Frameworks. - IETF. – April, 1999. ***2.*** *International Telecommunication Union, Rec. M.3010. Principles for a Telecommunications Management Network (TMN). – May,1996.* ***3.*** *Tele-Management Forum, Document GB910, Version 2.1. Telecom Operations Map. – Mart 2000.*

УДК 681.3.067:681.3.016

РАВНОМЕРНОСТЬ РАСПРЕДЕЛЕНИЯ В ШКАЛЕ НАИМЕНОВАНИЙ

Виктор Мясоедов, Виктор Куценко, Тарас Левченко
Научно-технический комплекс «Импульс»

Аннотация: **Проверены статистические свойства псевдослучайных последовательностей, полученных из генератора Фибоначчи. Намечено улучшение схемы порождения таких последовательностей, основанное на результатах численных экспериментов.**

Summary: **There was checked statistical properties of pseudo-random sequences given from Fibonacci generator. There is touched improvement of the creation scheme of such sequences based on results of numerical experiments.**

Ключевые слова: **Равномерность распределения, статистическая проверка, χ^2, численные эксперименты, генератор Фибоначчи.**

I Введение

Применение генераторов псевдослучайных битовых слов в системах телекоммуникации [1] требует статистической проверки свойств последовательностей битовых слов. Такими свойствами, исключающими статистический взлом данных в каналах коммуникации, являются плотность заполнения шкалы наименований битовых слов (используются все слова), нормальность распределения заселённости шкалы гистограммы (отклонения от теоретически ожидаемой заселённости – не более, чем ошибка измерения), и, наконец, соответствие распределения теоретически ожидаемому равномерному распределению (битовые слова появляются в последовательности с одинаковой вероятностью).

Псевдослучайные последовательности битовых слов с необходимостью периодичны. Поэтому перечисленные свойства выходных потоков генераторов должны иметь достаточные теоретические либо экспериментальные основания, т. е. должны проявляться, начиная с некоторой длины последовательности (сплошной выборки) слов. При этом зависимость свойств от начальных значений параметров генераторов должна быть в общем случае слабой.

Целью статьи является феноменологическое описание статистических явлений, наблюдаемых в численных экспериментах с генератором Фибоначчи [2], и уточнение алгоритма генерации.

II Постановка задачи

Совокупность всевозможных двоичных слов имеет свойства шкалы наименований, что сильно ограничивает выбор инструментов статистического изучения их последовательностей.

Фактически имеются стандартные средства частотного анализа: гистограммы, статистические моменты и критерий χ^2. Применимость последних двух ограничена требованием несмещённости оценок [3] свойств гистограммы, что легко обеспечить, увеличивая число наблюдений в численных экспериментах. Аналогично несмещённости достаточное основание для статистической надёжности формализуется в соотношениях параметров, а именно: длина выборки не менее чем в 32 раза превосходит «длину» шкалы слов. С другой стороны, длина выборки N не должна превосходить периода $3 \cdot 2^{L-1}$ генератора, где L – длина операндов генератора Фибоначчи [1], и в применении к качеству битовой последовательности должно быть $N < 2^{L-l}$, где l – длина слов, так что параметры экспериментов связаны неравенствами $2^{l+5} < N < 2^{L-l}$. Требование несмещённости оценок свойств гистограммы удовлетворяется при $l > 5$. Таким образом, численные эксперименты определены параметрами l, N, L. Зависимость поведения стандартных статистических моментов и критерия χ^2 от начальных значений генератора подвергается простой проверке.

Требуется выяснить, обладают ли генерируемые последовательности свойствами, перечисленными во введении. Наблюдение свойств выполняется для конкретной схемы генерации псевдослучайных последовательностей, а результаты представляются графически как зависимость статистических характеристик от параметров l, N, L.

III Основная часть

В схеме генерации с одной парой независимых начальных значений $\{v_1,v_2\}$, поставляемой на основе начальных десятичных цифр математических констант ***e*** и π внутренним генератором обобщённой последовательности Фибоначчи с периодом $60 \cdot 10^{3999}$, $u_0 = v_1$, $u_1 = v_2$; $u_{i+2} = u_i + u_{i+1}$, *i = 0, 1, ..., N*, слова *s* определены соотношением

$$s_i = \frac{u_i - \mathrm{mod}(u_i, 2^{L-l})}{2^{L-l}}.$$

В численных экспериментах статистически выявлена практическая проблема оценки по критерию χ^2 распределения последовательности слов *s* в шкале наименований. Эту проблему можно решить на основе качественного рассмотрения естественного явления «квантования» гистограммы при больших значениях *l*.

Точнее, вычисления статистических характеристик, проведенные с помощью Mathcad 2001i professional, дают зависимости основных моментов и критерия χ^2, показанные на рис. 1 и 2.

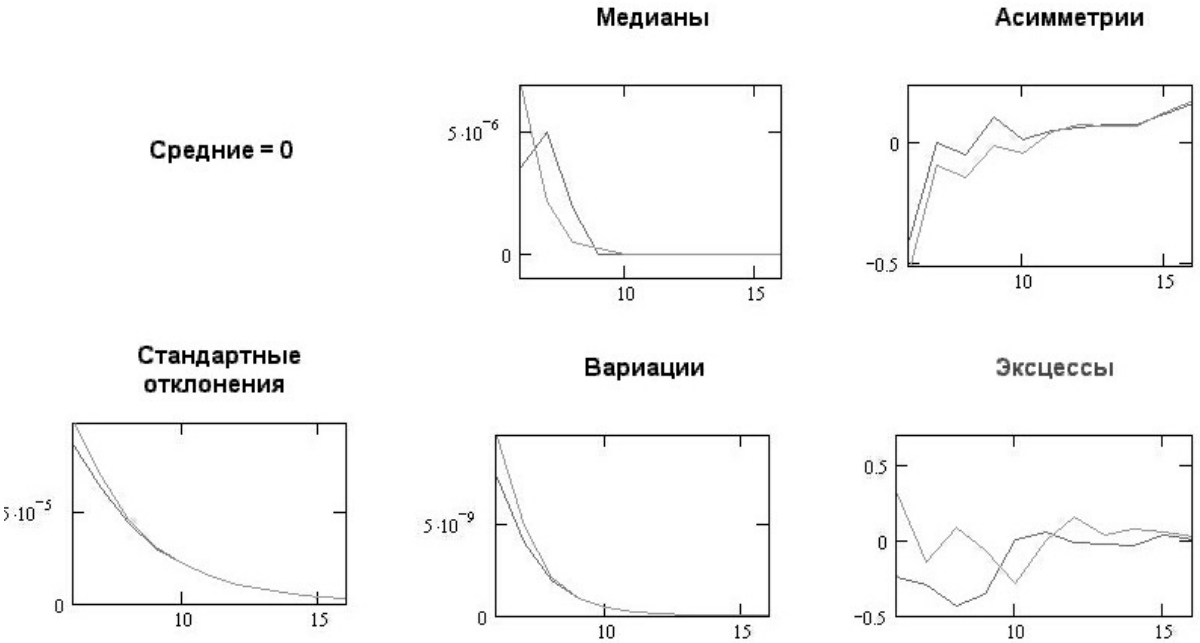

Рисунок 1 – Статистические моменты серии экспериментов с длиной слов от 6 до 16. Длина операндов – 50 бит, размер выборки – 2^{21}

В экспериментах изучены основная и «профильтрованная» по условию внутренней апериодичности [1] последовательности слов *s*. Как видно, статистические свойства последовательностей не имеют качественных отличий. Средние значения гистограммы, центрированной на теоретически ожидаемое равномерное заполнение, не превышают 10^{-19}. Обращают на себя внимание значительные величины асимметрии и эксцесса в области *l = 8*, что побуждает изменить схему генерации. Из рис. 2 видно, что относительная неравномерность распределения слов довольно значительна, но не выказывает особенного поведения. Дополнительный анализ процесса генерации псевдослучайных чисел приводит к последовательности битов переполнения скрытой части операндов. Зависимость суммы битов переполнения от длины скрытой части иллюстрируется рис. 3.

Теоретически доля битов ‘1’ в бесконечной последовательности битов может быть 0, 1/2, 1. Из рис. 3 видно, что последовательность битов переполнения скрытой части операндов близка к случайной последовательности с равновероятным появлением битов ‘0’ и ‘1’.

Несмещённые оценки вероятности появления чисел 0 и 1 в таких последовательностях не известны. Однако вполне возможно поэлементное объединение случайных битов в слова длиной *l* при условии порождения каждой последовательности с помощью независимых начальных значений генератора. Это увеличивает «длину» шкалы слов с 2 до 2^l и позволяет применить критерий χ^2 .Такое изменение схемы генерации, по-видимому, позволит также улучшить статистические характеристики их последовательности, показанные на рис. 1.

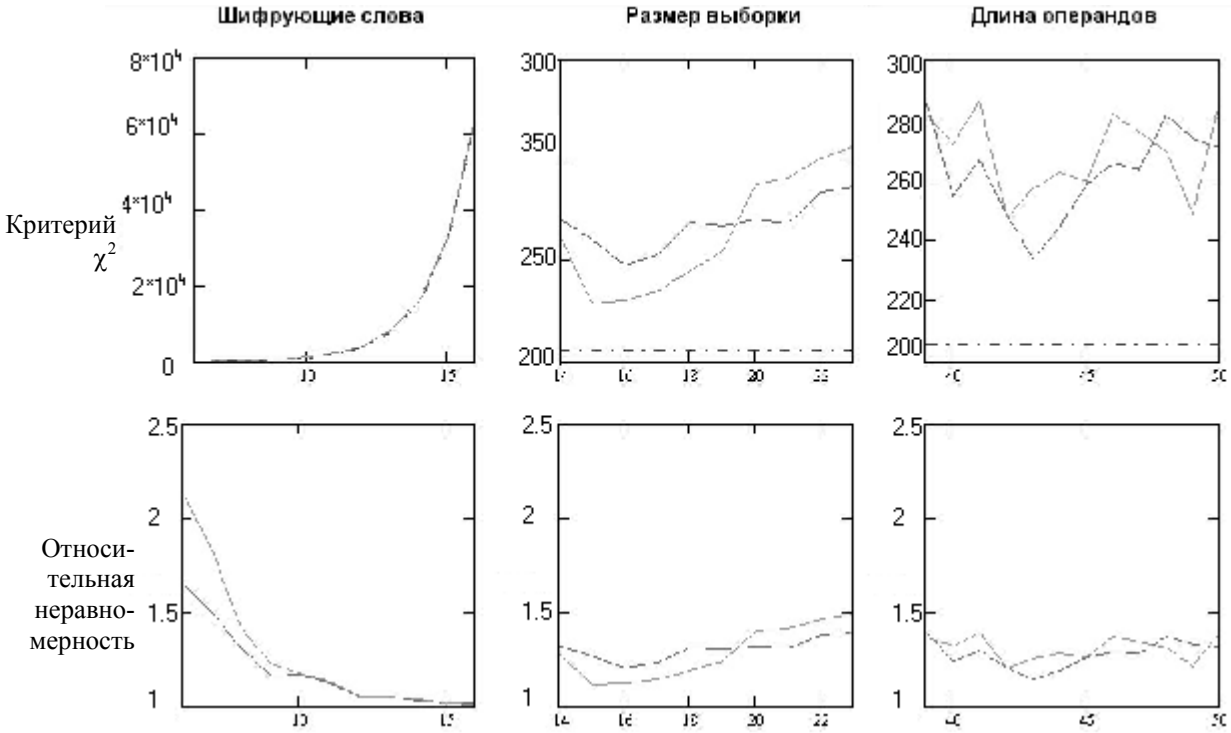

Рисунок 2 – Зависимость критерия χ^2 от параметров эксперимента (шкала размера выборки - $\log_2 N$)

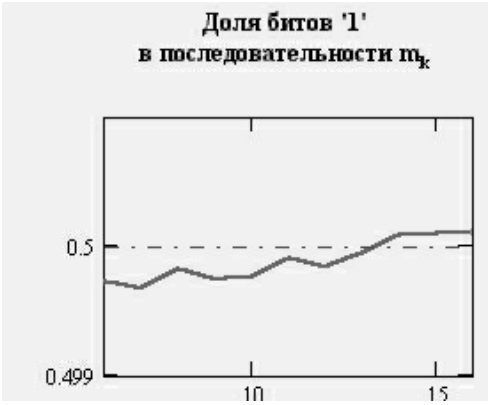

Рисунок 3 – Сумма битов переполнения скрытой части при длине операндов от 39 до 50

На рис. 4 приведен пример гистограммы, иллюстрирующий свойства последовательностей слов. Как видно из рис. 4, при длине выборки $N = 2^{21}$ гистограммы не обращаются в нуль, и, значит, используются все варианты слов. На рис. 5 эта же гистограмма представлена в точечном и несколько увеличенном виде. Справа от гистограммы на рис. 5 показана заселённость шкалы гистограммы (вторичная гистограмма). Очевидно, что на качественном уровне эта гистограмма может быть оценена как нормальная (с точностью до асимметрии и эксцесса), поэтому отклонения от теоретически ожидаемого равномерного заполнения можно трактовать как «ошибки измерения» равномерного распределения. Пример плотности распределения, в котором гистограммы имеют очевидные особенности, приведен на рис. 6.

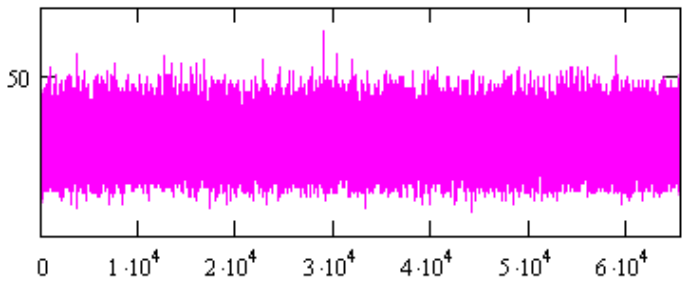

Рисунок 4 – Пример гистограммы $l = 16, N = 2^{21}, L = 50$

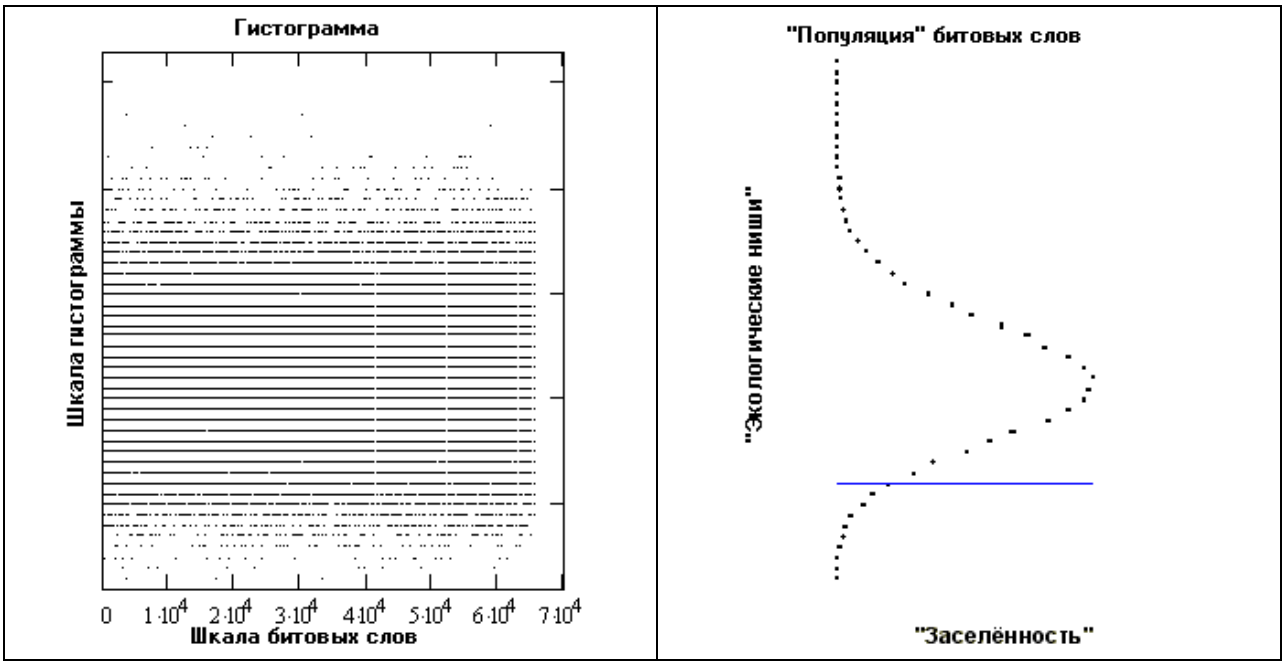

Рисунок 5 – Точечное изображение двух свойств гистограммы $l = 16, N = 2^{21}, L = 50$

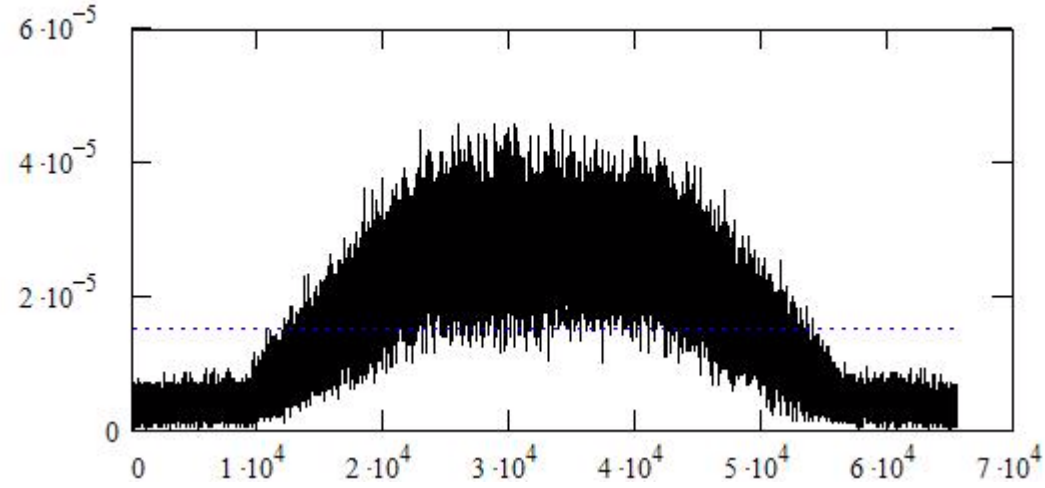

Рисунок 6 – «Усы Фибоначчи»: $u_{i+2} \equiv (-1)^i \cdot u_i + u_{i+1} (\mathrm{mod}\, 2^L), L = 50, l = 16$

Обращает внимание «линейная» организация точек гистограммы, причём расстояния между линиями практически одинаковы. Причина этих явлений заключается в том, что значения гистограммы – целые числа. По сути, гистограмма может рассматриваться как классификация слов. В таком рассмотрении наличие пробелов во вторичной гистограмме подсказывает, что априорный критерий χ^2 может быть сделан более реалистичным, если число степеней свободы определять по шкале гистограммы, а не по шкале слов. В первую очередь это касается апостериорного ограничения числа степеней свободы разностью между максимальным и минимальным значениями гистограммы. Кроме того, число степеней свободы может быть уменьшено исключением «внутренних» неиспользованных уровней заполнения гистограммы.

Разумеется, значения критерия χ^2, показанные на рис. 2, не зависят от таких ограничений. Поэтому для оценки равномерности распределения слов имеет смысл использовать классы значений гистограммы, т. е. включать в вычисление значения критерия χ^2 по одному представителю непустых классов слов. При таком способе оценки выводы о равномерности распределения будут относиться к классам слов без учёта веса класса в выборке. На рис. 7 показаны «реалистичные» (по фактическому числу степеней свободы) варианты критерия и оценка критерия χ^2 для классов значений гистограммы последовательности слов.

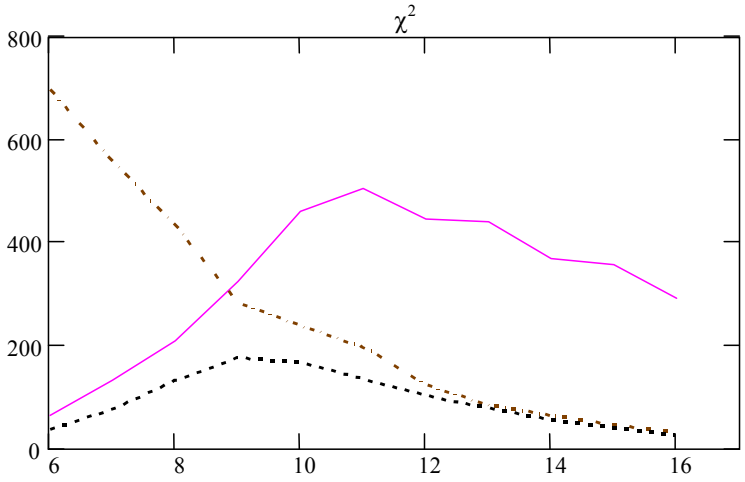

Рисунок 7 – Оценка равномерности распределения по опорным точкам гистограммы

Оценка критерия χ^2 для классов – это сумма квадратов отклонений от теоретически ожидаемой средней плотности заполнения $N/2^L$, делённая на эту плотность заполнения. Сумма вычисляется по произвольно выбранным из шкалы наименований представителям классов значений гистограммы, образующим множество опорных точек гистограммы. Самым простым способом определения опорных точек при просмотре гистограммы является выбор первого слова со значением заполнения, не содержащемся в списке уже встреченных значений. На рис. 8 показаны такие значения, упорядоченные линейным просмотром шкалы наименований.

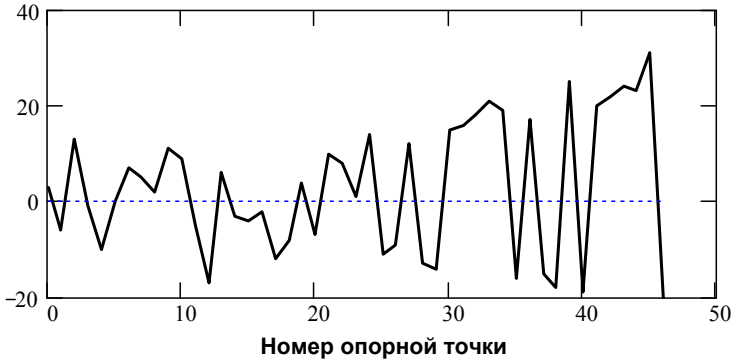

Рисунок 8 – Линейное изображение опорной гистограммы (*l* = 16)

Обращает внимание некая упорядоченность величины отклонения значений гистограммы от номера опорной точки, заметная во всех экспериментах, начиная с $l = 10$. Причины этого явления не ясны, но, по-видимому, оно имеет отношение к выходу оценки критерия χ^2 за пределы равномерности, показанные на рис. 7. Точечное изображение опорной гистограммы из эксперимента с $l = 8$ показано на рис. 9.

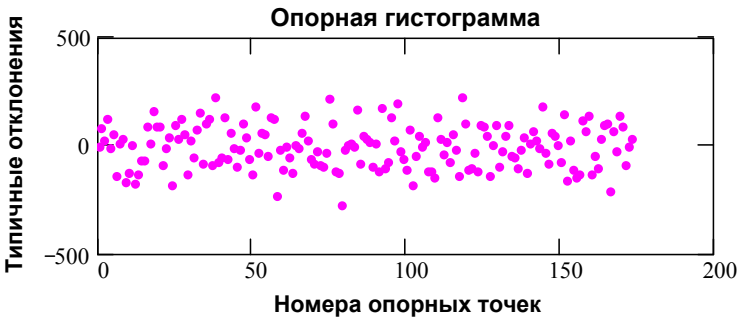

Рисунок 9 – Равномерность распределения в шкале наименований (*l* = 8)

IV Выводы

Экспериментальные данные показывают, что плотность распределения битовых слов в шкале $[0,1,...,2^l-1]$ не имеет особенностей по первым двум свойствам псевдослучайных последовательностей битовых слов. Поэтому использованная схема генерации с достаточным основанием может быть определена как генератор «серого шума». Качество шума может быть грубо оценено по опорной гистограмме. Основанием для этого является массовость данных численных экспериментов, не известная классической статистике.

Имеются достаточные основания для изменения схемы генерации.

*Литература: **1**. В. В. Мясоедов. Золотое сечение в шифровании данных. В сб.: Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - Науково-технічний збірник. - Випуск 4. - К.: НДЦ "Тезіс" НТУУ "КПІ". - 2002. – 214 с. - С. 105. **2**. В. Куценко, Т. Левченко, Н. Миронов, В. Мясоедов. Основная проблема тестирования датчиков случайных чисел. - В сб.: Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.-Науково-технічний збірник. - Випуск 5. - К.: НДЦ "Тезіс" НТУУ "КПІ". - 2002. – 213 с.- С.130-133. **3**. Дж. Бендат, А. Пирсол. Прикладной анализ случайных процессов. – М.: «Мир». - 1989. - 540 с. - С. 86.*

УДК 621.372:621.391

КОДУВАННЯ ЗОБРАЖЕНЬ ПОКОМПОНЕНТНИМ МЕТОДОМ

Володимир Майданюк, Юрій Бондар

Вінницький національний технічний університет

Анотація: **Розглядаються питання ущільнення зображень на основі покомпонентного кодування. Наведені результати досліджень залежності коефіцієнта ущільнення від характеристик фільтрів для формування компонент зображення.**

Summary: **The questions of images compression based on components coding are considered in this work. Results of researches the dependences of compression factor from filters characteristics for formation images components are given.**

Ключові слова: **Адаптивний, декодування, зображення, кодування, стеганографія, ущільнення.**

I Вступ

Одним із способів підвищення ефективності стеганографічних методів приховування інформації є застосування перетворень, характерних для ущільнення зображень. Особливо це відноситься до представлення та форматування цифрових водяних знаків, які знаходять все більш широке застосування при маркуванні мультимедійної інформації [1, 2].

Серед відомих методів ущільнення зображень з просторовою обробкою заслуговує на увагу метод покомпонентного кодування, відомий також як адаптивний до контурів двовимірний аналіз і синтез. Особливістю покомпонентного кодування є формування декількох двовимірних сигналів, які несуть інформацію про деталі зображення різних розмірів [3].

Відомі реалізації алгоритмів кодування на основі даного методу характеризуються малими обчислювальними затратами, оскільки використовують лінійні методи формування просторових компонент зображення при їх аналізі апертурами з розмірами 2x2, 4x4, 8x8 [4, 5]. Передаточні функції фільтрів для формування низькочастотних просторових компонент зображення в цьому випадку такі:

$$H_1(Z_1,Z_2)=\frac{1}{4}\sum_{k_1=0}^{1}\sum_{k_2=0}^{1}Z_1^{-k_1}Z_2^{-k_2} \tag{1}$$

$$H_2(Z_1,Z_2)=\frac{1}{16}\sum_{k_1=0}^{3}\sum_{k_2=0}^{3}Z_1^{-k_1}Z_2^{-k_2} \tag{2}$$

$$H_3(Z_1,Z_2)=\frac{1}{64}\sum_{k_1=0}^{7}\sum_{k_2=0}^{7}Z_1^{-k_1}Z_2^{-k_2} \tag{3}$$

де Z_1^{-1} , Z_2^{-1} – трансформоване представлення затримки на рядок зображення та такт дискретизації