DOI 10.31891/2307-5732-2024-333-2-18
УДК 004.4

ГАНЖЕЛО ДМИТРО
Чернівецький національний університет ім. Ю. Федьковича
https://orcid.org/0000-0002-0836-4568
e-mail: hanzhelo.dmytro@chnu.edu.ua
ПРОХОРОВ ГЕОРГІЙ
Чернівецький національний університет ім. Ю. Федьковича
https://orcid.org/0000-0001-7810-2785
e-mail: g.prokhorov@chnu.edu.ua

ДОСЛІДЖЕННЯ ЧИСЛОВОЇ ВИПАДКОВОЇ ПОСЛІДОВНОСТІ, ЩО ОДЕРЖАНА З ВЕБ КАМЕРИ

В роботі наведено результати досліджень числової випадкової послідовності, що була одержана за допомогою вебкамери, на відповідність вимогам криптозахисту інформації: рівень хаосу та рівномірність розподілення. В результаті виявлено, що навіть в повній темряві стохастичні теплові процеси зумовлюють високий рівень хаосу у зображенні, достатній для генерації випадкових послідовностей чисел. Лавинний ефект, який супроводжує процес генерації, достатній для вимог криптостійкості. Сам процес вилучення послідовності випадкових чисел з кадру зображення вебкамери істотно спрощується при використанні спеціалізованих бібліотек мови програмування Java.

Ключові слова: програмна інженерія, теорія хаосу, криптостійкісь, генератор послідовності випадкових чисел, лавинний ефект, вебкамера.

HANZHELO DMYTRO, PROKHOROV HEORHII
Chernivtsi National University

INVESTIGATION OF NUMERICAL RANDOM SEQUENCE OBTAINED FROM WEB CAMERA

The investigation object of this paper is a random numbers sequence (RNS) obtained from a single frame of a webcam, which can be practically used as a source of chaos for a hardware RNS generator.

The problem under consideration was to calculate the primary statistical characteristics of the RNS obtained from the webcam frame and compare them with the crypto-resistance requirements.

The obtained statistics confirmed the hypothesis of a high level of chaos using a webcam. In successive frames from image capture (40 milliseconds gap), the photodiode matrix records changes that are not visible to the human eye. Even in absolute darkness , 60% of the changes in the brightness values of the matrix pixels are recorded. Which is 10% higher than the software engineering crypto-resistance requirements for the avalanche effect parameter. This is probably explained by the chaos that accompanies the stochastic interaction of photons of light with the atoms of the material of the sensor. Thus, it is possible to speak about a high level of chaos in the generated RNS.

The peculiarity of the research is that for the purity of the experiment, frame generation was carried out in total darkness (approx. luminosity 10^{-4} lux), and a uniformly illuminated (luminosity 200 lux) white surface. Testing the web camera under extreme conditions gives a complete picture of the unpredictability and chaos of RNS generation. The primary investigation of the statistics of the generated RNS showed a good compliance with some crypto-resistance requirements.

The method built on this property allows designing an affordable hardware RNS generator in laboratory conditions without the involvement of special equipment.

Keywords: software engineering, chaos, crypto-resistant, random number sequence generator, avalanche effect, web camera.

Постановка проблеми

На сучасному етапі розвитку інформаційних технологій питання безпеки життєво важливих інтересів громадян, держави та суспільства, національних інтересів України у кіберпросторі з точки зору кібербезпеки набувають визначального значення [1].

Генератори послідовностей випадкових чисел (ПВЧ) є одними з важливих компонентів криптосистем. Тільки при використанні ключових даних, сформованих із застосуванням ПВЧ, можуть досягатися заявлені рівні стійкості криптографічного захисту інформації (КЗІ). ПВЧ використовуються при встановленні захищених з'єднань у різних мережах, для генерації криптографічних ключів, PIN-кодів, для балансування навантаження, контролю цілісності, і ще для багатьох застосувань [2].

Згенеровані ПВЧ називають псевдовипадковими, оскільки вони не є «істинно» випадковими, а детерміністично згенеровані з ентропії. "Істинні" (апаратні, фізичні) генератори випадкових чисел формують випадкові числа, засновані на справжніх імовірнісних процесах, наприклад, за рахунок використання шумових процесів резисторів та діодів. Для виробництва криптостійких ПВЧ потрібні джерело хаосу, які забезпечують достатню неповторність і непередбачуваність значень навіть у невеликих діапазонах.

ПВЧ формують ключову інформацію, від якості якої залежить стійкість криптографічних перетворень. Тому одним із важливих і необхідних напрямів досліджень та практичних робіт при розробці генераторів ПВЧ є дослідження методів та засобів оцінки статистичних властивостей випадкових послідовностей.

Аналіз останніх джерел

Алгоритм генерації псевдовипадкової послідовності знаходиться у відкритому доступі, наприклад, для мови Java [3,4], що робить теоретично можливим атакувати алгоритм шифрування. У грудні 2022 року з'явилась публікація групи китайських вчених, яка продемонструвала можливість зламу довгих RSA-ключів за допомогою сучасних квантових комп'ютерів. У роботі [5] розказано про перший в історії злом 48-бітного

ключа.

Для генерації ПВЧ використовують два підходи. Перший з них пов'язаний з створенням та застосуванням спеціальних пристроїв, які використовують будь-які фізичні джерела шуму. Так у роботі [5] для генерації випадкових значень використовується лічильник бета-випромінювання, що робить відповідні дослідження залежними від додаткового дорого та екзотичного обладнання.

Однак часто стоїть завдання отримання випадкових величин на звичайному персональному комп'ютері без застосування додаткового обладнання.

Враховуючи це, найчастіше більш актуальним є другий підхід, пов'язаний із використанням подій від стандартних пристроїв комп'ютера. Найбільш поширеним методом генерації випадкових чисел, що використовують цей підхід, є генерація випадкових чисел з використанням лічильника тактів процесора. Проте у роботі [6] інженери FreeBSD висловлюють недовіру цьому методу.

У роботі [7] запропонований спосіб генерації за допомогою оптичного маніпулятора «миша», що дозволяє отримувати нерівномірно розподілені випадкові числа. Недоліком цього методу є те, що швидкість генерації випадкових чисел складає не більше 1 Кбіт/с, що не дозволяє створити на його основі високошвидкісну систему шифрування.

Вище приведені недоліки існуючих рішень приводять до висновку про необхідність проведення дослідження на відповідність ПВЧ, що згенеровані з кадру вебкамери, вимогам КЗІ для подальшої розробки нескладного доступного генератора недетрмінованого хаосу на основі вебкамери.

Метою роботи є дослідження статистичних та криптографічних характеристик випадкових послідовностей, де джерелом чисел, виступають пікселі зображення, сформованого фотоматрицею вебкамери, яка побудована на основі пристрою із зарядовим зв’язком (ПЗЗ) чи КМОН (кремній-метал-окисел-напівпровідник) матриці камери, підключеної до персонального комп'ютера.

Задачі дослідження ПВЧ полягають у наступному:

- дослідити статистично рівень хаосу та випадковості як чутливість до лавинного ефекту;
- перевірити послідовність на рівномірне розподілення по об’єму;

Генератор випадкових чисел, реалізований у цій роботі, розроблявся як частина криптографічної системи захисту інформації на основі числових випадкових послідовностей.

Виклад основного матеріалу

Для чистоти експерименту як крайній випадок було взято зображення білої однорідної стіни при денному рівномірному освітленні (рис. 1). На кадрі можна помітити, що, незважаючи на однорідність образа, знімок на людське око виглядає неоднорідним. По центру більш світлий, ніж на периферії, видно вкраплення інших кольорів, зокрема червоного і сірого. Це дає змогу припустити, що у даному масиві пікселів присутні елементи випадковості. Наскільки ця випадковість задовольняє вимоги криптостійкості, наведених у [8,9], буде вияснено у подальшому.

Рис. 1. Зображення білої стіни, отримане за допомогою вебкамери

Для ще більшої чистоти і граничності експерименту камера була вміщена і загерметизована у темній коробці, щоб уникнути стороннього впливу. Ми спеціально не публікуємо темний знімок, бо на ньому людське око на помітить неоднорідності розподілення точок різної кольорової гами.

Таким чином експеримент проводився при протилежних граничних умовах: повна темрява (освітленість 10^{-4} люкса), та біле рівномірне освітлення у 200 люкс. Температура у приміщенні 20^{o} С.

Апаратно-програмна частина.

Експеримент проводився на апаратній частині із наступними характеристиками: desktop ASUS Z97K; CPU Intel® Core™ i3-4170 CPU @ 3.70GHz × 4; 32 Gb RAM; SDD Kingston 240 Gb; Web Digital Camera FULL HD 1080P, TrueColor.

Програмне забезпечення, що було застосоване у експерименті: ОС Ubuntu 22 LTS, 64 bit; Java Amazon Corretto 17.0.5; IntelliJ IDEA 2023.3.4 (Ultimate Edition); пакет com.github.sarxos.webcam версія 0.3.12 –

захоплення кадру; пакет javax.imageio – обробка відео зображення; пакет org.apache.commons.math3.stat.descriptive.DescriptiveStatistics; – статистичні підрахунки.

Обрана вебкамера підтримує наступні формати роздільної здатності: QQVGA (176 x 144); QVGA (320 x 240); VGA (640 x 480); SVGA (800 x 600). У обраній вебкамері верхня межа роздільної здатності згідно специфікації становить 800 x 600 (VGA), а дефолтним – режим 176 x 144 (QQVGA), the Quarter-QVGA resolution. При бажані цей розмір можна розширити до WebcamResolution.HXGA (4096 x 3072) - все залежить від роздільної здатності обраної камери [10].

Дослідження рівня хаосу у згенерованих числових послідовностях.

Для кожної з 50 пар захоплених послідовних кадрів була згенерована послідовність різниць відповідних значень. Для кожної такої послідовності було вирахувано кількість пікселів, які змінили своє значення за 40 мс.

Оскільки камера знаходилась – в умовах відсутності освітлення, у темній коробці без усякого стороннього впливу, то можна говорити, що внутрішні зміни являються продуктом внутрішнього неконтрольованого хаосу. Процент пікселів, які змінили свою величину упродовж мінімального часу, і буде характеризувати мінімальну міру хаосу та рівень лавинного ефекту.

Для обрахування статистики використовувався об'єкт класу DescriptiveStatistics мови програмування Java, який завантажив усі дані експерименту та згенерував статистику. Результати порівняння були занесені у нижченаведену табл. 1. Величина mean у таблиці означає середнє арифметичне, st dev — середньо квадратичне відхилення (standard deviation), skewness — коефіцієнт асиметрії, kurtosis — ексцес.

Таблиця 1

Залежність статистичних характеристик рівня хаосу від режиму захоплення та робочої температури

Режим температура	**QQGA(176 * 144)**	**QGA(320*240)**	**VGA (640*480)**
t = 20°C	min: 0.55 max: 0.61 **mean: 0.60** std dev: 0.012 median: 0.60 skewness: -2.48 kurtosis: 8.92	min: 0.60 max: 0.63 **mean: 0.62** std dev: 0.014 median: 0.62 skewness: -1.13 kurtosis: 3.18	min: 0.62 max: 0.64 **mean: 0.63** std dev: 0.003 median: 0.63 skewness: 0.74 kurtosis: 2.60
t = 0°C	min: 0.76 max: 0.89 **mean: 0.84** std dev: 0.038 median: 0.83 skewness: 0.005 kurtosis: -0.94	min: 0.84 max: 0.90 **mean: 0.88** std dev: 0.013 median: 0.88 skewness: -0.714 kurtosis: 0.59	min: 0.85 max: 0.91 **mean: 0.89** std dev: 0.011 median: 0.89 skewness: -0.466 kurtosis: -0.005

З даних, наведених у таблиці 1, можна сказати, що рівень хаосу тримається на рівні 60% (у таблиці величина mean = 0.6) і потроху зростає із збільшенням роздільної здатності кадру (режиму захоплення камери). Статистичні характеристики мають чітко виражене Гаусове розподілення, яке ще більше нормалізується (ексцес та кривизна) із збільшенням роздільної здатності кадру. Що свідчить про теплову природу генерації хаосу.

Для більш детального дослідження природи генерації камеру охолодили до 0 °C і повторили експеримент. На рівень хаосу збільшився до 90%, а статистичні характеристики ще більш поточнішали.

Дослідження рівномірності розподілу по об'єму.

Одна з вимог до послідовності випадкових чисел це відсутність скупчень певних чисел у певних місцях, або ж навпаки — відсутність «білих плям» у послідовності. Це і є одна з вимог по розподілу.

Алгоритм полягав у наступному. За одну секунду камера згенерувала 25 послідовностей. Цей ряд був розбитий на 24 пари (1-2, 2-3, 3-4, ... 24-25) У кожній парі відбирались координати, у яких відбулась зміна значень. Така координата записувалась у структуру Set, де можуть знаходитись тільки унікальні значення. Кожна пара записувала у Set свої координати змін.

Таким чином у результаті всіх ітерацій збереглися координати всіх пікселів, які за 1 секунду змінили свої значення хоча би раз. А статистика обробляла зміни для кожної пари (ітерації). Слід зазначити, що експеримент проводився у абсолютній темряві (освітленість складала 10^{-4} люкс). Результати порівняння були занесені у нижченаведеній таблиці 2.

Аналізуючи данні таблиці 2, можна сказати, що від кадру до кадру зміни покривають приблизно 60-64% простору. А от за 24 кадри (1 сек) зміни торкнулись від 69.5% (режим QQVGA) до 94.4% (режим SVGA).

Таблиця 2

Залежність розподілу по локалізації пікселів, що хаотично змінюють значення, від режиму захоплення кадру вебкамерою

Режим характеристика	**QQVGA(176 * 144)**	**QVGA(320*240)**	**VGA (640*480)**
Зміни за 1 ітерацію, статистика,	min: 58.8% max: 62.2% **mean: 61.0%** std dev: 0.8% median: 61.1% skewness: -0.84 kurtosis: 1.11	Min: 59.4% max: 65.1% **mean: 62.1%** std dev: 1.1% median: 62.2% skewness: 0.13 kurtosis: 1.79	Min: 54.85% max: 66.%5 **mean: 64.2%** std dev: 2.1% median: 64.4% skewness: -3.80 kurtosis: 17.34
Зміни за 24 ітерації, %	**69.47**	**87.03**	**94.42**

Обговорення результатів дослідження статистичних характеристик ПВЧ з кадру вебкамери.

Дослідження носять попередній характер, повне статистичне тестування може бути проведене на тестах NIST. Але ці тести вимагають великі ПВЧ — від 100 Мбіт, а згенеровані досліджувані послідовності знаходяться у межах 0.5-12.4 Мбіт. Проте великі послідовності можуть бути згенеровані як конкатенації малих згенерованих ПВЧ. Тому перед NIST тестами великих ПВЧ необхідно провести попереднє дослідження складових.

Особливістю запропонованого методу було рішення ізолювати вебкамеру від зовнішнього впливу, а саме забезпечення повної темряви – освітленості на рівні 10^{-4} люкса. Цю умову було виконати досить просто на відміну, наприклад, від роботи [6], де генератором хаосу було джерело бета-випромінювання.

Опрацювання великих ПВЧ (до 1.5 млн пікселів) було спрощено використанням класу Stream API та DescriptiveStatistics мови Java. Це швидко і точно обчислило статистичні характеристики.

Статистичні обчислення згенерованих числових послідовностей продемонстрували:

- 60-63% рівень хаосу при генерації випадкової послідовності із зображення вебкамери:
- рівень зберігається навіть при повній темряві (освітленість на рівні 10^{-4} люкса), при денному світлі зростає до 89%;
- статистичне розподілення рівня хаосу — нормальне (гаусове), середнє квадратичне відхилення від середнього арифметичного – 0.5-2.0 %;
- високу чутливість до лавинного ефекту, 60 % пікселів змінили свої значення через 40 мілісекунд (повна темрява, освітленість на рівні 10^{-4} люкса), через 1 сек — 94%.
- при зниженні температури рівень хаосу виріс до 90% на кадр;

З приводу дослідження розподілу елементів ПВЧ по об'єму в першу чергу цікавило відсутність скупчень або білих плям однакових елементів в об'ємі. Особливістю запропонованого методу було рішення перевірити локації тих пікселів, що змінюють значення на протязі 24 кадрів в умовах повної ізоляції камери (темрява) . Опрацювання величезних ПВЧ (до 1.5 млн. пікселів) було спрощено використанням класу Stream API мови Java. Це швидко і точно обчислило статистику. Статистичні обчислення продемонстрували:

1. Розподілення значень – рівномірне, локації пікселів, що міняють своє значення з часом (40 мс):
   - для темряви – 60 %;
   - для білої рівномірно освітленої поверхні – 84-89 %.
2. Статистичні характеристики розподілу по об'єму: відхилення від рівномірності – 1.5 - 3.0 %;
3. Чутливість до лавинного ефекту за 1 сек:
   - повна темрява (освітленість 10^{-4} люкс) - 0.6 - 0.9;
   - нормальне освітлення (200 люкс) - 1,0.

Висновки

1. Статистичні характеристики генерації випадкових послідовностей, що одержані шляхом обробки кадрів вебкамери, в основному задовольняють загальноприйнятим вимогам - високий рівень непередбачуваності (хаосу) і чутливості до лавинного ефекту при самих несприятливих умовах 60%, що на 10% перевищує необхідний рівень КЗІ.

2. Статистичні характеристики згенерованих ПВЧ підтверджують рівномірний елементів розподіл по об'єму послідовності у межах 94% для нормального освітлення і мінімальному часі оновлення 40 мілісекунд.

Загальний висновок: послідовності випадкових чисел, що згенеровані за допомогою вебкамери, можуть слугувати основою для розробки доступного апаратного генератора ПВЧ.

Подальші дослідження мають бути сконцентровані на дослідженні кореляції міри хаосу між кадрами, що дозволить визначити період зациклювання при генерації послідовностей великої довжини (100 Мбіт). Це дозволить спрогнозувати значення максимальної теоретичної та робочої швидкодії такого генератора.

Література

1. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №37/2022 "Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року "Про План реалізації Стратегії кібербезпеки України". URL:

https://www.president.gov.ua/documents/372022-41289

2. Asia Othman Aljahdal, "Random Number Generators Survey" International Journal of Computer Science and Information Security (IJCSIS),Vol. 18, No. 10, October 2020 https://zenodo.org/records/4249407

3. Class SecureRandom. Implemented Interfaces. URL: https://docs.oracle.com/javase/8/docs/api/java/ security

4. M. Cornejo, S. Ruhault, "(In)Security of Java SecureRandom Implementations", Journées Codage et Cryptographie, 2014. https://www-fourier.ujf-grenoble.fr/JC2/exposes/ruhault.pdf

5. Bao Yan, Ziqi Tan, Shijie Wei, Haocong Jiang, Weilong Wang, Hong Wang, *et al.* Factoring integers with sublinear resources on a superconducting quantum processor. arXiv:2212.12372v1 [quant-ph] 23 Dec 2022 https://arxiv.org/pdf/2212.12372.pdf

6. Seongmo Park, Byoung Gun Choi, Taewook Kang, Kyunghwan Park, Youngsu Kwon, Jongbum Kim, "Efficient hardware implementation and analysis of true random-number generator based on beta source." ETRI Volume 42, Issue4 ,Special Issue on SoC and AI processors, August 2020, Pages 518-526, https://onlinelibrary.wiley.com/doi/full/10.4218/etrij.2020-0083

7. Ostapov, S., Diakonenko, B., Fylypiuk, M., Hazdiuk, K., Shumyliak, L. and Tarnovetska, O. 2023. Symmetrical Cryptosystems based on Cellular Automata. *International Journal of Computing*. 22, 1 (Mar. 2023), 15-20. https://doi.org/10.47839/ijc.22.1.2874.

8. Randomness test. URL : ttps://en.wikipedia.org/wiki/Randomness_test

9. Lothar Afflerbach. Criteria for the assessment of random number generators, Journal of Computational and Applied Mathematics, Volume 31, Issue 1, 1990, Pages 3-10, ISSN 0377-0427, https://doi.org/10.1016/0377-0427(90)90330-3.

10. Webcam-capture Resolution URL: https://github.com/sarxos/webcam-capture/blob/master/webcam-capture/src/main/java/com/github/sarxos/webcam/WebcamResolution.java

References

1. UKAZ PREZYDENTA UKRAINY №37/2022 "Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 30 hrudnia 2021 roku "Pro Plan realizatsii Stratehii kiberbezpeky Ukrainy".
URL: https://www.president.gov.ua/documents/372022-41289

2. Asia Othman Aljahdal, "Random Number Generators Survey" International Journal of Computer Science and Information Security (IJCSIS),Vol. 18, No. 10, October 2020 https://zenodo.org/records/4249407

3. Class SecureRandom. Implemented Interfaces. URL: https://docs.oracle.com/javase/8/docs/api/java/ security

4. M. Cornejo, S. Ruhault, "(In)Security of Java SecureRandom Implementations", Journées Codage et Cryptographie, 2014. https://www-fourier.ujf-grenoble.fr/JC2/exposes/ruhault.pdf

5. Bao Yan, Ziqi Tan, Shijie Wei, Haocong Jiang, Weilong Wang, Hong Wang, *et al.* Factoring integers with sublinear resources on a superconducting quantum processor. arXiv:2212.12372v1 [quant-ph] 23 Dec 2022 https://arxiv.org/pdf/2212.12372.pdf

6. Seongmo Park, Byoung Gun Choi, Taewook Kang, Kyunghwan Park, Youngsu Kwon, Jongbum Kim, "Efficient hardware implementation and analysis of true random-number generator based on beta source." ETRI Volume 42, Issue4 ,Special Issue on SoC and AI processors, August 2020, Pages 518-526, https://onlinelibrary.wiley.com/doi/full/10.4218/etrij.2020-0083

7. Ostapov, S., Diakonenko, B., Fylypiuk, M., Hazdiuk, K., Shumyliak, L. and Tarnovetska, O. 2023. Symmetrical Cryptosystems based on Cellular Automata. *International Journal of Computing*. 22, 1 (Mar. 2023), 15-20. https://doi.org/10.47839/ijc.22.1.2874.

8. Randomness test. URL : ttps://en.wikipedia.org/wiki/Randomness_test

9. Lothar Afflerbach. Criteria for the assessment of random number generators, Journal of Computational and Applied Mathematics, Volume 31, Issue 1, 1990, Pages 3-10, ISSN 0377-0427, https://doi.org/10.1016/0377-0427(90)90330-3.

10. Webcam-capture Resolution URL: https://github.com/sarxos/webcam-capture/blob/master/webcam-capture/src/main/java/com/github/sarxos/webcam/WebcamResolution.java