Вестник Физико-технического института
Крымского федерального университета имени В. И. Вернадского
Том 2 (70). № 1. 2018. С. 81–85
Journal of Physics and Technology Institute of V. I. Vernadsky Crimean Federal University
Volume 2 (70). No. 1. 2018. P. 81–85

УДК 004.421.5

ГЕНЕРАТОР СЛУЧАЙНЫХ ЧИСЕЛ С НЕРАВНОМЕРНЫМ РАСПРЕДЕЛЕНИЕМ

Михерский Р. М.*, Исаев М. В., Полянчук Д. М.

Физико-технический институт, Крымский федеральный университет имени В. И. Вернадского, Симферополь 295007, Россия
****E-mail: mrm03@mail.ru***

Описан метод генерации случайных чисел с неравномерным распределением с помощью веб-камеры компьютера. На основе этого метода разработан и программно реализован генератор случайных чисел с неравномерным распределением. Проведено экспериментальное исследование скорости генерации случайных чисел. Показано, что данный генератор случайных чисел может быть с успехом использован в современных системах защиты информации.
***Ключевые слова*:** генератор случайных чисел, неравномерное распределение, системы шифрования.

PACS: 05.40.-a

ВВЕДЕНИЕ

В настоящее время насущно стоит проблема генерации случайных чисел с целью применения их в системах защиты информации.

Для генерации этих чисел используется два подхода. Первый из них связан с созданием и применением специальных устройств, использующих какие-либо физические источники шума. Однако часто стоит задача получения случайных величин на обычном персональном компьютере без применения дополнительного оборудования. Учитывая это, зачастую более актуальным является второй подход, связанный с использованием событий от стандартных устройств компьютера. Наиболее распространенным методом генерации случайных чисел, использующим этот подход, является генерация случайных чисел с использованием счетчика тактов процессора. К его недостаткам можно отнести чувствительность фазового шума генераторов частоты к внешним помехам, а значит, возможность влиять на генератор случайных чисел извне [1]. Счетчики тактов процессора позволяют получать равномерно распределенные случайные числа. Для большинства современных систем шифрования это является преимуществом, так как именно с такими числами эти системы и работают. Однако, в работе [2] был предложен метод шифрования данных, использующий неравномерно распределенные случайные числа, в котором непосредственное применение генератора случайных чисел на основе счетчика тактов процессора представляется затруднительным. В работе [3] предложен способ генерации с помощью оптического манипулятора «мышь», позволяющий получать неравномерно распределенные случайные числа. Недостатком данного метода является то, что скорость генерации случайных чисел составляет всего 971 бит/с, что не позволяет создать на его основе высокоскоростную систему шифрования.

Вопрос о возможности генерации случайных чисел с использованием шумов ПЗС матрицы астрономической монохромной камеры ATIK 383L и КМОП матрицы мобильного телефона Nokia N9 обсуждался в работе [4]. Разработанный авторами работы [4], генератор случайных чисел мог генерировать случайные числа со скоростью до 3 Гбит/с, однако, имел существенный недостаток – в его состав входил специальный экстрактор производивший оцифровку сигнала, т.е. получить случайные числа без использования дополнительного оборудования было невозможно.

Целью данной работы является исследование метода генерации случайных чисел с неравномерным распределением, в котором в качестве источника этих чисел выступают шумы ПЗС или КМОП матрицы камеры, подключенной к персональному компьютеру.

Генератор случайных чисел, реализованный в этой работе, разрабатывался как часть криптографической системы защиты информации на основе случайных чисел с неравномерным распределением.

1. АЛГОРИТМ ГЕНЕРАЦИИ СЛУЧАЙНЫХ ЧИСЕЛ С НЕРАВНОМЕРНЫМ РАСПРЕДЕЛЕНИЕМ С ПОМОЩЬЮ ШУМОВ МАТРИЦЫ ВЕБ-КАМЕРЫ

Для генерации случайных чисел с неравномерным распределением необходимо, чтобы веб-камера, подключенная к ноутбуку или компьютеру, находилась в темном помещении или была закрыта. Пример изображения, полученного с помощью веб-камеры, показан на рисунке 1.

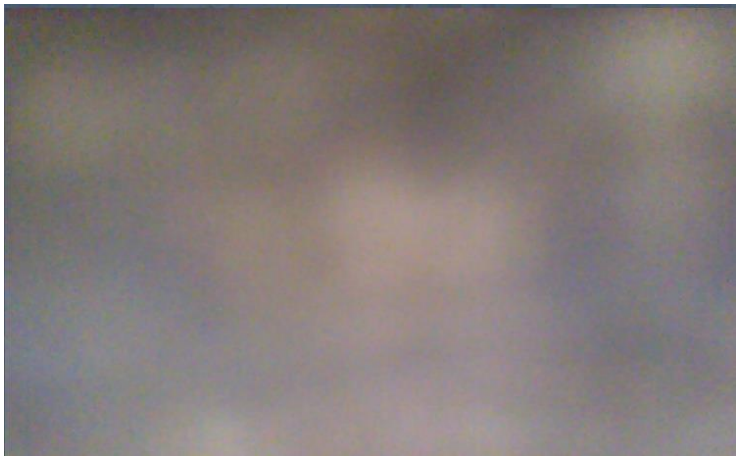

Рис. 1. Изображение, полученное с помощью веб-камеры

Когда камера находится в нужных условиях, делается два снимка. Размер каждого из этих снимков – 640×480 пикселей. Естественно, чем меньше промежуток времени между фотографированием, тем меньше вероятность того, что на них может что-то измениться и тем лучше. Далее из каждой фотографии

необходимо получить так называемый bitmap – матрицу, в которой хранятся значения элементов изображения (пикселей). Для 24-х разрядного изображения каждый пиксель содержит в себе информацию о трех цветах (для цветовой модели RGB) – соответственно красном, зеленом и синем. На каждый цвет отводится 8 бит, то есть максимально возможное значение в десятичном представлении – 255, а минимальное 0. Значению 255 соответствует максимальная интенсивность цвета, а значению 0 – минимальная. На следующем шаге, в общем случае формируется двумерный массив, в который записываются соответствующие значения разностей компонент цвета двух изображений для каждого из пикселей. Полученные разности могут изменяться от – 255 до 255. Эти разности и являются случайными числами. Далее будет показано, как меняются значения разностей в зависимости от условий, в которых находится камера.

2. ПРОГРАММНАЯ РЕАЛИЗАЦИЯ ГЕНЕРАТОРА СЛУЧАЙНЫХ ЧИСЕЛ

На основе приведенного выше алгоритма на языке C# в среде программирования VisualStudio 2015 была реализована компьютерная программа. Исследование проводилось на ноутбуке LenovoG-500 со следующими параметрами : 2-х ядерный процессор IntelCorei3-3110m с технологией HyperThreading; интегрированная видеокарта IntelHD-4000; дискретная видеокарта AMDRadeon 8570M; 8 ГБ ОЗУ; жесткий диск SeaGate, 1TB, 7200 rpm с интерфейсом передачи SATA-3; встроенная веб-камера LenovoEasyCamera с разрешением 1 Мп; операционная система Windows 10.

В результате проведенного исследования получены следующие результаты. Было сгенерировано 10^6 чисел в промежутке от -255 до 255. При этом, время затраченное на эту операцию, составило 0.628 с, а скорость генерации случайных чисел – 12.8 Мбит/с. Гистограмма распределения случайных чисел представлена на рисунке 2.

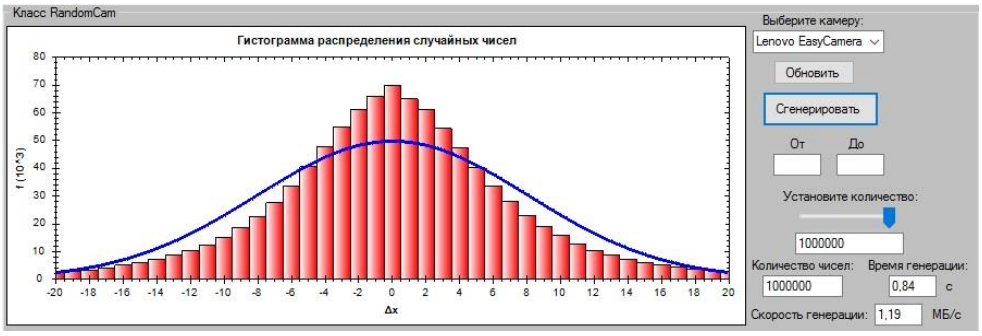

Рис. 2. Гистограмма разностей Δx

Сплошной линией изображен график для нормального распределения со среднеквадратическим отклонением $\sigma = 5.8$. Видно, что полученное распределение близко к нормальному.

При уменьшении количества чисел до 10^4 (в 100 раз меньше, чем в первом случае) время генерации уменьшилось незначительно (до 0.5 с), а скорость составила 0.026 МБ/с. Было проведено еще несколько тестов: для получения даже 10 чисел время составило около 0.5 с. Исходя из этого можно сделать вывод, что время генерации не сильно зависит от количества чисел и колеблется относительно некоторого значения (в данном случае это 0.5 с). Это говорит о том, что на такие операции, как получение bitmap-ов из фотографий, а также на само фотографирование уходит приблизительно 0.5 с. Непосредственно получение чисел занимает незначительное время.

ЗАКЛЮЧЕНИЕ

В заключении следует отметить некоторые вопросы, оставшиеся не до конца исследованные в этой работе.

Как известно, цифровой шум в матрице камеры может возникать по причине: дефектов потенциального барьера вызывающих утечку заряда, сгенерированного за время экспозиции; темнового тока, являющегося вредным следствием термоэлектронной эмиссии и «туннельного» эффекта и возникающего в сенсоре при подаче потенциала на электрод, под которым формируется потенциальная яма; из-за шума, возникающего вследствие стохастической природы взаимодействия фотонов света с атомами материала фотодиодов сенсора и т.д. Каким образом, и в какой пропорции эти причины влияют на суммарный цифровой шум матрицы авторам не известно. Данный вопрос требует дополнительного серьезного исследования.

Другим направлением, которое необходимо изучить в ходе дальнейших исследованиях: является ли генерируемая последовательность символов коррелированной или нет?

Не смотря на то, что в работе остались вопросы, требующие дальнейших исследований, реализованная компьютерная программа позволяет производить высокоскоростную генерацию случайных чисел с неравномерным распределением. Она с успехом может быть применена как составная часть криптографической системы защиты информации на основе случайных чисел с неравномерным распределением [2].

Список литературы

1. Реализация генераторов случайных чисел / А. В. Ковалев // Научная сессия МИФИ. 2007. Том 12. С. 176–177.
2. Шифр на основе случайных чисел с неравномерным распределением / Р. М. Михерский // Проблеми програмування. 2011. № 4. С. 90–95.
3. Generation of Random Numbers by Means of Optical Manipulator / R. M. Mikhersky, O. I. Popov // Journal of Automation and Information Sciences. 2011. Vol. 43(8). P. 76–80.
4. Quantum random number generation on a mobile phone / A. Martin, H. Zbinden, N. Gisin // [электронный ресурс] URI : http://arxiv.org/pdf/1405.0435v1.pdf (дата обращения : 05.12.2017).

GENERATOR OF RANDOM NUMBERS WITH NON-DIMENSIONAL DISTRIBUTION

Mikherskii R. M.**, *Isaev M. V.*, *Polyanchuk D. M.

Physics and Technology Institute, V. I. Vernadsky Crimean Federal University, Simferopol 295007, Russia
****E-mail: mrm03@mail.ru***

A method for generating random numbers with a nonuniform distribution using a computer web-cam is described. Based on this method, a random number generator with a non-uniform distribution is developed and programmed. An experimental study of the rate of generation of random numbers is carried out. It is shown that this random number generator can be successfully used in modern information security systems.
***Keywords*:** random number generator, uneven distribution, encryption.

References

1. A. V. Kovalev, *Scientific session of MEPhI* **12**, 176–177 (2007). [in Russian].
2. R. M. Mikherskii, *Problems of programming*, No. 4, 90–95 (2011).
3. R. M. Mikhersky, O. I. Popov, *Journal of Automation and Information Sciences* **43(8)**, 76–80 (2011).
4. A. Martin, H. Zbinden, N. Gisin, *Quantum random number generation on a mobile phone,* Available : http://arxiv.org/pdf/1405.0435v1.pdf.

Поступила в редакцию 07.04.2018 г. Принята к публикации 22.05.2018 г.
Received April 07, 2018. Accepted for publication May 22, 2018