



І. Г. Цмоць¹, О. Я. Різник¹, Ю. І. Бударецький², Ч. З. Львовський¹, М. В. Цицик²

¹ Національний університет "Львівська політехніка", м. Львів, Україна

² Національна академія сухопутних військ ім. гетьмана Петра Сагайдачного, м. Львів, Україна

УДОСКОНАЛЕННЯ МЕТОДУ СИНТЕЗУ ТА РОЗРОБЛЕННЯ ІМІТАЦІЙНОЇ МОДЕЛІ ЗАВАДОСТІЙКОГО КОДУВАННЯ

Завадостійкість є однією з найважливіших характеристик сучасних систем прийому/передачі даних. Підвищення завадостійкості при фіксованих швидкостях прийому/передачі даних є актуальною проблемою, наприклад, для керування безпілотниками. Досліджені кодові послідовності дають змогу збільшити потужність отриманих послідовностей завдяки використанню дзеркальних завадостійких кодових послідовностей. Підвищення завадостійкості передачі даних досягається за рахунок збільшення довжини та потужності завадостійкої кодової послідовності, яка використовується для передачі одного повідомлення. Переваги цих послідовностей, такі як висока завадостійкість відповідно до вузькосмугових завад великої потужності, можливість поділу абонентів за кодовою ознакою, скритність передачі, висока стійкість до багатопроменевого поширення, висока роздільна здатність при навігаційних вимірах матимуть широке практичне використання у системах зв'язку та геолокації. Вдосконалено метод синтезу завадостійких кодових послідовностей з використанням ідеальних кільцевих в'язанок. Удосконалено метод для швидкого знаходження таких завадостійких кодових послідовностей, які здатні в найбільшому обсязі знаходити і виправляти помилки відповідно до довжини отриманої кодової послідовності. Реалізовано алгоритм для швидкого знаходження таких завадостійких кодових послідовностей, які здатні в найбільшому обсязі знаходити і виправляти помилки відповідно до довжини отриманої кодової послідовності. Розроблено імітаційну модель завадостійкого кодування з використанням ідеальних кільцевих в'язанок. Здійснено програмну реалізацію імітаційної моделі завадостійкого кодування щодо знаходження та виправлення помилок в отриманих завадостійких кодових послідовностях. Запропоновані завадостійкі кодові послідовності мають практичну цінність, оскільки за допомогою отриманої кодової послідовності досить просто та швидко знаходити до 50 % та виправляти до 25 % спотворених символів від довжини завадостійкої кодової послідовності.

Ключові слова: дзеркальна кодова послідовність; ідеальна кільцева в'язанка; нееквідистантна кодова послідовність; нееквідистантна комбінаторна конфігурація.

Вступ

З огляду на безперервне збільшення обсягу інформації, який передається каналами зв'язку, дедалі важливішого значення набувають технології завадостійкого кодування та декодування даних у реальному часі. Аналіз діючих каналів показує, що при передачі даних частота виникнення організованих загроз значно вища, ніж природних. Тому необхідно захищати інформацію як від несанкціонованого доступу, так і від її спотворення.

Одним із методів захисту є кодування інформації за допомогою використання завадостійких кодів. Під завадостійким кодуванням інформації варто розуміти таку форму її трансформації, за допомогою якої знаходиться та виправляється певна кількість помилок. Підвищення завадостійкості передачі даних досягається за рахунок збільшення довжини кодової послідовності, яка використовується для передачі одного повідомлення. Використання завадостійкого кодування при передачі даних

Інформація про авторів:

Цмоць Іван Григорович, д-р техн. наук, професор, кафедра автоматизованих систем управління.

Email: ivan.tsmots@gmail.com; <https://orcid.org/0000-0002-4033-8618>

Різник Олег Яремович, канд. техн. наук, доцент, кафедра інформаційних технологій видавничої справи.

Email: riznykoleg@gmail.com; <https://orcid.org/0000-0002-3815-043X>

Бударецький Юрій Іванович, канд. техн. наук, пров. наук. співробітник, науково-дослідний відділ. Email: yuriybud@ukr.net;

<https://orcid.org/0000-0001-7208-3827>

Львовський Чеслав Збігневич, ст. викладач, кафедра дизайну та основ архітектури. Email: riznyk@meta.ua;

<https://orcid.org/0000-0001-5881-5120>

Цицик Михайло Васильович, наук. співробітник, науково-дослідний відділ. Email: yuriybud@ukr.net;

<https://orcid.org/0000-0003-4766-6363>

Цитування за ДСТУ: Цмоць І. Г., Різник О. Я., Бударецький Ю. І., Львовський Ч. З., Цицик М. В. Удосконалення методу синтезу та розроблення імітаційної моделі завадостійкого кодування. Науковий вісник НЛТУ України. 2020, т. 30, № 4. С. 114–122.

Citation APA: Tsmots, I. G., Riznyk, O. Ya., Budaretskij, Yu. I., Lvovskij, C. Z., & Tsitsyk, M. V. (2020). Improvement of the methods of synthesis and development of a simulation model of anti-jamming coding. *Scientific Bulletin of UNFU*, 30(4), 114–122.

<https://doi.org/10.36930/40300420>

призводить до збільшення часу передачі даних. При цьому збільшують витрати енергії на передачу одного повідомлення. Якщо тривалість передачі даних залишати незмінним, то це розширить спектр сигналу, за рахунок зменшення тривалості одного символу, та призведе до збільшення смуги частот, які відведені одному каналу передачі даних. Системи на базі завадостійкого кодування найбільше використовуються в ретрансляційних пунктах, у яких здійснюється демодуляція модульованого сигналу, а за потреби і декодування. Унаслідок сигнал "очищується" від шумів і завад і кожний ретранслятор передає сигнал без накопичення шумів і завад у лінії передачі. Отже, шуми та завади враховуються тільки між двома сусідніми ретрансляторами, що є основою для передачі даних на великі відстані. Передача модульованого сигналу без використання завадостійкого кодування призводить до нагромадження помилок, спотворень і не забезпечує ідентичності прийнятого сигналу із сигналом передавача.

Актуальність вирішення проблеми полягає у регулярному синтезі завадостійких кодів із заданими характеристиками для систем бездротового зв'язку.

Постановка завдання дослідження – потребі розроблення алгоритму для швидкого знаходження таких завадостійких кодових послідовностей, які здатні в найбільшому обсязі знаходити і виправляти помилки відповідно до довжини отриманої кодової послідовності.

Об'єкт дослідження – завадостійкі кодові послідовності.

Предмет дослідження – метод синтезу завадостійких кодових послідовностей.

Мета роботи – вдосконалити метод синтезу та розробити імітаційну модель завадостійкого кодування.

Для досягнення зазначеної мети потрібно виконати такі *основні завдання дослідження*:

- вдосконалити метод синтезу завадостійких кодових послідовностей з використанням ідеальних кільцевих в'язанок;
- розробити імітаційну модель завадостійкого кодування з використанням ідеальних кільцевих в'язанок;
- здійснити практичну реалізацію алгоритму знаходження та виправлення помилок отриманих завадостійких кодових послідовностей.

Наукова новизна отриманих результатів дослідження полягає в удосконаленні методу синтезу завадостійких кодових послідовностей.

Практична значущість результатів дослідження полягає в тому, що запропоновані завадостійкі кодові послідовності мають практичну цінність, оскільки за допомогою отриманої послідовності знаходяться до 50 % та виправляються до 25 % спотворених символів від довжини завадостійкої кодової послідовності.

Аналіз останніх досліджень та публікацій. У роботах [1, 2, 4] показано, що в основу алгоритмів синтезу завадостійких кодових послідовностей покладено принцип надмірності, який дає змогу знаходити і виправляти помилки завдяки особливостям структур цих послідовностей. Зазвичай, коди, що виправляють помилки, будуються на підставі циклічних кодових послідовностей, усі комбінації яких можна отримати шляхом циклічного зсуву однієї або декількох комбінацій коду.

Ідея побудови таких кодів базується на використанні багаточленів, що не приводяться в полі двійкових чисел та діляться без залишку тільки на себе або на одиницю.

З аналізу робіт [1, 4] видно, що для завадостійкого кодування широко використовуються коди Боуза-Чоудхури-Хоквінгема (БЧХ-коди). Для їх декодування використовується алгоритм Берлекемпа і його основні модифікації, які забезпечують виправлення всіх помилок ваги $W \leq W_o$, де $W_o + 1 = d_o$. Однак складність цього алгоритму складає порядок $n^2 \log_2 n$ операцій і потребує приблизно $(5 \dots 20) n$ біт пам'яті.

У роботах [1, 7] показано, що основним типом блокових кодів для боротьби зі завадами є недвійкові коди Рида-Соломона (РС). Довжина набору визначається вихідним полем 2^l , де l визначає довжину набору. Декодування цих кодів відбувається також на основі алгоритму Берлекемпа [1]. Незважаючи на пошуки багатьох дослідників, складність операцій, що виконуються декодером, залишається дуже великою. Так, у разі реалізації декодера РС для коду (31, 15) потрібне виконання приблизно 17 операцій на кожний біт повідомлення, що декодується, навіть якщо частина операцій проводиться паралельно, а перемноження в недвійкових полях виконується табличними методами.

У роботах [7, 12, 13] розглянуто каскадні коди, які забезпечують високі імовірнісні показники за досить високого рівня завад і помірної складності декодування. У роботі [14] показано, що алгоритм Вітербі широко використовується в техніці передачі даних з використанням згорткових кодів, які мають кращі характеристики порівняно з блоковими. Однак складність реалізації алгоритму Вітербі росте експоненційно з довжиною коду. У роботах [13, 15] розглянуто класи кодів, для яких складність декодування зі зростанням їх довжини зростає не експоненційно, а значно повільніше, наприклад, як квадрат довжини.

У роботах [6, 8, 9, 10, 11] розглянуто питання синтезу завадостійких кодів з використанням ідеальних кільцевих в'язанок. Недоліком методів і алгоритмів синтезу завадостійких кодів з використанням ідеальних кільцевих в'язанок є переборні методики кодування, що уповільнює пошук оптимізованих кодових послідовностей.

Результати дослідження та їх обговорення

1. Удосконалення методу синтезу завадостійких кодових послідовностей з використанням ідеальних кільцевих в'язанок. Найбільший ефект захисту інформації досягається, коли всі використовувані методи та засоби об'єднуються в єдиний цілісний механізм захисту інформації. Тут потрібно зазначити, що захист інформації повинен відбуватись паралельно на трьох рівнях: апаратному (скетч-картки, токени, криптографічні методи, реалізовані на програмному рівні), програмному (антивірусне ПЗ, архівація даних, обов'язкова ідентифікація, шифрування) та організаційному (по суті, контроль дотримання всіх апаратних і програмних способів захисту в повному обсязі).

Проте більшість експертів схиляється до думки про особливе місце завадостійкого кодування (програмно чи апаратно реалізованого) як чи не найнадійнішого методу, адже тут захищається сама інформація, а не доступ до неї. Ефективність такого підходу пояснюють тим, що зловмиснику не достатньо тільки отримати доступ до інформації у вигляді скетч-картки чи паролі, йому потрібно ще знати яким чином потрібна йому інформація закодована.

Завадостійка кодова послідовність складається з набору нулів і одиниць, за допомогою яких перетворюють символи для подальших дій прийому передачі. Основними властивостями цих завадостійких кодових послідовностей є покращені характеристики щодо знаходження і виправлення помилок. Від таких кодових послідовностей залежить завадостійкість системи. За однакових довжин властивості завадостійких кодових послідовностей можуть відрізнятися. Завадостійкість буде залежати як від довжин цих кодових послідовностей, так і від декількох інших характеристик, наприклад – взаємної кореляції послідовностей. Тобто вибір найкращої завадостійкої кодової послідовності зводиться до алгоритму пошуку таких кодових послідовностей.

Відомі способи перетворення кодових послідовностей не повністю дають змогу вдосконалити системи кодування/декодування. Тому однією з важливих задач є дослідження ефективних моделей удосконалення кодування/декодування інформації за такими показниками, як: швидкість передачі даних, завадостійкість кодових послідовностей, простота виправлення та знаходження помилок. Такими моделями можуть бути нееквідистантні кодові послідовності, які складаються з цілих чисел або послідовностей чисел, визначених як їх значення, так і значеннями всіх послідовних сум поруч розташованих елементів.

Для вирішення цієї проблеми розглянемо нееквідистантні кодові послідовності. Під нееквідистантними кодовими послідовностями будемо вважати послідовності, в яких дозволені кодові комбінації утворюють послідовності з різними відстанями між одиницями та нулями.

Табл. 1. Дозволені кільцеві суми завадостійкої нееквідистантної кодової послідовності

p_j	q_i					
	1	2	$l-1$	1	$n-1$	n
1	k_1	$\sum_{i=1}^2 k_i$	$\sum_{i=1}^{l-1} k_i$	$\sum_{i=1}^l k_i$	$\sum_{i=1}^{n-1} k_i$	$\sum_{i=1}^n k_i$
2	$\sum_{i=1}^n k_i$	k_2	$\sum_{i=2}^{l-1} k_i$	$\sum_{i=2}^l k_i$	$\sum_{i=2}^{n-1} k_i$	$\sum_{i=2}^n k_i$
$l-1$	$\sum_{i=l-1}^n k_i + \sum_{i=1}^1 k_i$	$\sum_{i=l-1}^n k_i + \sum_{i=1}^2 k_i$	k_{l-1}	$\sum_{i=l-1}^l k_i$	$\sum_{i=l-1}^{n-1} k_i$	$\sum_{i=l-1}^n k_i$
1	$\sum_{i=1}^n k_i + \sum_{i=1}^1 k_i$	$\sum_{i=1}^n k_i + \sum_{i=1}^2 k_i$	$\sum_{i=1}^n k_i$	k_l	$\sum_{i=l}^{n-1} k_i$	$\sum_{i=l}^n k_i$
$n-1$	$\sum_{i=n-1}^n k_i + \sum_{i=1}^1 k_i$	$\sum_{i=n-1}^n k_i + \sum_{i=1}^2 k_i$	$\sum_{i=n-1}^n k_i + \sum_{i=1}^{l-1} k_i$	$\sum_{i=n-1}^n k_i + \sum_{i=1}^l k_i$	k_{n-1}	$\sum_{i=n-1}^n k_i$
n	$\sum_{i=n}^n k_i + \sum_{i=1}^1 k_i$	$\sum_{i=n}^n k_i + \sum_{i=1}^2 k_i$	$\sum_{i=n}^n k_i + \sum_{i=1}^{l-1} k_i$	$\sum_{i=n}^n k_i + \sum_{i=1}^l k_i$	$\sum_{i=1}^n k_i$	k_n

Загальна кількість всіх кільцевих сум ваг елементів нееквідистантної кодової послідовності, які мають різні значення:

$$S_n = n^2 - (n-1). \quad (1)$$

При значеннях $p_j = 1$, $q_j = n$, а також при значеннях $p_j \neq 1$, $q_j = p_j - 1$ кільцеві суми ваг елементів нееквідистантної кодової послідовності дорівнюють S_n .

Число S_n^* кільцевих сум на послідовності ваг елементів визначається такою залежністю:

$$S_n^* = n(n-1). \quad (2)$$

Ці нееквідистантні кодові послідовності мають деякі переваги перед іншими завадостійкими послідовностями. Це простота знаходження і виправлення помилок на стороні прийому даних, бо поява символу "1" та/або символу "0", у вигляді завади говорить про помилку, оскільки змінилась кількість дозволених відстаней.

Помилка не знаходиться тільки тоді, коли кількість хибних кодів рівна або більше кодової відстані. Якщо в цій нееквідистантній кодовій послідовності появились спотворені символи, то вони будуть виявлені, що сприяє високій завадостійкості нееквідистантної послідовності.

Завдання покращення завадостійких характеристик нееквідистантних кодових послідовностей варто вирішувати на основі застосування ідеальних кільцевих в'язанок (ІКВ).

Ідеальною числовою в'язанкою будемо називати в'язанку, в якій множина всіх чисел вичерпує значення, які є пропорційні елементам натурального ряду зі заданою кількістю повторів для кожного елемента цього ряду.

Нееквідистантною кодовою послідовністю називають послідовність елементів $K_n = \{k_i, i = \overline{1, n}\}$, де всі можливі поруч розташовані елементи у вигляді кільцевих сум дають значення всіх чисел натурального ряду $1, 2, \dots, S_n = n^2 - (n-1)$.

Виходячи з визначення побудуємо таблицю кільцевих сум моделі нееквідистантної кодової послідовності K_n (табл. 1).

Розглянемо побудову завадостійкої кодової послідовності. Для прикладу, візьмемо нееквідистантну кодову послідовність, побудовану відповідно до ваг елементів ІКВ 8-го порядку 4-тої кратності: 1, 1, 1, 2, 2, 1, 3, 4.

Оскільки ці значення ваг елементів є числами в'язанки 8-го порядку 4-тої кратності, то кожне з цих чисел натурального ряду від 1 до $n(n-1)/r = 15$ буде представлено різними чотирма способами, а кількість всіх способів дорівнює кількості отриманих чисел.

Для нееквідистантної кодової послідовності з кількістю (n) елементів в'язанки наш алгоритм дає можли-

вiсть кодування будь-яких чисел вiд 1 до $S_n = n(n-1)/r+1$.

Кодовi комбiнацiї нееквiдистантної кодової послiдовностi 00000100, 00100000, 01000000, 10000000 представляють чотири способи кодування числа 1. Число 2 кодується в такий спосiб 00001000, 00010000, 01100000, 11000000. Число 3 кодується вiдповiдно

00000010, 00001100, 00110000, 11100000, число 4 – 00000001, 00000110, 00011000, 01110000, i т. д., число 14 – 10111111, 11111011, 11011111, 01111111, число 15 – 11111111.

Синтезовану завадостiйку кодову послiдовнiсть на основi ваг IKB показує табл. 2.

Табл. 2. Завадостiйка кодова послiдовнiсть на основi ваг IKB порядку $n = 8$ кратностi $r = 4$: 1, 1, 1, 2, 2, 1, 3, 4

1	1	1	1	0	1	0	1	1	0	0	1	0	0	0
0	1	1	1	1	0	1	0	1	1	0	0	1	0	0
0	0	1	1	1	1	0	1	0	1	1	0	0	1	0
0	0	0	1	1	1	1	0	1	0	1	1	0	0	1
1	0	0	0	1	1	1	1	0	1	0	1	1	0	0
0	1	0	0	0	1	1	1	1	0	1	0	1	1	0
0	0	1	0	0	0	1	1	1	1	0	1	0	1	1
1	0	0	1	0	0	0	1	1	1	1	0	1	0	1
1	1	0	0	1	0	0	0	1	1	1	1	0	1	0
0	1	1	0	0	1	0	0	0	1	1	1	1	0	1
1	0	1	1	0	0	1	0	0	0	1	1	1	1	0
0	1	0	1	1	0	0	1	0	0	0	1	1	1	1
1	0	1	0	1	1	0	0	1	0	0	0	1	1	1
1	1	0	1	0	1	1	0	0	1	0	0	0	1	1
1	1	1	0	1	0	1	1	0	0	1	0	0	0	1

Кожнiй числовiй комбiнацiї завадостiйкої нееквiдистантної кодової послiдовностi вiдповiдає набiр одиниць та нулiв, який будується за вагами IKB за таким правилом: 1 це 1, 2 – 10, 3 – 100, 4 – 1000 i так далi.

Кiлькiсть рiзних $S_N(S_N-1)/2$ кодових послiдовностей мiстить точно R iз N одиничних символiв у вiдповiдних розрядах, що впливає з властивостей IKB. Iншi $N-R$ символiв будь-яких двох нееквiдистантних кодових послiдовностей вiдрiзняються вiд символiв, якi представленi в одинийменних розрядах.

Отже, мiнiмальна кодова вiдстань будь-якої завадостiйкої нееквiдистантної кодової послiдовностi, що побудована за допомогою IKB, буде визначена у виглядi спiввiдношення порядку та кратностi IKB:

$$d_{\min} = 2(n-r) \quad (3)$$

Для збiльшення кiлькостi дозволених комбiнацiй нееквiдистантних кодових послiдовностей за допомогою IKB побудуємо дзеркальну завадостiйку нееквiдистантну кодову послiдовнiсть з вагами IKB, де помiняємо мiсцями одиниць i нулi при кодуваннi. Кодовi комбiнацiї 01111111, 10111111, 11011111, 11111011 вiдповiдають чотирьом способам кодування числа 1. Кодуванню числа 2 вiдповiдають 00111111, 10011111, 11101111, 11110111. Числу 3 вiдповiдають 00011111, 11001111, 11110011, 11111101, числу 4 – 10001111, 11100111, 11111001, 11111110 i т. д., числу 14 – 10000000, 01000000, 00100000, 00000100, числу 15 – 00000000. Реалiзовану дзеркальну завадостiйку нееквiдистантну кодову послiдовнiсть з вагами IKB iлюструє табл. 3.

Табл. 3. Дзеркальна завадостiйка кодова послiдовнiсть на основi ваг IKB порядку $n = 8$ кратностi $r = 4$: 1, 1, 1, 2, 2, 1, 3, 4

0	0	0	0	1	0	1	0	0	1	1	0	1	1	1
1	0	0	0	0	1	0	1	0	0	1	1	0	1	1
1	1	0	0	0	0	1	0	1	0	0	1	1	0	1
1	1	1	0	0	0	0	1	0	1	0	0	1	1	0
0	1	1	1	0	0	0	0	1	0	1	0	0	1	1
1	0	1	1	1	0	0	0	0	1	0	1	0	0	1
1	1	0	1	1	1	0	0	0	0	1	0	1	0	0
0	1	1	0	1	1	1	0	0	0	0	1	0	1	0
0	0	1	1	0	1	1	1	0	0	0	0	1	0	1
1	0	0	1	1	0	1	1	1	0	0	0	0	1	0
0	1	0	0	1	1	0	1	1	1	0	0	0	0	1
1	0	1	0	0	1	1	0	1	1	1	0	0	0	0
0	1	0	1	0	0	1	1	0	1	1	1	0	0	0
0	0	1	0	1	0	0	1	1	0	1	1	1	0	0
0	0	0	1	0	1	0	0	1	1	0	1	1	1	0
0	0	0	1	0	1	0	0	1	1	1	0	1	1	0

Кiлькiсть дозволених комбiнацiй основної та дзеркальної завадостiйких кодових послiдовностей:

$$P = 2S_n^r \quad (4)$$

Кiлькiсть помилок t_1 , якi виявляються за допомогою завадостiйкої кодової послiдовностi, визначається за допомогою мiнiмальної кодової вiдстанi d_{\min} :

$$t_1 \leq d_{\min} - 1 \quad (5)$$

Кiлькiсть помилок t_2 , якi виправляються за допомогою завадостiйкої кодової послiдовностi, визначається кiлькiстю помилок, що виявляються t_1 :

$$t_2 \leq (t_1 - 1) / 2 \quad (6)$$

Визначимо залежнiсть, що визначає кiлькiсть помилок, що можуть бути виявленi t_1 завадостiйкою кодовою послiдовнiстю:

$$t_1 \leq 2(n-r) - 1 \quad (7)$$

Визначимо залежність, що визначає кількість помилок, що можуть бути виправлені t_2 завадостійкою кодовою послідовністю:

$$t_2 \leq n - r - 1. \quad (8)$$

Мінімальну кодову відстань для завадостійкої кодової послідовності визначимо як

$$d_{1,2} = S_n - 2(n - r). \quad (9)$$

Знайдемо залежності для визначення кількості помилок, що можуть бути виявлені за допомогою завадостійкої кодової послідовності:

$$t_1 \leq \begin{cases} 2(n - r) - 1, & \text{якщо } S_n \geq 4(n - r), \\ S_n - 2(n - r) - 1 - \text{в іншому випадку.} \end{cases} \quad (10), (11)$$

Знайдемо залежності для визначення кількості помилок, що можуть бути виправлені за допомогою завадостійкої кодової послідовності:

$$t_2 \leq \begin{cases} n - r - 1, & \text{якщо } S_n \geq 4(n - r), \\ \frac{S_n - 2(n - r + 1)}{2} - \text{в іншому випадку.} \end{cases} \quad (12), (13)$$

Знайдемо оптимальний взаємозв'язок між значеннями параметрів n і r з погляду найкращої коригувальної здатності завадостійкої кодової послідовності. Завадостійкість цієї кодової послідовності зростає зі збільшенням значення різниці $l = n - r$.

Найбільше значення l буде за умови:

$$S_n = 2n. \quad (14)$$

Наведемо взаємозв'язок між параметрами n і r , коли завадостійка кодова послідовність максимально виявляє та виправляє найбільшу кількість помилок:

$$L = \begin{cases} n/2, & n - \text{парне,} \\ (n-1)/2, & n - \text{непарне.} \end{cases} \quad (15)$$

Отримані на основі ідеальних кільцевих в'язанок завадостійкі кодові послідовності можуть знаходити до $n-1$ та виправляти до $n/2-1$ помилок за парними значеннями n , і знаходити до n та виправляти до $(n-1)/2$ помилок за непарними значеннями n за умови, що кількість дозволених комбінацій завадостійких кодових послідовностей на основі в'язанок теоретично збільшується вдвічі за рахунок впровадження дзеркальних завадостійких кодової послідовностей.

2. Розроблення імітаційної моделі завадостійкого кодування. Алгоритм роботи імітаційної моделі завадостійкого кодування за допомогою нееквідистантних комбінаторних конфігурацій, які гуртуються на основі поняття ідеальної кільцевої в'язанки, та представлені числа, які кодуємо в ASCII – формату та реалізованого методу кодування з використанням ідеальної кільцевої в'язанки.

Алгоритм роботи імітаційної моделі завадостійкого кодування охоплює такі етапи:

- ввід даних параметрів коду та вибір ідеальної кільцевої в'язанки;
- вибір кодової комбінації за допомогою ідеальної кільцевої в'язанки;
- генерація завадостійкого коду вибраного числа.

Розроблено блок-схему алгоритму роботи імітаційної моделі завадостійкого кодування за допомогою нееквідистантних комбінаторних конфігурацій (рис. 1).

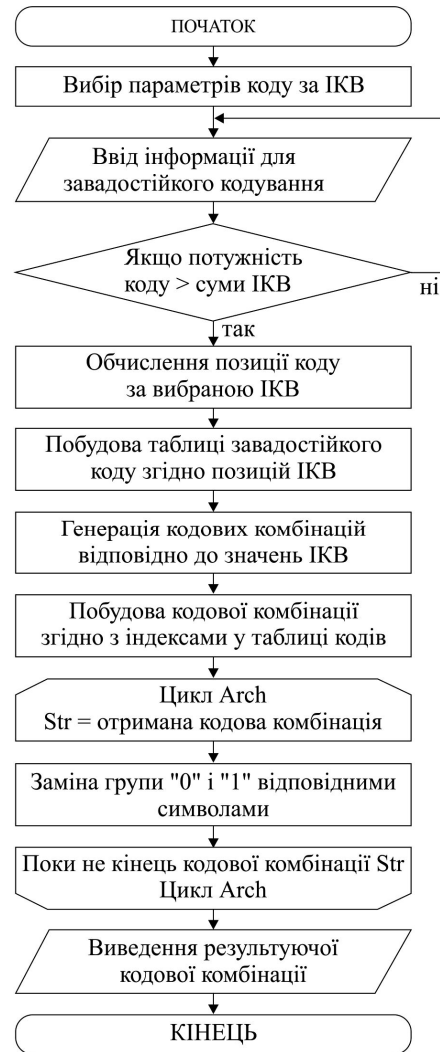


Рис. 1. Блок-схема алгоритму розроблення імітаційної моделі завадостійкого кодування за допомогою нееквідистантних комбінаторних конфігурацій

Блок-схема алгоритму розроблення імітаційної моделі завадостійкого кодування за допомогою нееквідистантних комбінаторних конфігурацій складається з таких блоків:

- блок "Вибір параметрів коду за ІКВ" – за значеннями параметрів коду вибираємо ідеальну кільцеву в'язанку;
- блок "Ввід інформації для завадостійкого кодування" – ввід бажаних параметрів завадостійкого коду з обмеженнями ІКВ;
- блок "Якщо потужність коду більше суми ІКВ" – здійснюється порівняння суми елементів ІКВ із введеним значенням. Якщо введене значення є більше від суми елементів ІКВ, то необхідний повторний ввід числа для вибору іншої ІКВ;
- блок "Обчислення позиції коду за вибраною ІКВ" – знаходяться відповідні позиції у ІКВ та знаходяться відповідні їм суми елементів, які відповідають вибраному числу;
- блок "Побудова таблиці завадостійкого коду згідно позицій ІКВ" – генерується таблиця знайдених комбінацій ІКВ;
- блок "Генерація кодових комбінацій відповідно до значень ІКВ" – генерується таблиця кодових комбінацій, де кожному елементу ІКВ відповідає свій унікальний код;
- блок "Побудова кодової комбінації згідно індексів в таблиці кодів" – формується результат згенерованого завадостійкого коду за рахунок з'єднання двох кодів по чотири біти;
- блок "Цикл Arch. Отримана кодова комбінація" – цикл оброблення отриманої комбінації. Заміна групи "0" та "1" відповідними групами при знаходженні та виправленні помилок.
- блок "Вивід результуючої кодової комбінації" – запис результатів завадостійкого кодування у файл.

Для прикладу, розглянемо розрахунок коригувальної спроможності завадостійких кодів, побудованих за допомогою ІКВ з параметрами: 1) $N = 6, R = 1$; 2) $N = 15, R = 7$; 3) $N = 16, R = 8$.

Оскільки сума ІКВ $S_n = 31$, то довжина кодових комбінацій і потужність коду у всіх цих трьох випадках є однаковою. Максимальна кількість помилок, що підлягають виявленню або виправленню помилок під час реалізації першого з визначених кодів, дорівнює 9 і 4. У кожному з двох інших випадків ІКВ дає змогу згенерувати код, який може виявити до 15 і виправити до 7 помилок. Отже, останні два результати є набагато кращі від попереднього. Отже, загалом будь-яка ІКВ може бути використана для побудови завадостійкого коду. Однак найдоцільніше використовувати коди, що утворені за допомогою ІКВ, параметри яких зв'язані співвідношенням (15).

Імітаційну модель завадостійкого кодування за допомогою нееквідистантних комбінаторних конфігурацій розроблено на мові програмування Borland Delphi 7. Розроблена імітаційна модель безпомилково працює з використанням широкого спектра операційних систем Windows. Для синтезу нееквідистантних завадостійких кодових послідовностей на основі ІКВ розроблено діаграму програмних компонентів, яку подано у вигляді модулів кодування завадостійкої послідовності, модулів генерації випадкових завад, модулів декодування завадостійкої послідовності (рис. 2).

Як видно з діаграми послідовності дій процесу кодування даних, першою дією є вибір користувачем файлу і відкриття потоку читання файлу. Далі йде команда кодування файлу. Поки нема кінця файлу, зчитуємо блок даних. Далі випадково генеруємо завади і записуємо їх у вихідний файловий потік. Потім закриваємо потоки.

Наведемо діаграму послідовності дій для процесу декодування файлу (рис. 3).

Процес декодування даних почнемо з команди відкриття файлу. Після цього подаємо команду на декодування файлу. Закодовані дані з файлу будемо зчитувати блоками поки не кінець файлу. Далі кодер робить перевірку на наявність помилок. У разі, коли помилки знайдені, кодер виправляє їх. Наступною дією є декодування даних блоку та запис у файл.

Після завершення декодування виводимо статистичну інформацію про результат дій декодування.

Діаграми програмних послідовностей показують процес роботи програмного продукту завадостійкого кодування за допомогою нееквідистантних завадостійких кодових послідовностей та ілюструють можливості знаходження та виправлення випадкових завад.

Імітаційна модель завадостійкого кодування за допомогою нееквідистантних комбінаторних конфігурацій має такі особливості:

- вхідними даними будуть параметри завадостійкої нееквідистантної кодової послідовності порядку N кратності R ;
- забезпечує проведення кодування і декодування зі знаходженням та виправленням помилок в кількості до t_2 .

Програма має простий у користуванні та інтуїтивно зрозумілий інтерфейс. Основні елементи на формі вікна (рис. 4):

- Вхідні дані (параметри ІКВ порядку N кратності R).
- Кількість помилок, які треба виправляти (не більше кількості, вказаної у вікні Info).
- Кнопка з надписом <OpenFile>, дає змогу вибрати необхідний файл для кодування, створення генерації випадкових завад та декодування з можливістю виправлення помилок.

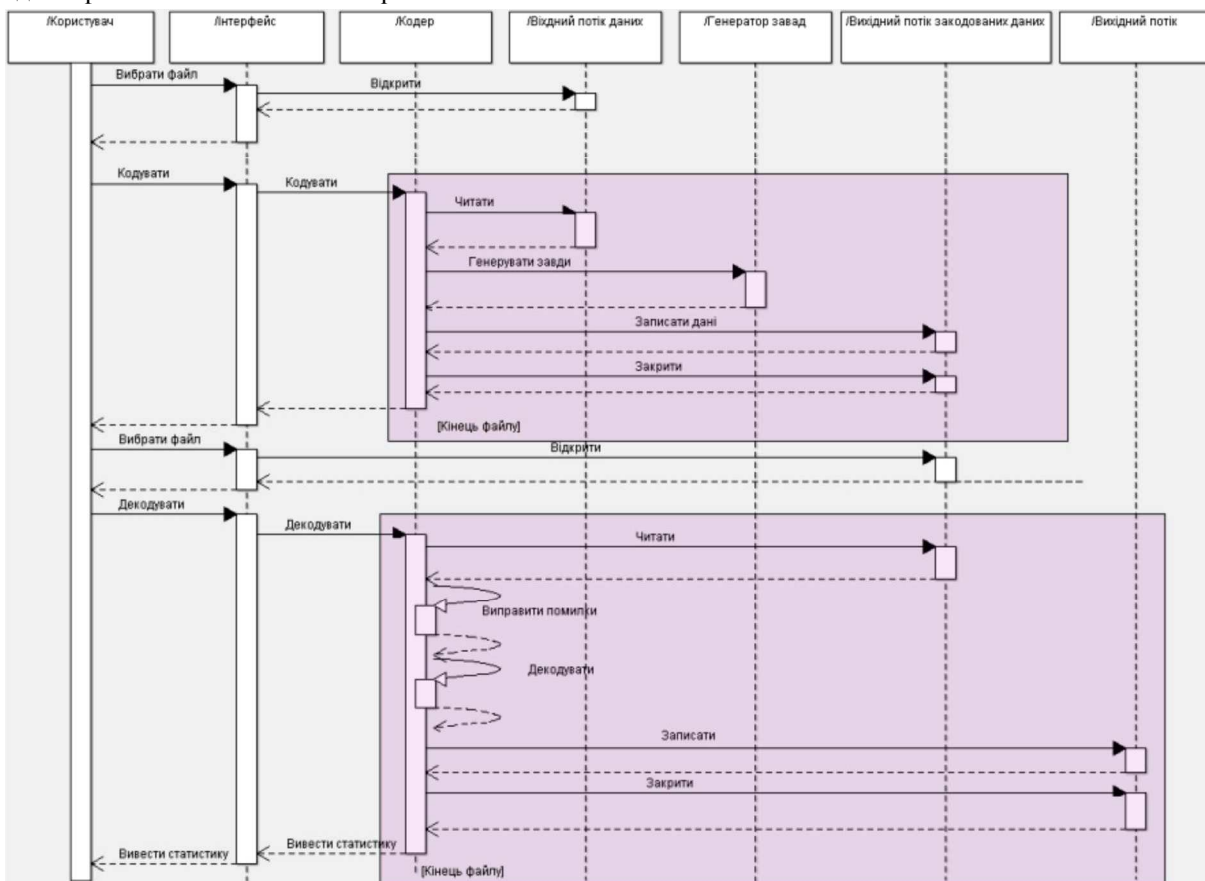


Рис. 2. Діаграма програмних компонентів процесу кодування даних

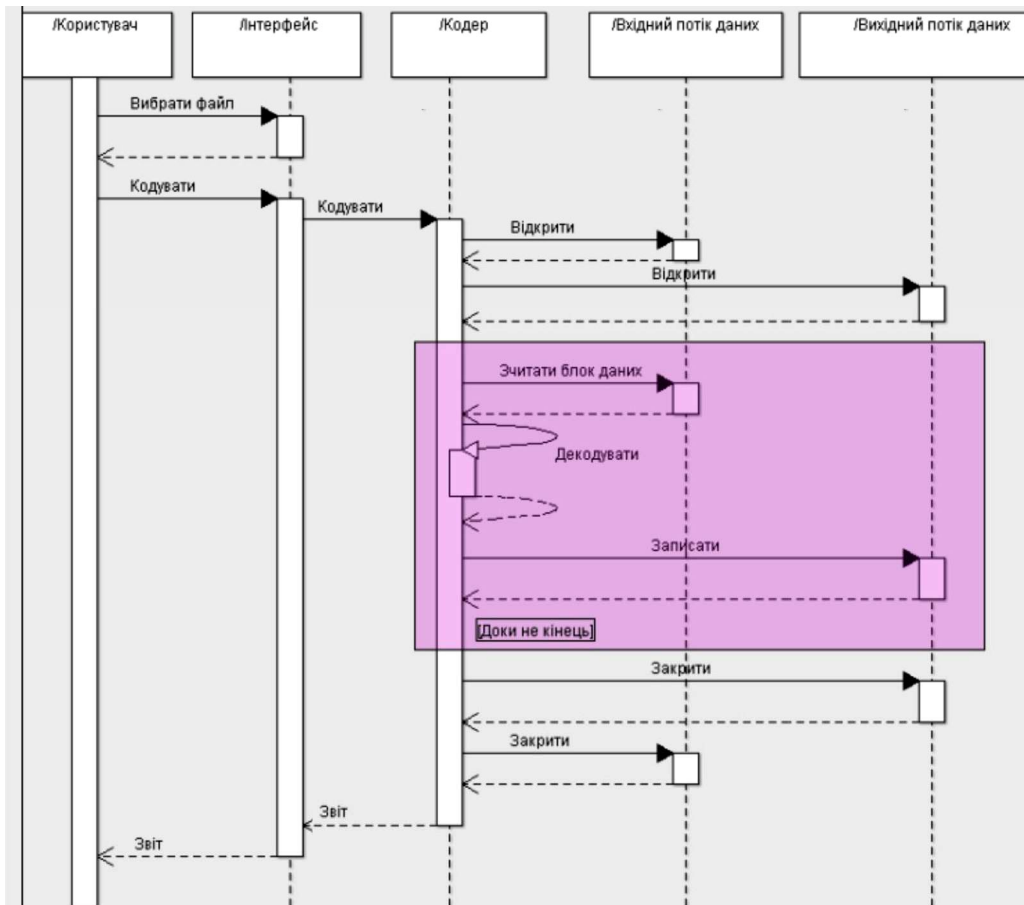


Рис. 3. Діаграма програмних компонентів процесу декодування даних

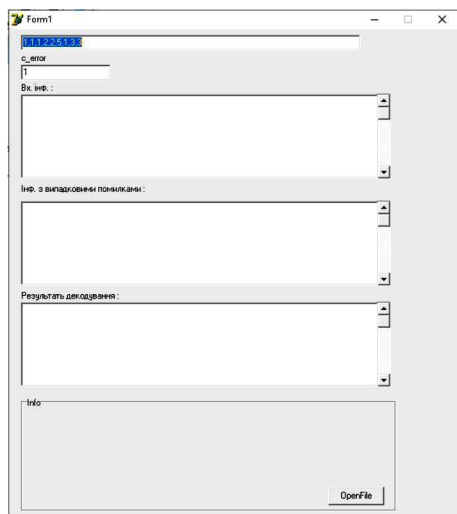


Рис. 4. Основні елементи на формі вікна кодування/декодування з можливістю виправлення за допомогою ІКВ

3. Обговорення результатів дослідження. Проведемо порівняння з кращими відомими завадостійкими кодами Боуза-Чоудхурі-Хоквінхема (БЧХ), які виявляють і виправляють максимальну кількість помилок. Розрахунок залежності між кількістю і інформаційних і кількістю k корегувальних символів у кодовій комбінації завдовжки n , яка може виправляти не менше s помилок, здійснюється на підставі таких виразів:

$$n = i + k ; \quad (16)$$

$$2k \geq n + 1 ; \quad (17)$$

$$2i \leq 2n / (n + 1) ; \quad (18)$$

$$s = \text{ent}(d - 1) / 2 , \quad (19)$$

де d – мінімальна кодова відстань.

Для здійснення порівняльного аналізу кодів БЧХ та досліджуваних кодів скористаємось такими залежностями:

$$N = 2n - 1 ; \quad (20)$$

$$t = 2n - 2 - 1 ; \quad (21)$$

$$P = 2n + 1 ; \quad (22)$$

$$N^* = 2n + 1 ; \quad (23)$$

$$t^* = (N^* - 3) / 4 ; \quad (24)$$

$$P^* = 2(N^* + 1) , \quad (25)$$

де: N і N^* – довжини кодових послідовностей; t і t^* – кількість помилок, що виправляються; P і P^* – потужність кодових послідовностей БЧХ і ІКВ відповідно.

Формули (20)–(22) відповідають співвідношенням параметрів кодів БЧХ [3], а (23)–(25) – параметрам кодів ІКВ, що забезпечують максимальну завадостійкість на довжину кодових послідовностей [4].

Аналіз результатів порівняння цих кодів, здійснених на основі формул (20)–(25), показує, що за фіксованої довжини кодових послідовностей максимальна завадостійкість кодів ІКВ не поступається кодам БЧХ за однакової потужності цих послідовностей. Деякою перевагою коду БЧХ є можливість забезпечення зростання потужності (22), але за рахунок втрати його завадостійкості. На відміну від кодів БЧХ для синтезу кодів ІКВ з високим рівнем завадостійкості не потрібні складні обчислення, а довжина кодових послідовностей визначається лінійною залежністю (23), що дає можливість побудови кодових послідовностей з високим рівнем захищеності від завад.

Результати проведеного кодування і декодування зі знаходженням та виправленням всіх помилок в кількості від одної до чотирьох з використанням завадостійких нееквідистантних кодових послідовностей наведено на рис. 5.

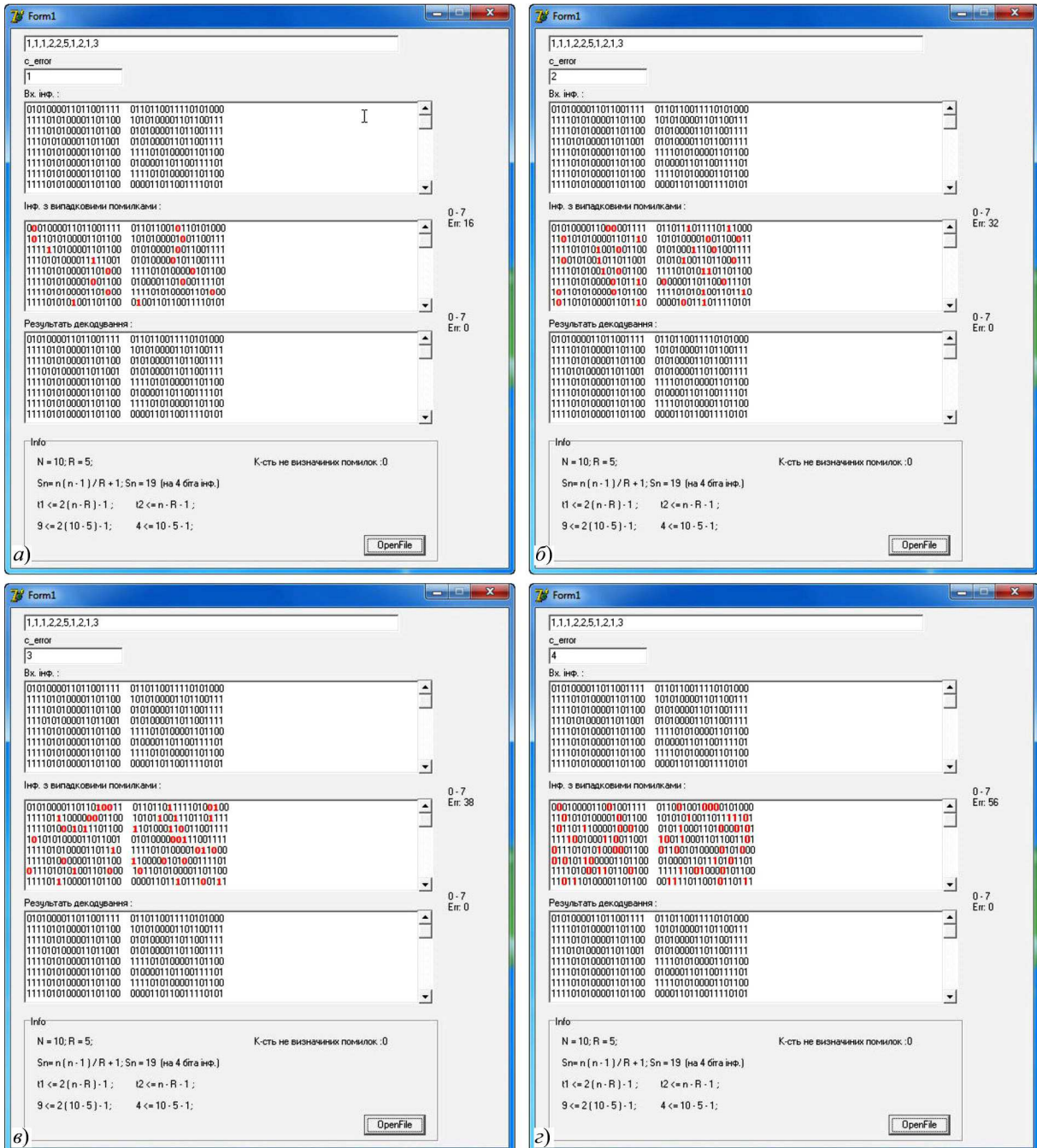


Рис. 5. Проведення операцій кодування, генерації завад та операцій декодування з виправленням всіх однократних (а), двократних (б), трьохкратних (в), чотирьохкратних (г) помилок

Результати проведеного кодування і декодування зі знаходженням та виправленням не всіх п'ятикратних помилок з використанням завадостійких нееквідистантних кодових послідовностей наведено на рис. 6.

Аналізуючи наведені експериментальні дані, які отримано за допомогою розробленої моделі, бачимо, що знаходження та виправлення всіх помилок подано на рис. 5. На рис. 6 є досить значна кількість знайдених, але не виправлених помилок, що повністю відповідає теорії нееквідистантних завадостійких кодових послідовностей.

Висновки

1. Показано, що для усунення завад при передачі кодових послідовностей по каналах бездротового зв'язку доцільно використовувати завадостійке кодування.
2. Удосконалено метод синтезу завадостійких кодових послідовностей, який завдяки використанню ідеальних

кільцевих в'язанок забезпечив збільшення завадостійкості отриманих послідовностей, знаходження до 50 % та виправлення до 25 % спотворених символів від довжини завадостійкої кодової послідовності.

3. Розроблено на мові програмування Borland Delphi 7 імітаційну модель завадостійкого кодування за допомогою нееквідистантних конфігурацій, яка орієнтована на невеликі обчислювальні потужності та безпомилково працює з використанням широкого спектра операційних систем Windows.
4. Показано, що використання ідеальних кільцевих в'язанок для синтезу завадостійких кодових послідовностей істотно спрощує процес синтезу та забезпечує його реалізацію в реальному часі.
5. Визначено, що перспективою подальших досліджень є зменшення надлишковості, яке можна досягнути шляхом використання дзеркальних нееквідистантних завадостійких кодових послідовностей.

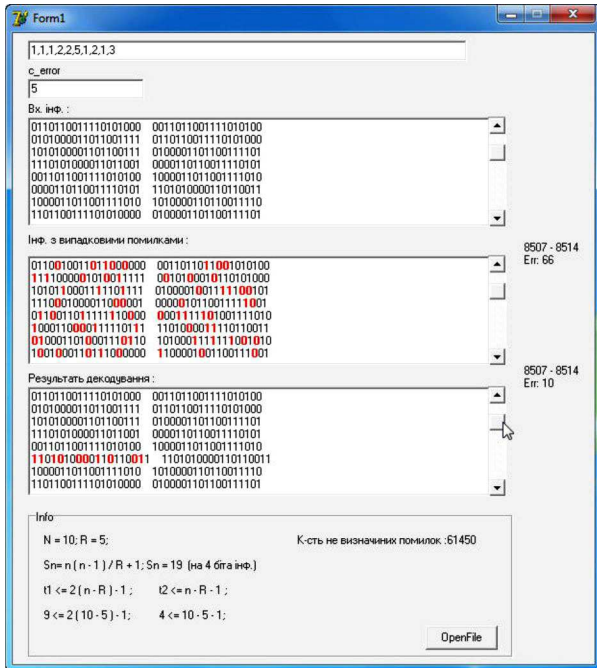


Рис. 6. Проведення операцій кодування, генерації завдань та операцій декодування з виправленням не всіх п'ятикратних помилок

References

1. Бэрлекэмп, Э. (1971). *Алгебраическая теория кодирования*. Москва: Изд-во Мир, 478 с.
2. Касами, Т., Токура, Н., Ивадари, Е., Инасаки, Я. (1978). *Теория кодирования*. Москва: Изд-во Мир, 576 с.
3. Різник, В. В. (1989). *Синтез оптимальних комбінаторних систем*. Львів: Вища шк., 168 с.
4. Цымбал, В. П. (1982). *Теория информации и кодирование*. Київ: Вища шк., 304 с.
5. Ahmad, J., Akula, A., Mulaveesala, R., & Sardana, H. K.. (2019). Barker-Coded Thermal Wave Imaging for Non-Destructive Testing and Evaluation of Steel Material. In *IEEE Sensors Journal*, 19(2), 735–742. <https://doi.org/10.1109/JSEN.2018.2877726>
6. Gryciuk, Yu., Grytsyuk, P. (2015). Perfecting of the matrix Affine cryptosystem information security. *Computer Science and Information Technologies: Proceedings of Xth International Scientific and Technical Conference (CSIT'2015)*, 14–17 September, 2015, pp. 67–69. <https://doi.org/10.1109/scsit.2015.7325433>

7. Fu, J., & Ning, G. (2018). Barker coded excitation using pseudo chirp carrier with pulse compression filter for ultrasound imaging (BIBE 2018). *International Conference on Biological Information and Biomedical Engineering*, Shanghai, China, pp. 1–5.
8. Riznyk, O., Kynash, Y., Povshuk, O., & Bohdan, B. (2017). Information technologies of optimization of structures of the systems are on the basis of combinatorics methods. *12th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT)*. Lviv, pp. 232–235. [https://doi.org/10.1109/STC-\(CSIT\).2017.8098776](https://doi.org/10.1109/STC-(CSIT).2017.8098776)
9. Riznyk, O., Kynash, Y., Povshuk, O., & Noga, Y. (2018). The Method of Encoding Information in the Images Using Numerical Line Bundles. *IEEE 13th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT)*. Lviv, pp. 80–83. [https://doi.org/10.1109/STC-\(CSIT\).2018.8526751](https://doi.org/10.1109/STC-(CSIT).2018.8526751)
10. Riznyk, O., Povshuk, O., Kynash, Y., & Yurchak, I. (2017). Composing method of anti-interference codes based on non-equidistant structures. *XIIIth International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH)*. Lviv, pp. 15–17.
11. Riznyk, O., Povshuk, O., Noga, Y., & Kynash, Y. (2018). Transformation of Information Based on Noisy Codes. *IEEE Second International Conference on Data Stream Mining & Processing (DSMP)*. Lviv, pp. 162–165. <https://doi.org/10.1109/DSMP.2018.8478509>
12. Tsmots, I., Rabyk, V., & Riznyk, O., Kynash, Y. (2019). Method of Synthesis and Practical Realization of Quasi-Barker Codes. *2019 IEEE 14th International Conference on Computer Sciences and Information Technologies (CSIT)*. Lviv, Ukraine, pp. 76–79. [https://doi.org/10.1109/STC-\(CSIT\).2019.8929882](https://doi.org/10.1109/STC-(CSIT).2019.8929882)
13. Wang, M., Cong, S., & Zhang, S. (2018). Pseudo Chirp-Barker-Golay coded excitation in ultrasound imaging. *Chinese Control And Decision Conference (CCDC)*, Shenyang, 4035–4039. <https://doi.org/10.1109/CCDC.2018.8407824>
14. Wang, S., & He, P. (2018). Research on Low Intercepting Radar Waveform Based on LFM and Barker Code Composite Modulation. *International Conference on Sensor Networks and Signal Processing (SNSP)*, Xi'an, China, pp. 297–301. <https://doi.org/10.1109/SNSP.2018.00064>
15. Xia, S., Li, Z., Jiang, C., Wang, S., & Wang, K. (2018). Application of Pulse Compression Technology in Electromagnetic Ultrasonic Thickness Measurement. *IEEE Far East NDT New Technology & Application Forum (FENDT)*, Xiamen, China, pp. 37–41. <https://doi.org/10.1109/FENDT.2018.8681975>

I. G. Tsmots¹, O. Ya. Riznyk¹, Yu. I. Budaretskij², C. Z. Lvovskij¹, M. V. Tsitsyuk²

¹ Lviv Polytechnic National University, Lviv, Ukraine

² Hetman Petro Sahaidachnyi National Army Academy, Lviv, Ukraine

IMPROVEMENT OF THE METHODS OF SYNTHESIS AND DEVELOPMENT OF A SIMULATION MODEL OF ANTI-JAMMING CODING

Noise immunity is one of the most important characteristics of modern data reception/transmission systems. Improving noise immunity at fixed data reception/transmission speeds is an urgent problem, for example, for drone control. The studied code sequences allow increasing the power of the obtained sequences due to the use of mirror noise-resistant code sequences. Increasing the noise immunity of data transmission is achieved by increasing the length and power of the noise-tolerant code sequence used to transmit a single message. The advantages of these sequences, such as high noise immunity in relation to high-band narrowband noise, the possibility of dividing subscribers by code, transmission secrecy, high resistance to multipath, high resolution in navigation measurements will be widely used in communication and geolocation systems. The method for synthesizing noise-tolerant code sequences using ideal ring bundles is improved. The method for quick finding such noise-tolerant code sequences that are able to find and correct errors to the greatest extent depending on the length of the obtained code sequence is also improved. The algorithm for fast finding of such noise-tolerant code sequences, which are able to find and correct errors to the greatest extent depending on the length of the obtained code sequence, is implemented. A simulation model of noise-tolerant coding using ideal ring bundles is developed. The software implementation of the simulation model of noise-tolerant coding for finding and correcting errors in the obtained noise-tolerant code sequences is performed. The proposed noise-tolerant code sequences have practical value, as the resulting code sequence allows us to easily and quickly find up to 50 % and correct up to 25 % of distorted characters from the length of the noise-tolerant code sequence.

Keywords: ideal ring bundle; mirror code sequence; non-equidistant code sequence; non-equidistant combinatorial configuration.