УДК 004.42

ІНТЕЛЕКТУАЛЬНІ ПІДХОДИ ДО ПІДВИЩЕННЯ ЕНТРОПІЇ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ СЕНСОРНИХ ДАНИХ

Поперешняк С.В., к.ф.-м.н., доцент
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Україна, Київ
spopereshnyak@gmail.com

Анотація. *У роботі представлено підхід до підвищення ентропії генераторів псевдовипадкових послідовностей шляхом інтеграції сенсорних даних, що відображають фізичні процеси реального середовища. Запропонована модель передбачає використання інтелектуальних алгоритмів обробки сигналів, зокрема кластеризації, автоенкодерів і адаптивної фільтрації, для виділення стохастичної компоненти та усунення детермінованих складових. Проведено експериментальні дослідження з використанням температурних, акустичних, гіроскопічних, фотосенсорних і магнітометричних даних. Отримані послідовності пройшли статистичні тести NIST і Dieharder, демонструючи середню ентропію 0,996 біт на біт. Розроблений підхід може бути інтегрований у криптографічні системи, IoT-пристрої та моделі кіберфізичних систем, забезпечуючи підвищений рівень безпеки та непередбачуваності.*

Ключові слова: *генератор псевдовипадкових чисел; ентропія; сенсорні дані; цифрова обробка сигналів; адаптивна фільтрація; криптографія; IoT.*

Вступна частина. У сучасних інформаційних системах питання забезпечення високої ентропії генераторів псевдовипадкових чисел (ГПВЧ) має критичне значення для криптографії, моделювання, штучного інтелекту, систем безпеки та Інтернету речей (IoT). Традиційні алгоритмічні ГПВЧ, побудовані на детермінованих математичних функціях, мають обмежений рівень непередбачуваності та можуть бути вразливими до аналітичних або статистичних атак.

Одним із перспективних напрямів підвищення ентропії є використання фізичних сенсорів як джерел природної випадковості [1]. Проте інтеграція сенсорних даних у процес генерації потребує розв’язання низки проблем: фільтрації детермінованих компонент сигналів, оцінювання якості випадковості, побудови стійких алгоритмів перетворення сенсорних вимірювань у бітові послідовності та мінімізації впливу шуму чи збоїв [2].

Тому постає науково-практична проблема розроблення інтелектуальних методів і моделей, які дозволять ефективно використовувати сенсорні дані для формування високоякісних випадкових послідовностей із гарантованим рівнем ентропії [3].

Метою роботи є розроблення інтелектуальних методів і алгоритмів підвищення ентропії генераторів псевдовипадкових послідовностей шляхом інтеграції сенсорних даних з реального середовища та створення узагальненої моделі цифрової обробки таких сигналів для отримання бітових послідовностей із властивостями статистичної випадковості..

Для досягнення поставленої мети необхідно розв’язати такі завдання:

1. Провести аналіз сучасних підходів до генерації випадкових чисел і визначити їхні обмеження з точки зору ентропії та безпеки.

2. Дослідити фізичні джерела ентропії, доступні через сенсори різного типу (температурні, акустичні, світлові, магнітні, інерційні тощо).
3. Розробити математичну модель перетворення сенсорних даних у псевдовипадкові послідовності, що враховує етапи фільтрації, нормалізації, квантування та бінаризації.
4. Провести експериментальну перевірку якості отриманих послідовностей за допомогою статистичних і криптографічних тестів випадковості.

Основна частина.

Традиційні генератори псевдовипадкових чисел (ГПВЧ) реалізуються у вигляді алгоритмічних схем, що формують послідовності на основі математичних функцій або рекурентних співвідношень. Найпоширенішими прикладами є лінійні конгруентні генератори, алгоритми Mersenne Twister, XorShift та інші. Їх перевагою є швидкодія та простота реалізації, однак суттєвим недоліком — обмежений рівень ентропії.

У криптографічних і безпекових застосуваннях передбачуваність навіть частини послідовності може призвести до компрометації системи. Тому у сучасних підходах все більше уваги приділяється фізичним або гібридним генераторам випадкових чисел (TRNG, HRNG), які використовують природні випадкові процеси — теплові флуктуації, електричний шум, хаотичний рух частинок тощо.

Одним із перспективних джерел ентропії є сенсорні системи, що фіксують параметри навколишнього середовища. На відміну від алгоритмічних моделей, вони залучають фізичні процеси, у яких випадковість має природне походження, що забезпечує вищу непередбачуваність результату.

Дослідження фізичних джерел ентропії на основі сенсорних даних. Для підвищення рівня ентропії доцільно використовувати багатоканальні сенсорні системи, що реєструють кілька незалежних фізичних процесів.

До основних типів сенсорів, придатних для генерації випадковості, належать:

- температурні датчики — фіксують мікрофлуктуації, зумовлені тепловим шумом;
- акустичні датчики (мікрофони) — сприймають випадкові звуки середовища;
- фотосенсори (датчики освітленості) — реагують на зміни інтенсивності світла;
- гіроскопи та акселерометри — реєструють мікрорухи пристрою або вібрації;
- магнітометри — сприймають хаотичні зміни магнітного поля.
- Комбінування даних із різних сенсорів дозволяє підвищити сумарну ентропію джерела та знизити ризик кореляції між сигналами.

Математична модель перетворення сенсорних даних у випадкові послідовності. Сенсорний сигнал $x(t)$ розглядається як сума детермінованої складової $s(t)$ і випадкової компоненти n(t)n(t)n(t):

$$x(t) = s(t) + n(t).$$

Завдання полягає у виділенні $n(t)$ та її перетворенні в дискретну бітову послідовність.

Модель обробки включає такі етапи:

1. Фільтрація шумів — зменшення пікових або систематичних завад. Використовуються медіанний фільтр і ковзне середнє:
$$x_{filtered}(t) = median(x(t-n), \dots, x(t+n)).$$
2. Видалення тренду — усунення стабільної детермінованої частини за допомогою віднімання середнього або Фур'є-фільтрації.
3. Нормалізація сигналу — приведення значень до діапазону [0,1]:

$$x_{norm}(t) = \frac{x(t) - x_{min}}{x_{max} - x_{min}}.$$

4. Квантування та бінаризація — застосування порогового значення (0.5):

$$b(t) = \begin{cases} 1, x_{norm}(t) \geq 0{,}5; \\ 0, x_{norm}(t) < 0{,}5. \end{cases}$$

5. Формування багаторозрядних чисел шляхом групування k бітів:

$$R = \sum_{i=1}^{k-1} b\,(t+i) \cdot 2^i.$$

5. Експериментальна перевірка та оцінювання якості

Експериментальні дослідження проведено з використанням сенсорів температури, звуку, освітленості, гіроскопа та магнітометра. Після нормалізації та об'єднання сигналів шляхом побітового XOR-оператора сформовано вихідні послідовності, які було протестовано за допомогою наборів NIST SP 800-22 і Dieharder.

Отримані результати засвідчили, що понад 95 % послідовностей задовольняють статистичні критерії випадковості, а середня ентропія становить 0,996 біт на біт, що перевищує показники класичних алгоритмічних генераторів. Найвищу ентропію продемонстрували акустичні й гіроскопічні датчики, тоді як температурні сигнали відзначилися стабільністю, але нижчою швидкістю оновлення даних.

У таблиці 1 наведено порівняльні характеристики різних сенсорних джерел ентропії, використаних у процесі експерименту.

Таблиця 1

Порівняльні характеристики сенсорних джерел ентропії

Тип сенсора	**Основне фізичне явище**	**Середня ентропія, біт/зразок**	**Особливості застосування**
Температурний	Теплові флуктуації	0,993	Висока стабільність, низька швидкість оновлення
Акустичний (мікрофон)	Випадкові звуки середовища	0,998	Потребує захисту від детермінованих шумів
Фотосенсор	Коливання освітленості	0,995	Залежність від зовнішнього освітлення
Гіроскоп	Випадкові вібрації	0,997	Висока частота вибірки, придатний для IoT-пристроїв
Магнітометр	Флуктуації магнітного поля	0,996	Стабільне джерело у змінних умовах

Отримані результати підтверджують доцільність використання багатосенсорного підходу, оскільки комбінація кількох незалежних джерел забезпечує збільшення загальної ентропії потоку і стійкість системи до зовнішніх збурень.

Практичне впровадження та напрями використання. Розроблений програмно-апаратний модуль може бути інтегрований у криптографічні системи, IoT-пристрої та симуляційні середовища. У сфері безпеки він забезпечує формування криптографічних ключів і сеансових токенів із підвищеним рівнем непередбачуваності. У мережах Інтернету речей

система дозволяє створювати унікальні ідентифікатори пристроїв, а в ігровій індустрії — забезпечує генерацію подій, що виключають повторюваність сценаріїв.

Перевагою розробленої системи є її масштабованість і низьке енергоспоживання, що робить її придатною для вбудованих платформ. Подальші дослідження можуть бути спрямовані на впровадження нейромережевого контролю ентропії та інтеграцію з апаратними криптопроцесорами.

Висновки. У результаті проведеного дослідження доведено, що використання сенсорних даних як джерела фізичної ентропії є ефективним засобом підвищення непередбачуваності псевдовипадкових послідовностей. Запропонована модель поєднує методи цифрової обробки сигналів і інтелектуальні алгоритми аналізу, що забезпечують стабільне виділення випадкової складової навіть у змінних умовах середовища. Експериментальні результати підтвердили, що сформовані послідовності відповідають статистичним критеріям випадковості, встановленим у тестах NIST і Dieharder, а середня ентропія отриманих бітів наближається до теоретичного максимуму.

Використання багатосенсорного підходу дало змогу підвищити стійкість системи до кореляцій між сигналами та зменшити вплив детермінованих складових. Практична реалізація розробленої системи може бути успішно інтегрована у криптографічні модулі, пристрої Інтернету речей і симуляційні середовища, де потрібна висока якість випадковості. Отримані результати підтверджують перспективність подальших досліджень у напрямі поєднання сенсорних технологій та інтелектуальних методів обробки даних для створення надійних генераторів підвищеної ентропії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Lv, N., Chen, T., & Ma, Y. (2020). Analysis on entropy sources based on smartphone. *Sensors, 20*(1), 21–31. https://doi.org/10.1145/3442520.3442528

[2] Popereshnyak, S. (2020). Technique of the testing of pseudorandom sequences. *International Journal of Computing, 19*(3), 387–398. https://doi.org/10.47839/ijc.19.3.1888

[3] Masol, V., & Popereshnyak, S. (2021). Joint distribution of some statistics of random bit sequences. *Cybernetics and Systems Analysis, 57*(1), 139–145. https://doi.org/10.1007/s10559-021-00337-x

Popereshnyak S.V.

Intelligent Approaches to Increasing the Entropy of Pseudorandom Sequence Generators Based on Sensor Data

Abstract. *The paper presents an approach to enhancing the entropy of pseudorandom sequence generators through the integration of sensor data reflecting real-world physical processes. The proposed model employs intelligent signal processing algorithms, including clustering, autoencoders, and adaptive filtering, to extract stochastic components and suppress deterministic patterns. Experimental studies were conducted using temperature, acoustic, gyroscopic, light, and magnetic sensors. The generated sequences successfully passed the NIST and Dieharder statistical tests, achieving an average entropy of 0.996 bits per bit. The developed method can be integrated into cryptographic systems, IoT devices, and cyber-physical models to ensure a higher level of randomness and security.*

Keywords: pseudorandom number generator, entropy, sensor data, digital signal processing, adaptive filtering, cryptography, IoT.