УДК 004.056, 519.724, 621.391

ПОТОКОВОЕ ВСТРАИВАНИЕ ИНФОРМАЦИИ В СЛУЧАЙНУЮ ПОСЛЕДОВАТЕЛЬНОСТЬ

студент гр. 014301 Шмат И. В.
Научный руководитель - канд. техн. наук Ролич О. Ч.
Белорусский государственный университет
информатики и радиоэлектроники
Минск, Беларусь

Встраивание информационного цифрового сигнала (ИЦС) в случайную последовательность представляется как способ защиты или сокрытия информации при её передаче по каналам связи [1]. Предлагаемое встраивание заключается в модуляции информационным сигналом интегральных параметров распределения генерируемой случайной последовательности: математического ожидания, дисперсии, асимметрии, эксцесса. Для обеспечения должного сокрытия ИЦС модулируемая характеристика случайной последовательности должна иметь достаточно высокий порядок. Поэтому в качестве модулируемого параметра при встраивании ИЦС выбирается коэффициент асимметрии, представляющий интегральную характеристику случайной последовательности третьего порядка.

Одним из распространённых распределений с управляемым коэффициентом асимметрии выступает распределение Вейбулла [2]:

$$W(b,x) = b \cdot x^{b-1} \cdot e^{-x^b} . \qquad (1)$$

Функции его реализации присутствуют в современных программно-математических средах, что упрощает генерирование случайной последовательности и, соответственно, формирование случайного потокового контейнера (СПК) со встроенным ИЦС [3].

Структура СПК со встроенным ИЦС изображена на рисунке 1. Она включает кадры в виде случайных последовательностей длиной L каждый с распределением Вейбулла и параметрами a_i (i = 1, 2, 3, …, m) асимметрии, прямо пропорциональными значениям встраиваемых отсчётов ИЦС.

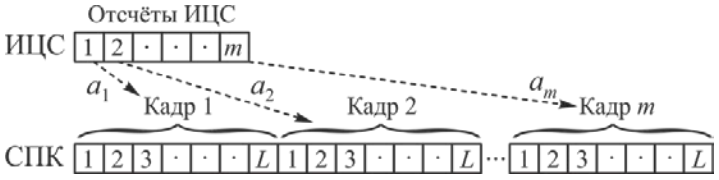


Рис 1. Схема встраивания ИЦС в СПК.

В предлагаемом варианте встраивания ИЦС в СПК встают две задачи:

1. Способ выделения информационного сигнала из СПК.
2. Оценка оптимальной длины L кадра.

Выделение информационного сигнала из СПК на приёмной стороне возможно как посредством вычисления оценки либо коэффициента асимметрии, либо среднеквадратичного отклонения (СКО) в последовательных выборках, перемещающихся вдоль СПК, с дополнительным нелинейным корректирующим преобразованием, так и путём анализа двумерной гистограммы СПК [4, 5].

Оптимальная длина L кадра выбирается исходя из оптимизации уровня шумов в кривой, построенной на множестве оценок коэффициента асимметрии или СКО СПК со встроенным в него ИЦС прямолинейной формы.

Для оценки оптимальной длины L отдельного кадра СПК, в который встраивается отсчёт ИЦС, необходимо определиться с разрядностью и форматом отсчётов ИЦС. Так, в дальнейших рассуждениях применяется 16-разрядный целочисленный беззнаковый тип данных (d = 16) с соответствующим диапазоном значений отсчётов от 0 до $(2^d - 1) = 65535$.

В распределении (1) Вейбулла на асимметрию влияет параметр b, и оно приобретает симметричный вид при $b = b_0 \approx 3.60235$. Как показывают исследования, при встраивании отсчётов ИЦС в случайную последовательность с распределением Вейбулла параметр b целесообразно варьировать вблизи $(b_0/2)$ так, чтобы среднему значению рабочего целочисленного диапазона ИЦС шириной 2^d соответствовало значение $(b_0/2)$, и непосредственный диапазон изменений b являлся симметричным относительно $(b_0/2)$.

В этом случае модуляция $b(f)$ встраиваемого ИЦС $f_j = j$ (j = 0, 1, 2, …, $(2^d - 1)$, d = 16) прямолинейной формы запишется в виде:

$$b\left(f_j\right) = b_{\min} + \frac{b_0 - 2b_{\min}}{2^d} f_j, \qquad (2)$$

где f_j – отсчёт исходного ИЦС, $b_{\min}$ – левая граница отрезка $[b_{\min}, b_0 - b_{\min}]$ изменения параметра b, определяющего асимметрию распределения (1) Вейбулла, d – разрядность представления целочисленных беззнаковых отсчётов ИЦС, d = 16.

Оптимальная длина L кадра встраивания отсчёта ИЦС оценивается способом компьютерных статистических испытаний путём вычисления для каждого кадра оценки коэффициента A асимметрии как центрального момента третьего порядка:

$$A(b)=\frac{1}{L}\sum_{l=0}^{L-1}\left(F_l(b)-\frac{1}{L}\sum_{j=0}^{L-1}F_l(b)\right)^3, \qquad (3)$$

где $F_l(b)$ – отсчёт кадра случайной результирующей последовательности СПК, l – индекс элемента (отсчёта) кадра случайной последовательности СПК, l = 0, 1, 2, …, (L – 1) (на рисунке 1 l = 1, 2, …, L), $\frac{1}{L}\sum_{j=0}^{L-1}F_l(b)$ – оценка математического ожидания кадра, с последующим анализом уровня шумов статистической зависимости $A(b)$. Анализ уровня шумов целесообразно проводить сравнением результата статистической зависимости (3) с явным выражением для асимметрии:

$$\hat{A}(b)=b\int_0^{\infty}\left(x-b\int_0^{\infty}x^b e^{-x^b}dx\right)^3 x^{b-1}e^{-x^b}dx \qquad (4)$$

по формуле суммы квадратов разностей:

$$\sum_b\left(A(b)-\hat{A}(b)\right)^2<\delta, \qquad (5)$$

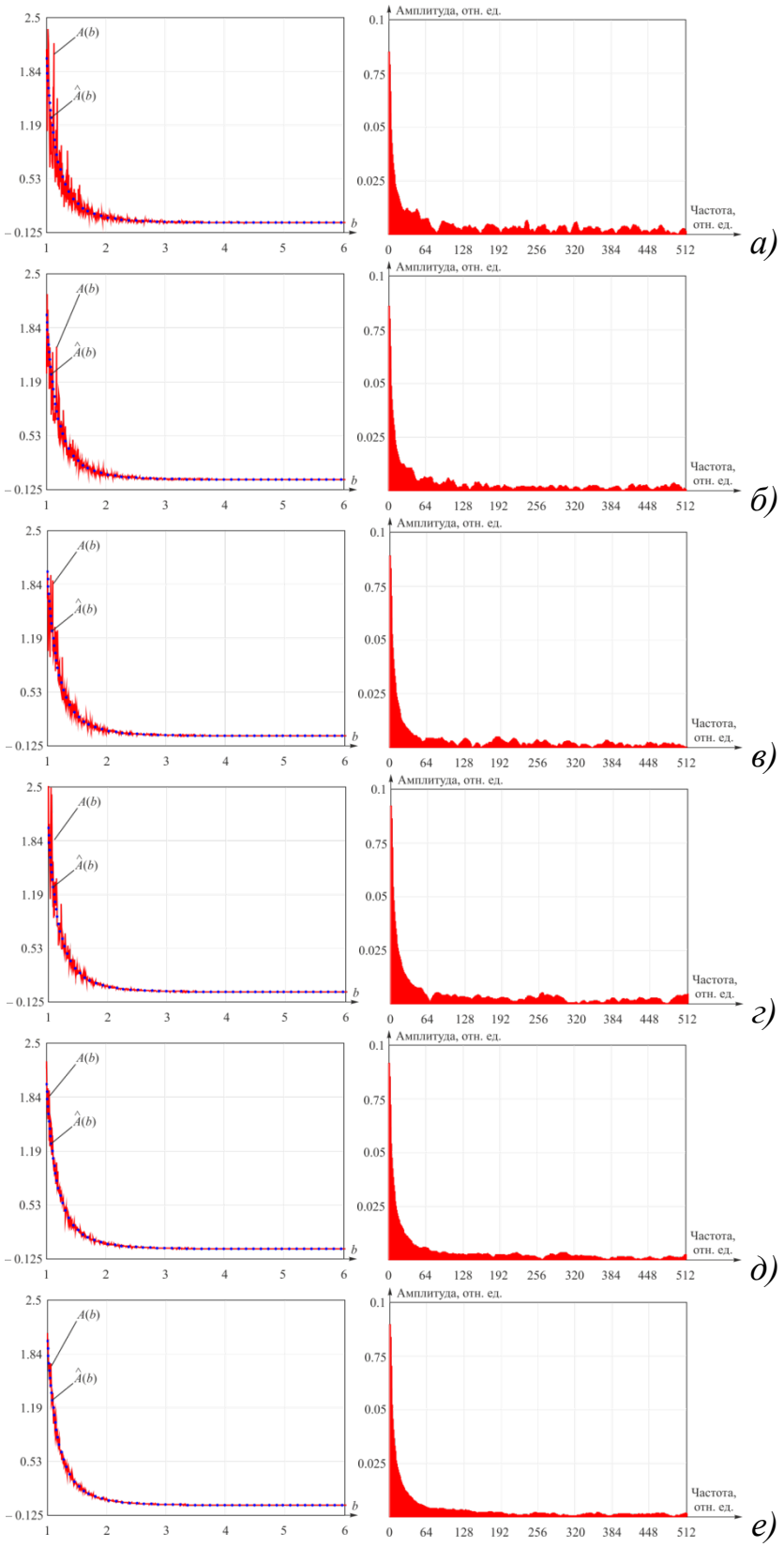
где δ – заданный порог, $\delta > 0$.

Иными словами, оптимальная длина L кадра СПК выбирается таким образом, чтобы для заданного $\delta > 0$ и всех $b \in [b_{\min}, b_0 - b_{\min}]$ выполнялось условие (5).

На рисунке 2 изображена серия статистических кривых $A(b)$, вычисленных по формуле (3), в сравнении с явной кривой $\hat{A}(b)$ выражения (4), а также соответствующие зависимостям $A(b)$ амплитудно-частотные характеристики (АЧХ) для L = 256, 512, 1024, 2048, 4096, 8192 и 16384.

Рисунок 2 подтверждает, что с повышением длины кадра уровень шумов снижается. Так, при длине L = 16384 статистическая кривая $A(b)$ и её АЧХ выглядят значительно более гладкими, чем при L = 512. Шероховатость области высоких частот статистической кривой $A(b)$ с увеличением L также снижается, т.е. и она сглаживается.

Если изменение L с 256 на 512 или на 1024 влечёт очевидные изменения в АЧХ результирующей статистической кривой, то для L = 8192 и 16384 эти изменения малозаметны, и отличия неочевидны. Поэтому, с позиции очевидности изменений АЧХ длину L кадра следует выбирать около 8192, по крайней мере, не менее 4096.


2.5
1.84
1.19
0.53
– 0.125
A(b)
Â(b)
b
1 2 3 4 5 6
Амплитуда, отн. ед.
0.1
0.75
0.05
0.025
Частота, отн. ед.
0 64 128 192 256 320 384 448 512
а)
б)
в)
г)
д)
е)

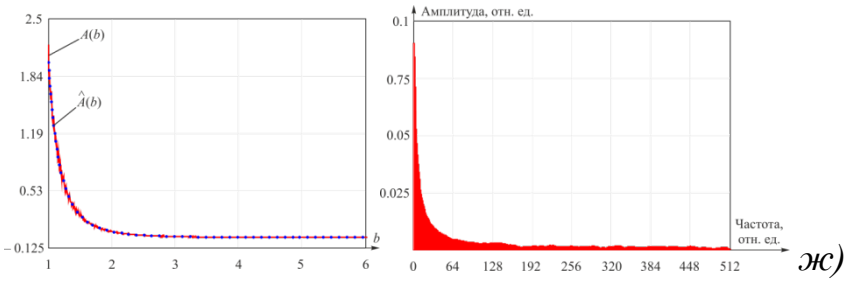


Рис 2. Статистические кривые $A(b)$ и соответствующие им АЧХ для L = 256 (*а*), L = 512 (*б*), L = 1024 (*в*), L = 2048 (*г*), L = 4096 (*д*), L = 8192 (*е*) и L = 16384 (*ж*).

Выводы из рисунка 2 подтверждают и данные таблицы 1, где представлены среднестатистические суммы квадратов разностей для различной длины L кадра.

Таблица 1. Зависимость среднестатистических сумм квадратов разностей от длины L кадра СПК.

L	$\sum_b \left(A(b)-\hat{A}(b)\right)^2$	L	$\sum_b \left(A(b)-\hat{A}(b)\right)^2$	L	$\sum_b \left(A(b)-\hat{A}(b)\right)^2$	L	$\sum_b \left(A(b)-\hat{A}(b)\right)^2$
56	8.67	024	3.52	096	1.10	6384	0.20
12	4.34	048	3.80	192	0.42		

Согласно таблице 1 увеличение L вдвое сначала ведёт к значительному снижению среднестатистической суммы квадратов разностей $A(b)$ и $\hat{A}(b)$ (см. формулу (5)), также примерно в два раза, затем к её заметному снижению (переход от L = 512 к 1024 или от 1024 к 2048) и последующему повторному достаточно резкому росту её уменьшения (переход от L = 2048 к 4096 или от 4096 к 8192, или от 8192 к 16384).

Выбирая порог δ, равным 0.5, рекомендуемая длина L кадра СПК, согласно таблице 1, равна 8192 элемента.

В восстановлении информационного сигнала и его выделении из СПК путём вычисления изменения во времени оценки коэффициента асимметрии применяется зависимость $b(A)$, обратная (4), с последующим вычислением информационных отсчётов по формуле, обратной (2).

Результаты встраивания тестового ИЦС гармонической формы длиной m = 64 16-разрядных беззнаковых отсчётов в СПК на базе распределения Вейбулла и его восстановления отражены на рисунке 3.

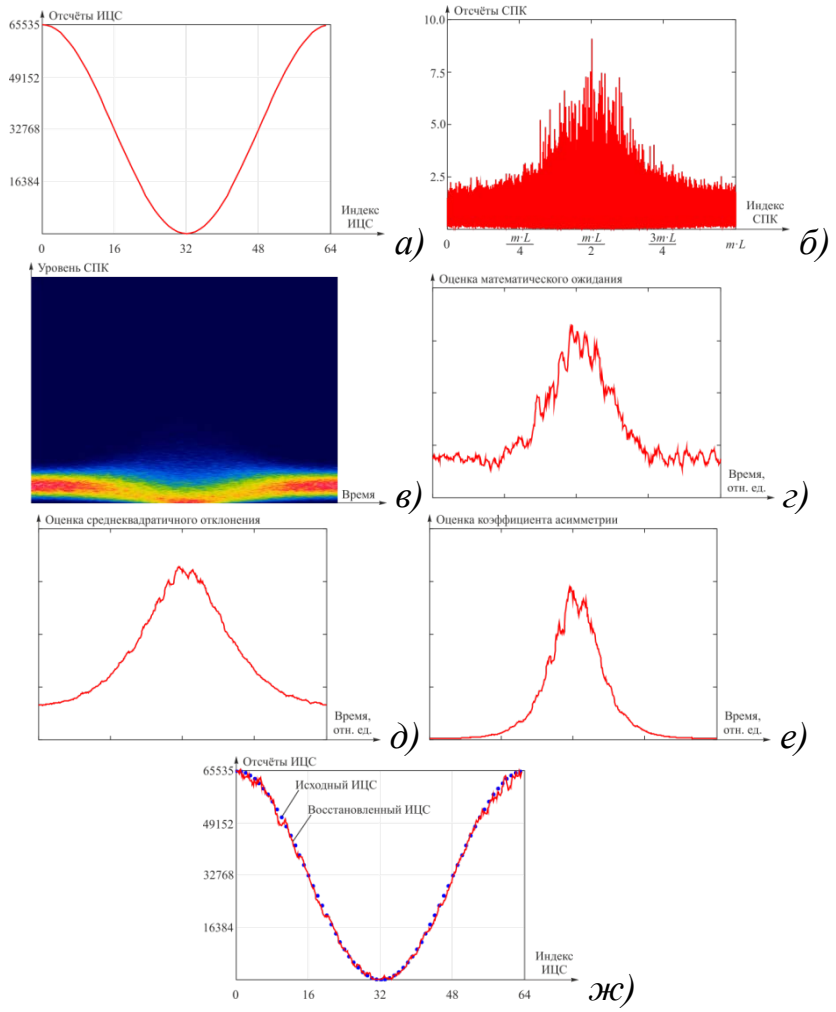


Рис 3. Результаты встраивания и восстановления ИЦС гармонической формы:
а) – исходный ИЦС; *б*) – СПК на базе распределения Вейбулла со встроенным ИЦС; *в*) – двумерная гистограмма СПК с учётом прямоугольного окна;
г) – изменение оценки математического ожидания для СПК со встроенным ИЦС;
д) – изменение оценки СКО для СПК со встроенным ИЦС;
е) – изменение оценки коэффициента асимметрии для СПК со встроенным ИЦС;
ж) – выделенный из СПК информационный сигнал с учётом корректирующей зависимости $b(A)$, обратной (4).

Согласно представленным результатам, форма встроенного ИЦС в СПК на рисунке 3, (*б*) неочевидна. Но эта «неочевидность» проявляется в двумерной гистограмме, изображённой на рисунке 3, (*в*) [4, 5].

По приведённым изменениям оценок математического ожидания, СКО и коэффициента асимметрии наименьшую шероховатость, т.е. наибольшую гладкость имеет зависимость оценки СКО. Поэтому, несмотря на основную идею встраивания ИЦС в моменты относительно высокого

порядка, в частности, в асимметрию, для качественного восстановления информационного сигнала следует использовать изменение оценки СКО.

Восстановленный же из СПК информационный сигнал по изменению оценки коэффициента асимметрии с учётом корректирующей функции $b(A)$, обратной к функции (4), изображён на рисунке 3, (*ж*). Следует отметить, что восстановленный сигнал достаточно точно описывает исходно встраиваемый тестовый ИЦС.

Главным выводом проведённых исследований и представленных результатов является требование к усложнению вида базового распределения. Для повышения сокрытия встраиваемого ИЦС распределение должно характеризоваться полимодальностью с асинхронной и неравномерной динамикой мод в зависимости от модулируемого момента высокого порядка, в частности, коэффициента асимметрии. В противном случае исходный сигнал проявляется на двумерной гистограмме и, очевидно, может быть выделен посредством её пикового анализа.

Автором разработана компьютерная программа автоматизации исследования процесса встраивания определённого пользователем ИЦС в случайную последовательность с заданным законом распределения, а также редактор встраивания аудиосигнала в случайную последовательность с распределением Вейбулла с возможностью его последующего восстановления.

Литература

1. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации / П. П. Урбанович. Минск: БГТУ, 2016. – 220 с.

2. ГОСТ Р 50779.27–2017 «Национальный стандарт Российской Федерации. Статистические методы. Распределение Вейбулла. Анализ данных» [Электронный ресурс]. – 2021. – Режим доступа : https://files.stroyinf.ru/Data/649/64919.pdf.

3. Алефиренко, В. М. Основы защиты информации / В. М. Алефиренко. Минск: БГУИР, 2004. – 44 с.

4. Тарасенко, В. Е. Алгоритмы обработки сигналов в интегрированной системе виброакустической и тепловой диагностики дизельных двигателей / В. Е. Тарасенко, О. Ч. Ролич, Д. А. Михаевич // Агропанорама. – 2020. – № 6 – С. 38 – 41.

5. Пуркова, М. В. Алгоритм статистического анализа данных / М. В. Пуркова, О. Ч. Ролич // Интеллектуальные, сенсорные и мехатронные системы-2021: сборник научных трудов (по материалам студенческих научно-технических конференций). – Минск: БНТУ, 2021. – С. 26 – 28.