Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

Предложенный алгоритм шифрования изображений позволяет повысить степень защиты информации, стойкость к различным атакам и может быть интегрирован в аппаратуру. Преимуществами данного алгоритма является его гибкость, а также возможность обеспечения шифрования с необходимым уровнем безопасности.

ОЦЕНКА УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ ФИЗИЧЕСКОГО ДАТЧИКА СЛУЧАЙНЫХ ЧИСЕЛ

А. И. ТРУБЕЙ, И.К. ПИРШТУК, В.Ю. ПАЛУХА, М.В. МАЛЬЦЕВ

НИИ прикладных проблем математики и информатики БГУ

Функционирование физического датчика случайных чисел (ФДСЧ) основано на преобразовании случайного физического процесса в случайную последовательность с равномерным распределением на интервале [0, 1]. Основным недостатком данного метода является возможная нестабильность вероятностных характеристик случайной величины используемого процесса. Поэтому необходимо оценить стабильность функционирования параметров ФДСЧ, то есть рассмотреть гипотезу о том, что распределение вероятностей случайной величины физического процесса зависит от времени, и определить статистическую значимость отклонений данных параметров. Для подтверждения стабильности эмпирического закона распределения необходимо осуществлять проверку устойчивости работы ФДСЧ в течение определенного времени.

1. Формулировка гипотезы об однородности выборок

Предположим, что имеем комплект, состоящий из $M \geq 2$ двоичных последовательностей, выработанных датчиком в промежутки времени $t_1,...,t_M$. Из комплекта сформируем M независимых выборок, полученных в результате статистического анализа последовательностей. Каждая из выборок есть реализация полиномиальной схемы с N исходами. Объемы выборок равны $n_1,...,n_M$. Обозначим $n = \sum_{k=1}^{M} n_k$, $n_0 = min\{n_1,...,n_M\}$, $\nu_{k,i}$ – частота символа i. В качестве выборок можно рассматривать, например, частоты встречаемости пересекающихся (непересекающихся) l-грамм, гистограммы частот F_k попадания вероятностей p_{ij} матрицы статистического портрета датчика в каждый из 10 подинтервалов, на которые разбивается интервал [0; 1]. Гипотеза однородности предполагает, что вероятностные свойства наблюдаемой последовательности не изменяются во времени. Это означает, что возможные изменения внешних условий и отклонения параметров физического датчика не являются статистически значимыми.

Полагаем, что выборки статистически однородны и для них выполняется гипотеза H_0, если $p_{1,i} = ... = p_{M,i}$; $i = 1,..., N$. В противном случае будем говорить, что выполняется альтернатива H_1. При альтернативе вероятности исходов могут быть постоянными или изменяться с ростом объемов выборок.

Для проверки однородности используем статистику хи-квадрат:

$$\chi^2 = n\sum_{k=1}^{M}\sum_{k=1}^{N}\frac{1}{n_k m_i}\left(\nu_{k,i} - m_i\frac{n_k}{n}\right)^2, \text{ где } m_i = \sum_{k=1}^{M}\nu_{k,i}.$$

Для подтверждения и уточнения полученных результатов будем применять также следующую модификацию статистики χ^2 [1]:

$$\zeta^2 = \inf_{p_1,\ldots,p_N>0} n\sum_{k=1}^{M}\sum_{i=1}^{N}\frac{1}{n_k m_i}\left(\nu_{k,i} - p_i\right)^2 = \left(\sum_{i=1}^{N}\sqrt{\sum_{k=1}^{M}\frac{\nu_{k,i}^2}{n_k}}\right)^2 .$$

Если и справедлива гипотеза H_0, то при $n_0 \to \infty$ статистики χ^2 и $\zeta^2 - n$ сходятся к распределению хи-квадрат с *(M–1)(N–1)* степенями свободы. При этом для всех ожидаемых частот должно соблюдаться условие: $n_k p_{k,i} \geq 10$.

2. Оценка однородности выборок, состоящих из непересекающихся отрезков

С применением статистик χ^2 и ζ^2 проведена оценка однородности выборок, состоящих из непересекающихся отрезков (длиной 1, 4, 8, 12, 16 бит) последовательностей, выработанных датчиками G_1 и G_2 (входящими в состав СКЗИ) в один день (10.11.2016). Для анализа были взяты по 50 последовательностей объемом по 1 *Mb*, выработанные каждым из датчиков. Результаты приведены в таблице 1.

Таблица 1 – Оценка однородности последовательностей, выработанных датчиками

Длина отрезка/степени свободы	*p*-значения	G_1	G_2
1/49	$p(\chi^2)$	0,9836	0,7237
1/49	$p(\zeta^2 - n)$	0,9836	0,7237
4/735	$p(\chi^2)$	0,1076	0,4816
4/735	$p(\zeta^2 - n)$	0,1077	0,4816
8/12 495	$p(\chi^2)$	0,0101	0,8470
8/12 495	$p(\zeta^2 - n)$	0,0101	0,8471
12/200 655	$p(\chi^2)$	0,2995	0,9214
12/200 655	$p(\zeta^2 - n)$	0,3060	0,9241
16/3 211 215	$p(\chi^2)$	0,4563	0,5922
16/3 211 215	$p(\zeta^2 - n)$	***0,9166***	***0,9571***

В результате анализа данных, приведенных в таблице 1, можно отметить, что все полученные *p*-значения превосходят максимальное значение диапазона уровня значимости α = 0,01, рекомендуемое NIST. Это свидетельствует о справедливости гипотезы H_0 об однородности распределения последовательностей. Следовательно, можно утверждать, что возможные изменения внешних условий и отклонения параметров исследуемых физических датчиков G_1 и G_2 в указанные промежутки времени не являются статистически значимыми.

При этом *p*-значения статистики $\zeta^2 - n$ равны или превышают соответствующие *p*-значения статистики χ^2. Различия между ними постепенно возрастают с увеличение количества степеней свободы. Поэтому при большом количестве исходов (в особенности, в пограничных случаях, когда *p*-значения располагаются в окрестности уровня значимости α) для повышения достоверности принятия нулевой или альтернативной гипотезы следует применять статистику ζ^2.

3. Оценка однородности распределения элементов статистического портрета

Применим другой подход. Для датчика G_1 оценим однородность распределения элементов (столбцов) p_{ij} матрицы статистического портрета датчика, представляющих

собой *p*-значения, полученные в результате тестирования *i*-й последовательности *j*-м тестом. Оценим однородность гистограмм частот p_{ij}-значений, полученных в ходе применения теста многомерной дискретной равномерности по непересекающимся отрезкам (МДРН) к последовательностям, выработанным датчиком G_1 соответственно 26.10.2016 и 10.11.2016. В каждый из дней тестированию подвергались 10 последовательностей объемом 1 *MB*, каждая из которых разбивалась на 104 подпоследовательности объемом 80 *KB*. Вероятностный интервал [0; 1] разбивался на 10 подинтервалов. Результаты представлены в таблице 2.

Таблица 2 – Оценка однородности *p*-значений теста МДРН (отрезки, длиной 9 бит)

Подинтервал	26.10.2016										10.11.2016									
	01	02	03	04	05	06	07	08	09	10	01	02	03	04	05	06	07	08	09	10
0,0; 0,1	16	8	9	13	10	10	11	9	15	10	8	5	13	8	8	12	11	6	11	9
0,1; 0,2	11	11	11	9	13	12	7	9	8	9	11	12	11	12	6	6	7	7	16	9
0,2; 0,3	9	6	10	10	8	14	9	9	7	13	12	12	13	9	13	12	9	11	11	15
0,3; 0,4	9	11	11	14	12	12	15	9	14	16	11	10	13	11	8	14	7	9	6	9
0,4; 0,5	12	16	11	10	13	6	8	13	12	4	12	12	11	13	6	9	8	7	9	11
0,5; 0,6	9	9	9	8	9	11	8	13	10	15	5	6	7	9	17	5	12	10	8	8
0,6; 0,7	13	10	14	11	8	9	10	10	6	7	11	6	10	12	14	8	8	6	10	11
0,7; 0,8	5	7	12	11	7	7	9	6	11	10	11	13	10	8	12	15	17	16	14	11
0,8; 0,9	10	13	15	9	8	12	10	6	7	10	10	12	6	14	11	12	13	9	12	9
0.9; 1.0	10	13	2	9	16	11	17	20	14	10	10	7	11	7	11	7	11	20	14	11
$p(\chi^2) = 0{,}1385$; $p(\zeta^2 - n) = 0{,}1435$ (81 степ. своб.)											$p(\chi^2) = 0{,}6266$; $p(\zeta^2 - n) = 0{,}6353$ (81 степ. своб.)									
$p(\chi^2) = 0{,}6224$; $p(\zeta^2 - n) = 0{,}6296$ (171 степ. свободы)																				

В колонках таблицы 2 приведены частоты F_k попадания значений p_{ij}, полученных в ходе применения теста МДРН, в каждый из 10 подинтервалов для каждой из 10 последовательностей, сгенерированных датчиком G_1 в первый и во второй день. На однородность отдельно проверялись выборки за 26.10.2016, выборки за 10.11.2016, а также суммарные выборки за указанные дни. Оценка однородности проводилась с использованием статистик χ^2 и $\zeta^2 - n$, *p*-значения которых приведены в таблице 2.

Все приведенные значения вероятностей $p(\chi^2)$ и $p(\zeta^2 - n)$ значительно превышают уровень значимости $\alpha = 0{,}05$ что свидетельствует о том, что подтверждается гипотеза H_0 об однородности распределения *p*-значений по соответствующим подинтервалам. Это подтверждает гипотезу об однородности распределения последовательностей, выработанных датчиком G_1 в указанные дни.

4. Оценка отклонения вероятности единицы от теоретического значения

Для наглядной оценки статистической значимости отклонения вероятности единицы от теоретического значения построим график вероятности единицы $p(\xi_t = 1)$ для датчика G_1, входящего в состав СКЗИ. Построим также границы 95-процентного доверительного интервала (уровень значимости $\alpha = 0{,}05$) для вероятности единицы по формуле: $p_{[\min;\max]} = 0{,}5 \mp \dfrac{\Phi^{-1}\left(1 - \alpha/2\right)}{2\sqrt{n}}$, где n – длина последовательности в битах.

Оценка вероятности производилась для 50 последовательностей объемом по 1 *MB*, выработанных датчиком G_1 в течение 10.11.2016. График приведен на рис. 1.

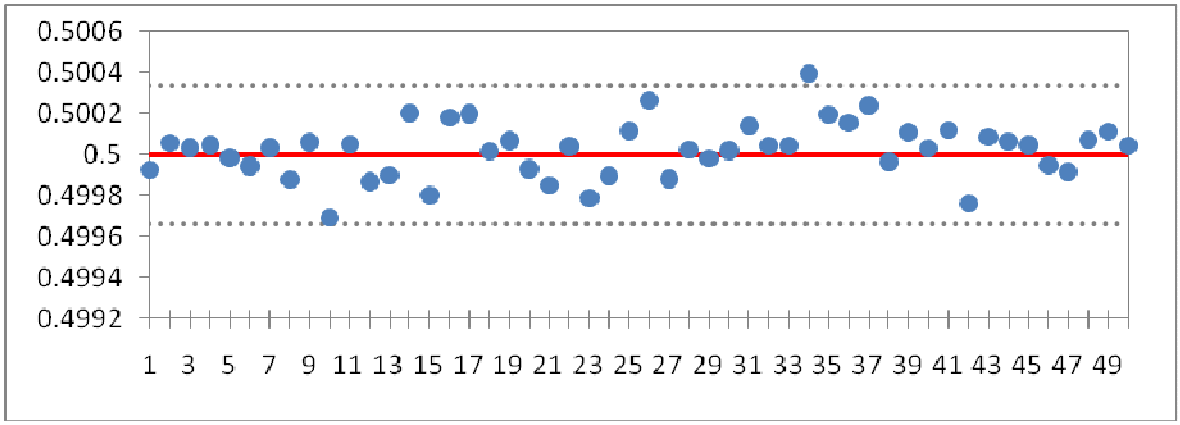

Рис. 1 – График вероятности единицы

Очевидно, что $p(\xi_t = 1)$ практически не выходит за пределы данного интервала. Это означает, что отклонения вероятности, не являются статистически значимыми.

Список литературы

1. *Зубков, А.М.* Об одной статистике для проверки однородности полиномиальных выборок / А.М. Зубков, Б.И. Селиванов // Дискретная математика. – 2014. – т. 26, Вып. 3. – С. 30–44.

ПОВЫШЕНИЕ ВЕРОЯТНОСТИ ОБНАРУЖЕНИЯ РАДИОЭЛЕКТРОННЫХ СРЕДСТВ НА ОСНОВЕ ОЦЕНКИ ПАРАМЕТРОВ ПЕРЕОТРАЖЕННОГО ЗОНДИРУЮЩЕГО СИГНАЛА

В.М. ЧЕРТКОВ, В.К. ЖЕЛЕЗНЯК

Полоцкий государственный университет

Введение. Высокая скрытность и помехоустойчивость радиоэлектронных средств (РЭС) съема информации в различных режимах работы обусловливает необходимость совершенствования методов и алгоритмов их обнаружения, оценки демаскирующих признаков в условиях значительной неопределенности [1].

Цель. Разработка способа обнаружения РЭС с высокой вероятностью на основе оценки параметров принимаемого переотраженного зондирующего сигнала в условиях неопределённости.

Основная часть. На основе анализа математической интерпретации процесса переизлучения гармонического и составного зондирующего сигналов разработана математическая модель формирования и преобразования зондирующего сигнала элементам с нелинейной вольтамперной характеристикой (ВАХ) [2]. Структура модели включает структурные блоки: формирование зондирующего сигнала; трансформация спек-