УДК 519.688, 004.932

ФОРМИРОВАНИЕ ПСЕВДОСЛУЧАЙНОГО МАССИВА С ЗАДАННЫМ ЗАКОНОМ РАСПРЕДЕЛЕНИЯ НА ОСНОВЕ ОПЕРАЦИИ ЭКВАЛИЗАЦИИ

студент гр. 914302 Медведская Ю. И.
Научный руководитель - канд. техн. наук Ролич О. Ч.
Белорусский государственный университет информатики и радиоэлектроники
Минск, Беларусь

В прикладной криптографии и стеганографии, моделировании сигналов, технических систем и их статистических испытаниях актуальна задача быстрого генерирования псевдослучайных стационарных последовательностей с заданным законом распределения [1, 2]. Данную задачу удобно решать на базе операции эквализации входных сигналов датчиков, в особенности, их шума.

В качестве входного сигнала как источника шума выбирается поток данных от MEMS-акселерометра. Это обусловлено конструктивными особенностями современных MEMS-акселерометров и, как следствие, их высокой чувствительностью к постоянной окружающей вибрации за счёт процессов различного рода жизнедеятельности, погодных изменений и гравитации [3].

Алгоритм формирования псевдослучайной последовательности путём выравнивания закона распределения сигнала от датчика рассматривается на примере равномерной эквализации [4].

На рисунке 1 изображены входной сигнал $s(t)$ некоторого процесса от датчика-акселерометра LIS3DSH с соответствующими гистограммами вероятности. Так как в математической модели эквализации фигурирует функция $F(s)$ вероятности, то в решении поставленной задачи логично оперировать именно гистограммами вероятности. Одномерная и двухмерная гистограммы вероятности для последовательности $s(t)$ представлены на рисунках 1, (*б*) и 1, (*в*). Для удобства чтения двухмерной гистограммы вероятности к рисунку 1, (*в*) прилагается цветовая палитра с вариацией цветов от фиолетового, означающего минимальное (в данном случае нулевое) значение, до розовато-белого, означающего максимальное (единичное) значение.

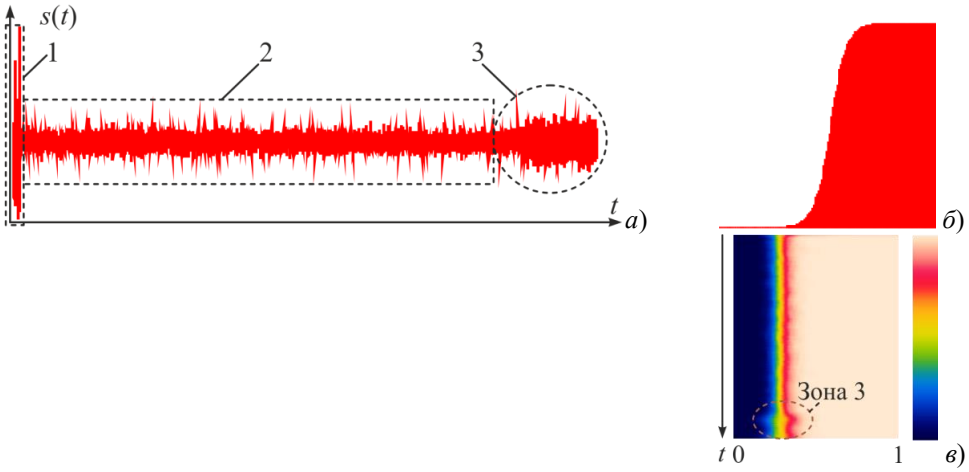

Рис 1. Входной сигнал (*а*) и его одномерная (*б*) и двухмерная (*в*) гистограммы вероятности.

В рисунках 1, (*а*) и 1, (*в*) отчётливо выделяются три зоны: зона 2 стационарного процесса и зоны 1 и 3 переходных процессов, причём зона 3 явно шире зоны 1. На рисунке 1, (*в*) начало зоны 3 обозначено выраженным всплеском.

Согласно характеристике передачи уровней для равномерной эквализации [4]:

$$g(s) = F(s) \cdot (g_{\max} - g_{\min}) + g_{\min},$$

где g_{min} и g_{max} – соответственно минимальное и максимальное значения в генерируемой псевдослучайной последовательности, исходный (или входной) сигнал $s(t)$ преобразуется в эквализованный сигнал $g(t)$, изображённый на рисунке 2, (*а*).

Гистограмма вероятности эквализованного сигнала $g(t)$ выровнялась и приняла требуемый, соответствующий в данном случае равномерному распределению вид (см. рисунок 2, (*б*)). Стационарность эквализованного процесса не изменилась – он остался нестационарным с заметной, заключённой в штрихпунктирный прямоугольник на рисунке 2, (*а*) зоной 3 рисунка 1, (*а*). Нестационарность эквализованного процесса подтверждается и двухмерной гистограммой вероятности на рисунке 2, (*в*), в котором прослеживается явное непостоянство во времени ширины вероятностных уровней. Наиболее важным результатом операции эквализации является формирование числового набора, удовлетворяющего заданному закону распределения.

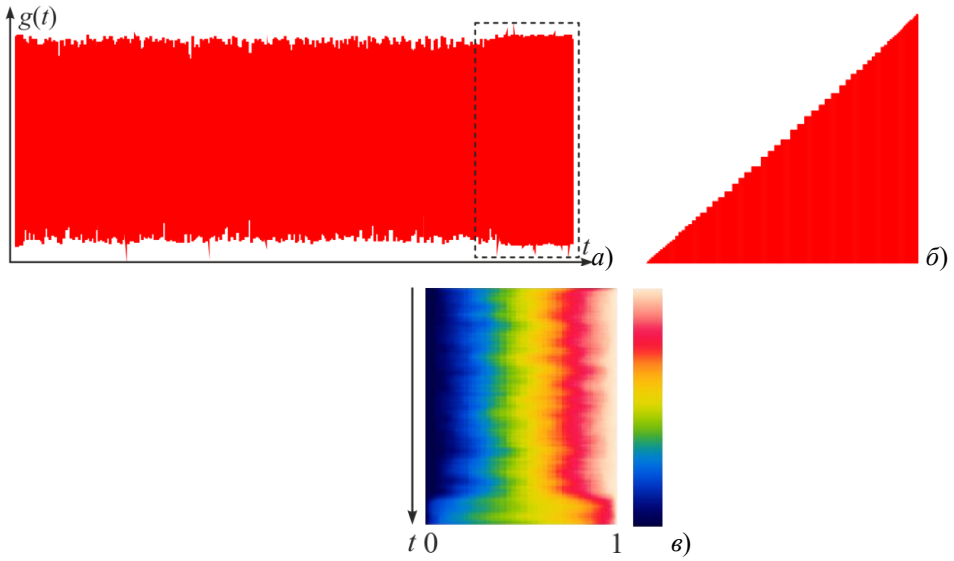

Рис 2. Эквализованный сигнал (*а*) и его одномерная (*б*) и двухмерная (*в*) гистограммы вероятности.

Несмотря на выровненную гистограмму вероятности, что на рисунке 2, (*б*), многие числа в полученной последовательности близки друг к другу, о чём свидетельствует гистограмма распределения плотности на рисунке 3, (*б*).

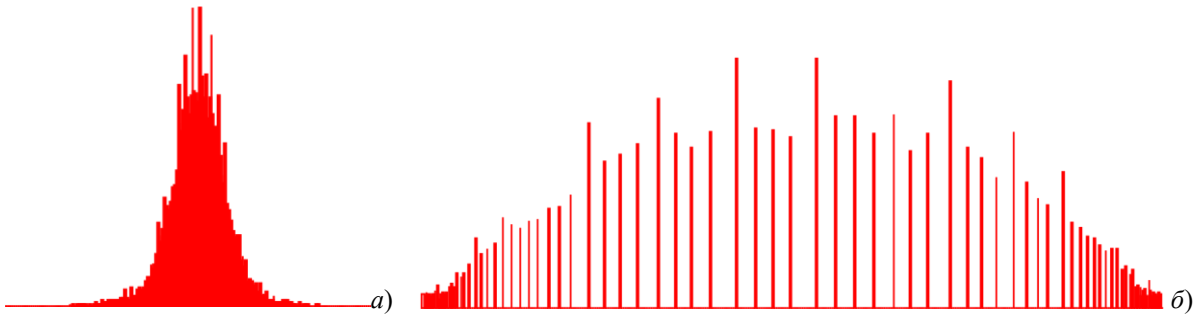

Рис 3. Гистограмма плотности уровней числовой последовательности до эквализации (*а*) и после неё (*б*).

Для дифференциации чисел формируемой последовательности разработан алгоритм дополнительного выравнивания, предназначенный, в первую очередь, для выравнивания гистограммы плотности уровней. Результат предложенного алгоритма дополнительного выравнивания гистограммы плотности представлен на рисунке 4.

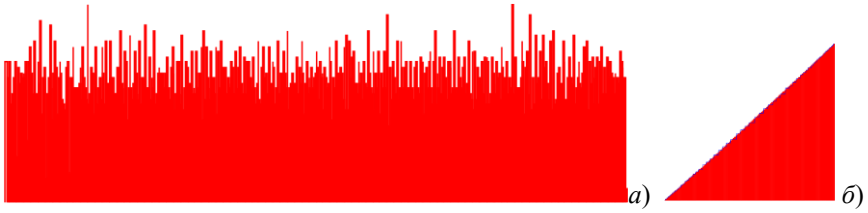

Рис 4. Гистограмма плотности (*а*) и вероятности (*б*) после действия алгоритма дополнительного выравнивания.

По сравнению с гистограммой плотности на рисунке 3, (*б*), гистограмма рисунка 4, (*а*) после действия алгоритма дополнительного выравнивания стала подобной на гистограмму заданного равномерного распределения. При этом выровнялась и гистограмма вероятности, приняв более сглаженный по сравнению с рисунком 2, (*б*) вид.

Однако соответствующая выровненным гистограммам числовая последовательность осталась нестационарной. Для приведения её к стационарному виду проводится двухэтапная перегруппировка, включающая сортировку «выровненной» последовательности и её непосредственную перегруппировку. Результирующая перегруппированная псевдослучайная последовательность и её двухмерная гистограмма вероятности изображены на рисунке 5.

Следует отметить, что вид двухмерной гистограммы вероятности окончательно сформированной псевдослучайной последовательности указывает на её стационарность.

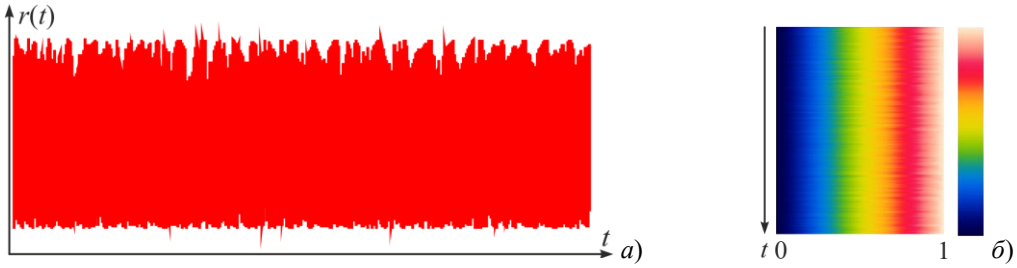

Рис 5. Результирующая псевдослучайная числовая последовательность (*а*) и его двухмерная (*б*) гистограмма вероятности.

Таким образом, предложенный способ формирования псевдослучайного массива с заданным законом распределения на основе операции эквализации позволяет генерировать стационарные псевдослучайные последовательности с выровненными гистограммами вероятности и плотности распределения уровней.

Литература

1. Будько, М. Б. Методы генерации и тестирования случайных последовательностей / М. Б. Будько, М. Ю. Будько, А. В. Гирик, В. А. Грозов. – СПб: Университет ИТМО, 2019. –70 с. – [Электронный ресурс]. – 2020. – Режим доступа: https://books.ifmo.ru/file/pdf/2474.pdf.

2. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации : учеб.-метод. пособие / П. П. Урбанович. – Минск: БГТУ, 2016. – 220 с. – [Электронный ресурс]. – 2020. – Режим доступа: https://elib.belstu.by/bitstream/123456789/23763/3/Urbanovich_zashhita.pdf.

3. Одинец А. И. Датчики МЭМС для управления и диагностирования автомобиля // А. И. Одинец, Л. Д. Фёдорова / Омский научный вестник. – 2015. – № 2 (140). – С. 177 – 179. – [Электронный ресурс]. – 2020. – Режим доступа: https://www.omgtu.ru/general_information/media_omgtu/journal_of_omsk_research_journal/files/arhiv/2015/2(140)/177-184 Технические науки Ч.7.pdf.

4. Калацкая, Л. В. Компьютерный анализ и синтез изображений: курс лекций / Л. В. Калацкая. – Минск: БГУ, 2008. – 101 с.