	■	■
2		■		■	■		■				■		■	■	■
3		■								■	■		■	■	■
4		■	■		■		■	■		■	■		■	■	■
5		■	■	■	■	■	■	■	■	■	■	■	■	■	■
6		■	■	■	■	■	■	■	■		■	■	■	■	
7		■	■		■		■				■		■	■	■
8		■	■	■	■		■	■		■	■		■	■	■
9		■	■	■	■		■	■		■	■		■	■	■
10	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
11		■		■		■		■						■	■
12		■						■						■	■
13		■	■	■	■		■			■	■		■	■	
14			■	■	■		■	■		■	■	■			■
15			■	■	■		■	■		■	■	■			■

ТАБЛИЦА 5. Частость (в %) прохождения тестов для 1000 последовательностей, извлеченных по правилу (2) из MPEG-2 файлов без вложения

TABLE 5. Pass Rates (in percent) of Passed NIST Tests Obtained for Statistic Constituting of 1000 Sequences Extracting from MPEG-2 Files without Embedding Based on the Formula 2

NIST-тест	1	2	3	4	5	6	7	8
Частость	49,0	45,9	29,1	66,0	96,2	82,5	53,2	68,4
NIST-тест	9	10	11	12	13	14	15	
Частость	68,4	97,2	43,8	45,7	43,0	32,1	33,2	

Для минимизации полной вероятности ошибки обнаружения СГ $P_e = \frac{1}{2}(P_m + P_{fa})$ целесообразно выбрать порог, равный прохождению 13 NIST-тестов (см. таблицу 6). В этом случае $P_e = 11{,}15$ %.

Лучшего результата можно добиться, используя технику SVM. Для эксперимента была выбрана SVM с нелинейным взвешиванием и выбором гауссовского ядра [1]. Параметр SVM C, который называется «box constraint», был оптимизирован для получения минимальной вероятности ошибки. В таблице 7 показаны вероятности ошибок при оптимальном выборе параметров SVM, когда для «тренировки» SVM и тестирования было использовано по 1000 различных видеофайлов.

Видно, что в случае использования техники SVM вероятность ошибки обнаружения СГ оказывается значительно меньше, чем при использовании порогового метода. Однако этот результат достигается за счет использования значительно бóльших ресурсов на стадии тренировки SVM.

ТАБЛИЦА 6. Зависимость вероятностей ошибок P_m, P_{fa} и P_e (в %) от величины порога прохождения NIST-тестов

TABLE 6. The Probabilities P_m P_{fa} and P_e Against Chosen Threshold Values of Passed NIST Tests

Порог	P_m (%)	P_{fa} (%)	P_e (%)
0	0	100	50
1	0	99,9	49,95
2	0	98,7	49,35
3	0	93,5	46,75
4	0	85,7	42,85
5	0	82,4	41,2
6	0	75,9	37,95
7	0	69,7	34,85
8	0	59,8	29,9
9	0	53,9	26,95
10	0	47	23,5
11	0,2	37,2	18,7
12	1,4	26,3	13,85
13	3,5	18,8	11,15
14	27,7	3	15,35
15	40,4	1,9	21,15

ТАБЛИЦА 7. Вероятности ошибочного обнаружения СГ при использовании техники SVM с оптимальным выбором параметров и при тренировке и тестировании на 1000 различных видеофайлах

TABLE 7. The Best Probabilities of Error for Detecting Stegosystem Obtained Due to SVM Technique with Optimal Parameters γ and C for Each 1000 Different Video-Files on Training Stage and Testing Stage

SVM-параметры	$\gamma = 32; C = 1$
P_{fa}(%)	8,6
P_m(%)	1,8
P_e(%)	5,2

5. Результаты эксперимента по обнаружению модифицированной схемы видео СГ

Как было отмечено ранее, вложение по одному биту в каждую из 8×8 областей *I*-кадров обеспечивает достаточно большой объем вложения даже для 3-минутного файла. Если не требуется такого большого объема вложения, то можно повысить стойкость к обнаружению данной СГ, вкладывая информацию не во все, а лишь в некоторые *I*-кадры, выбираемые при вложении и извлечении по секретному (и согласованному ранее) стегоключу. В качестве основного примера были выбраны две скорости частичного вложения: 25 % и 50 % в среднем (когда *I*-кадры выбираются по стегоключу).

Поскольку секретный стегоключ предполагается неизвестным стегоаналитику, то процедура СГА производится для случайного погружения в *I*-кадры абсолютно так же, как она выполнялась (см. Раздел 3) и для 100-процентного погружения.

Конечно, в случае погружения по стегоключу, часть *I*-кадров не будет содержать биты криптограммы, а лишь биты, извлеченные из обычного видеофайла, и это обстоятельство должно ухудшить эффективность обнаружения. В таблице 8 представлены величины частостей прохождения NIST-тестов (в %) для случая 25 % и 50 % скорости погружения.

ТАБЛИЦА 8. Частость прохождения NIST-тестов для скорости погружения 25 % и 50 % при статистике 1000 файлов для каждого случая

TABLE 8. Pass Rates (in Percent) of Passed NIST Tests Obtained for Statistic Constituting of 1000 Sequences for Each Test within Embedding Rates = 25 % and 50 %

	NIST-тест/ Частость							
Скорость погружения в I-кадр	1	2	3	4	5	6	7	8
25 %	59,3	54,3	40,6	72,5	97,4	83,4	61,9	74,1
50 %	74,3	64,0	56,3	79,7	97,9	84,5	71,9	79,1
Скорость погружения в I-кадр	9	10	11	12	13	14	15	
25 %	74,1	98,8	49,3	54,0	54,8	40,1	42,1	
50 %	79,1	98,8	56,1	62,6	70,4	53,3	53,4	

Сравнивая результаты таблицы 8 и таблицы 3, можно увидеть их существенную разницу, особенно для скорости 25 %. Для того, чтобы оценить количественное улучшение стойкости обнаружения СГ при уменьшении скорости вложения, в таблицах 9 и 10 показаны достижимые вероятности ошибок обнаружения при выборе порогового метода.

ТАБЛИЦА 9. Вероятности ошибочного обнаружения СГ при выборе различных порогов при средней скорости вложения 25 %

TABLE 9. The Probabilities of Error for Detecting Stegosystem within Embedding Rate = 25 %, Against Chosen Threshold Values of Passed NIST Tests

Порог	P_m (%)	P_{fa} (%)	P_e (%)
0	0	100	50
1	0	99,9	49,95
2	0,6	98,7	49,65
3	5,3	93,5	49,4
4	10,6	85,7	48,15
5	13,4	82,4	47,9
6	19,1	75,9	47,5
7	24,6	69,7	47,15
8	31,2	59,8	45,5
9	37,5	53,9	45,7
10	43,4	47	45,2
11	50,3	37,2	43,75
12	60,9	26,3	43,6
13	70,1	18,8	44,45
14	84,6	3	43,8
15	91,7	1,9	46,8

Из данных таблиц видно, что при уменьшении скорости вложения вероятность ошибки существенно возрастает.

Некоторого улучшения результатов обнаружения можно, конечно, добиться, применяя технику SVM. В таблице 11 показаны результаты такого эксперимента. Видно, что P_e несколько уменьшилась, но, все же, она оказывается достаточно большой, особенно при скорости 25 %, когда в среднем каждая из четырех СГ или ПО будет классифицирована с ошибкой.

ТАБЛИЦА 10. Вероятности ошибок обнаружения СГ в зависимости от выбора порога при средней скорости вложения 50 %

TABLE 10. The Probabilities of Error for Detecting Stegosystem within Embedding rate = 50 %, Against Chosen Threshold Values of Passed NIST Tests

Порог	P_m (%)	P_{fa} (%)	P_e (%)
0	0	100	50
1	0	99,9	49,95
2	0,6	98,7	49,65
3	4,2	93,5	48,85
4	7,5	85,7	46,6
5	8,9	82,4	45,65
6	11,9	75,9	43,9
7	16,6	69,7	43,15
8	20,4	59,8	40,1
9	26	53,9	39,95
10	30,9	47	38,95
11	37	37,2	37,1
12	45,2	26,3	35,75
13	54,9	18,8	36,85
14	72	3	37,5
15	82,5	1,9	42,2

ТАБЛИЦА 11. Вероятности ошибок обнаружения СГ при использовании техники SVM для скорости 25 % и 50 %

TABLE 11. The Probabilities of Error for Detecting Stegosystem within Embedding rates = 25 % and 50 % Obtained Due to SVM Technique

Скорость погружения в I-кадр	25 %	50 %
SVM параметры	$\gamma = 64; C = 4$	$\gamma = 128; C = 4$
P_{fa}(%)	22,4	23,8
P_m(%)	19,4	9,0
P_e(%)	20,9	16,4

Заключение

В работе рассмотрено применение авторского метода обнаружения видео СГ формата MPEG-2 на основе использования NIST-тестов. Метод вполне пригоден для обнаружения, особенно, при использовании техники SVM. Установлено, что стойкость видео СГ к обнаружению может быть существенно улучшена при снижении скорости вложения в I-кадры по стегоключу. Дополнительные результаты исследования показали, что при скорости вложения не более 5 % вероятность обнаружения СГ близка к «случайному угадыванию» СГ и ПО.

В качестве перспективных, на взгляд авторов, направлений исследований обнаружения СГ данным методом, можно указать модифицированную схему СГ с вложением по стегоключу не только в I-кадры, но и в каждую из 8×8 областей различных I-кадров. Еще одним перспективным направлением дальнейших исследований является использование методов модификации шифров для защиты от обнаружения на основе NIST-тестов [7].

Авторы не утверждают, что использование метода обнаружения СГ на основе NIST-тестов является оптимальным среди всех возможных методов обнаружения СГ, однако данный метод является наиболее простым и быстродействующим по сравнению с другими методами обнаружения.

Список используемых источников

1. Fridrich J. Steganography in Digital Media: Principles, Algorithms and Applications. Cambridge: Cambridge University Press, 2009.

2. Коржик В.И., Небаева К.А., Герлинг Е.Ю., Догиль П.С., Федянин И.А. Цифровая стеганография и цифровые водяные знаки. Часть 1. Цифровая стеганография. СПб: СПбГУТ, 2016. 226 с.

3. Коржик В.И., Яковлев В.А. Основы криптографии: учебное пособие. СПб: ИЦ Интермедия, 2016. 296 с.

4. Korzhik V., Fedyanin I., Godlewski A., Morales-Luna G. Steganalysis Based on Statistical Properties of the Encrypted Messages // Proceedings of the 7th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security (MMM-ACNS, Warsaw, Poland, 28–30 August 2017). Lecture Notes in Computer Science. Vol. 10446. Cham: Springer, 2017. PP. 288–298. DOI:10.1007/978-3-319-65127-9_23

5. Korzhik V., Nguyen C., Fedyanin I., Morales-Luna G. Side Attacks on Stegosystems Executing Message Encryption Previous to Embedding // Preprints. 2018. DOI:10.20944/preprints201802.0143.v1

6. Bassham III L.E., Rukhin A.L, Soto J., Nechvatal J.R., Smid M., Barker E., et al. NIST Special Publication 800–22 Revision 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Technical report, Gaithersburg, 2010.

7. Korzhik V., Nguyen D.C., Morales-Luna G. Cipher Modification Against Steganalysis Based on NIST Tests // Proceedings of the 24th Conference of Open Innovations Association (FRUCT, Moscow, Russia, 8–12 April 2019). IEEE, 2019. PP. 179–186. DOI:10.23919/FRUCT.2019.8711958

* * *

Detection of Video Steganography with the Use of Universal Method Based on NIST-Tests

K. Akhrameeva[1], **V. Korzhik**[1], **C. Nguyen**[1]

[1]The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Article info
DOI:10.31854/1813-324X-2020-6-1-70-76
Received 1st November 2019
Accepted 27th January 2020

For citation: Akhrameeva K., Korzhik V., Nguyen C. Detection of Video Steganography with the Use of Universal Method Based on NIST-Tests. *Proc. of Telecom. Universities.* 2020;6(1):72–78. (in Russ.) DOI:10.31854/1813-324X-2020-6-1-70-76

Abstract: *We propose a universal method of video stegosystem detection, which was recently suggested by the authers. They describe the detecting algorithm and its efficiency is presented in terms of the missing and false detection probabilities. The article considers the possibility of the detection resistance of such stegosystems by the means of reducing the speed of embedding secret information in them.*

Keywords: *video stegosystem, algorithms embedding and extraction, NIST-tested embedding rate, the probability of missing and false alarm.*

References

1. Fridrich J. *Steganography in Digital Media: Principles, Algorithms and Applications*. Cambridge: Cambridge University Press; 2009.
2. Korzhik V.I., Nebaeva K.A., Gerling E.Y., Dogil P.S., Fedyanin I.A. *Digital Steganography and Digital Watermarks. Part 1. Digital Steganography*. St. Petersburg: The Bonch-Bruevich Saint-Petersburg State University of Telecommunications Publ.; 2016. 226 p. (in Russ.)
3. Korzhik V.I., Yakovlev V.A. *The Basics of Cryptography*. St. Petersburg: Intermedia Publ.; 2016. 296 p. (in Russ.)
4. Korzhik V., Fedyanin I., Godlewski A., Morales-Luna G. Steganalysis Based on Statistical Properties of the Encrypted Messages. *Proceedings of the 7th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security (MMM-ACNS), 28–30 August 2017, Warsaw, Poland. Lecture Notes in Computer Science.* vol.10446. Cham: Springer; 2017. p.288–298. DOI:10.1007/978-3-319-65127-9_23
5. Korzhik V., Nguyen C., Fedyanin I., Morales-Luna G. Side Attacks on Stegosystems Executing Message Encryption Previous to Embedding. *Preprints*. 2018. DOI:10.20944/preprints201802.0143.v1
6. Bassham III L.E., Rukhin A.L, Soto J., Nechvatal J.R., Smid M., Barker E., et al. NIST Special Publication 800–22 Revision 1a. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. Technical report, Gaithersburg; 2010.
7. Korzhik V., Nguyen D.C., Morales-Luna G. Cipher Modification Against Steganalysis Based on NIST Tests. *Proceedings of the 24th Conference of Open Innovations Association (FRUCT), 8–12 April 2019, Moscow, Russia*. IEEE; 2019. p.179–186. DOI:10.23919/FRUCT.2019.8711958

Сведения об авторах:

АХРАМЕЕВА Ксения Андреевна — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, cbor.mail@gmail.com
https://orcid.org/0000-0002-9165-0265

КОРЖИК Валерий Иванович — доктор технических наук, профессор, почетный профессор Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, val-korzhik@yandex.ru
https://orcid.org/0000-0002-8347-6527

НГУЕН Зуи Кыонг — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, Cuong0111@gmail.com
https://orcid.org/0000-0002-0272-3443