



УКРАЇНА

(19) UA (11) 64597 (13) U

(51) МПК (2011.01)

H03M 13/00

G06F 11/273 (2006.01)

ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИ

ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

видається під
відповідальність
власника
патенту

(54) СПОСІБ ПЕРЕДАВАННЯ ДВІЙКОВОЇ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ СИГНАТУРНОГО КОНТРОЛЮ

1

2

(21) u201105016

(22) 20.04.2011

(24) 10.11.2011

(46) 10.11.2011, Бюл.№ 21, 2011 р.

(72) РИСОВАНІЙ ОЛЕКСАНДР МИКОЛАЙОВИЧ, ГОГОВ ВАЛЕРІЙ ВАСИЛЬОВИЧ, КОЛОМІЙЦЕВ ОЛЕКСІЙ ВОЛОДИМИРОВИЧ, ЛИТОВСЬКИЙ ВІТАЛІЙ ДМИТРОВИЧ, ПРИХОДЬКО ВОЛОДИМИР МУСІЙОВИЧ, ШОСТАК АНАТОЛІЙ ВАСИЛЬОВИЧ, КОЗИНА ОЛЬГА АНДРІЇВНА, ТІМОНОВ ОЛЕКСІЙ ОЛЕКСІЙОВИЧ, ЛЕГЕЗА ОЛЕКСІЙ МИКОЛАЙОВИЧ

(73) НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ "ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"

(57) Спосіб передавання двійкової інформації з використанням сигнатурного контролю, в якому двійкову інформаційну n -розрядну послідовність кодують циклічним кодом, який відрізняється тим, що інформаційна n -розрядна послідовність ділиться на частини розрядністю k , всі ці частини представляються в паралельному вигляді, для кожної такої частини, за утворюючим поліномом $P(X)$ при $2^{\deg P(X)} \leq n$, отримується сигнатура, яка обчислюється з урахуванням ваги кожного розряду у цій послідовності n .

Корисна модель належить до техніки передавання даних і може бути використана в інформаційно-вимірювальних системах та комп'ютерних мережах.

Відомий спосіб кодування двійкової інформації із захистом [1], в якому на боці передавача додатково формують кодові комбінації з використанням матриць Хаара, формують таблиці відповідності між інформаційними повідомленнями та кодовими комбінаціями, на боці приймача кодові комбінації з каналу зв'язку порівнюють з базовими, що зберігаються у таблиці відповідності, а захист даних забезпечується завдяки нероздільності інформаційних і контрольних символів в кодовому слові.

Недоліком цього способу є складність математичних перетворень з використанням функцій Хаара при великій кількості додаткових символів коду (обсяг даних, що передаються, вдвічі перевищує обсяг інформаційних повідомлень). Це призводить до великих витрат часу на кодування та збільшення часу на передавання заданого обсягу інформаційних повідомлень.

Найбільш близьким по технічній суті до запропонованого є спосіб, вибраний як прототип [2], завадостійкого кодування на основі БХ-фільтрів, в якому на стороні передавача на тактах від 1 до k одночасно кодують k -розрядні інформаційні вектори множенням на g -розрядний породжувальний поліном циклічного (n, k) - коду і шифрують їх ді-

ленням на допоміжні поліноми степені не більше k , вибрані по псевдовипадковому алгоритму, потім на тактах від $k+1$ до n кодують k -розрядні обчислені кодові вектори множенням на g -розрядний породжувальний поліном коду, а на стороні приймача спочатку декодують отримані по каналу зв'язку кодові вектори за допомогою алгоритму Берлекемпа-Мессі, а потім дешифрують їх множенням на допоміжні поліноми.

Недоліками цього способу є зменшення завадостійкості кодування на боці передавача та ускладнення процесу дешифрування кодових векторів на боці приймача. Це призводить до збільшення загальних витрат часу на кодування, декодування та захист інформаційних повідомлень.

В основу корисної моделі поставлена задача створити спосіб передавання двійкової інформації з використанням сигнатурного контролю цієї послідовності, що дозволяє спростити процес утворення коду та локалізувати однократні помилки.

Задача вирішується за рахунок того, що двійкова інформаційна послідовність розрядністю n ділиться на частини (канали) розрядністю k та представляється в паралельному вигляді; для кожної такої частини, за утворюючим поліномом $P(X)$ при $2^{\deg P(X)} \leq n$, отримується сигнатура sig , яка обчислюється з урахуванням ваги кожного розряду у n -розрядній послідовності. Таким чином,

(19) UA (11) 64597 (13) U

результуюча сигнатура завжди дорівнює сумі часткових сигнатур всіх каналу.

Розглянемо приклад. Нехай вхідна послідовність $V(t) = 11111000010010000011001000101$

має розрядність $n = 30$. Вибрано утворюючий поліном $P(X) = x^5 \oplus x^3 \oplus 1$, матриця станів якого має вигляд:

1	0	0	1	0	1	1	0	0	1	1	1	1	1	0	0	0	1	1	0	1	1	1	0	1	0	1	0	0	0	0
0	1	0	0	1	0	1	1	0	0	1	1	1	1	1	0	0	0	1	1	0	1	1	1	0	1	0	1	0	0	0
0	0	1	0	0	1	0	1	1	0	0	1	1	1	1	1	0	0	0	1	1	0	1	1	1	0	1	0	1	0	0
0	0	0	1	0	0	1	0	1	1	0	0	1	1	1	1	1	0	0	0	1	1	0	1	1	1	0	1	0	1	0
0	0	0	0	1	0	0	1	0	1	1	0	0	1	1	1	1	1	1	0	0	1	1	0	1	1	1	0	1	0	1
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Припустимо, що послідовність передається по трьом каналам з розрядністю в кожному $k_i = 10$, $i = \overline{1,3}$. Інформаційні дані по кожному каналу супроводжується своїми сигнатурами, які отримані з урахуванням ваги кожного розряду у цій двійковій послідовності. Таким чином, двійкова інформація, яка поділена на три канали по 10 інформаційних розрядів в кожному та відповідними сигнатурами ($\text{sig} A1 = 11101 \text{sig} A2 = 11010 \text{sig} A3 = 00101$),

отриманими за поліномом $P(X) = x^5 \oplus x^3 \oplus 1$, мають вигляд, наведений на фіг. 1.

Введемо однократну помилку в 22 розряді (на фіг. 1 у верхньому рядку розряд виділено підкреслюванням) та кратну помилку (розряди: 1, 7, 11, 17). В такому випадку сигнатури з помилками будуть мати вигляд:

$$\text{sig}^{\text{ном}} A1 = 10111 \text{sig}^{\text{ном}} A2 = 00000 \text{sig}^{\text{ном}} A3 = 10111$$

Для визначення помилкових розрядів необхідно обчислити синдром помилки, який визначається як:

$$\text{sid} V(t) = \text{sig} V(t) \oplus \text{sig}^{\text{ном}} V(t).$$

Тоді

$$\text{sid} A3 = 00101 \oplus 11110 = 11011 = h_{22};$$

$$\text{sid} A2 = 11010 \oplus 00000 = 11011 = h_7;$$

$$\text{sid} A1 = 11101 \oplus 10111 = 01010 = h_{28},$$

де h_i – i - розряд в матриці станів.

У зв'язку з тим, що по першому каналу $A1$ передаються інформаційні розряди з номерами 1-10, а синдром помилки відповідає 28-му розряду, який не належить цьому діапазону, то робиться висновок про здійснення багатократної помилки. Відповідно й до другого каналу $A2$: по ньому передаються інформаційні розряди з номерами 11-20, а синдром помилки відповідає 7-му розряду; робиться висновок про здійснення багатократної помилки. По третьому каналу $A3$ передаються інформаційні розряди з номерами 21-30 та синдром помилки відповідає 22-му розряду, номер якого належить до цього діапазону. Таким чином, робиться висновок, що здійснена однократна помилка по 22-му розряду, який слід виправити на правильний (виконати операцію інвертування).

Позитивним технічним результатом є те, що отримано спосіб передавання двійкової інформації, який дозволяє спростити процес формування

коду, як контрольні розряди якого використано сигнатури, виявляти багатократні та локалізувати однократні помилки.

При пошуку в патентній та науково-технічній літературі не виявлено об'єктів з ознаками, подібними до відмінних ознак технічного рішення, що заявляється, на підставі чого можна зробити висновок про відповідність його критерію "суттєвої відмінності".

Спосіб, що пропонується, може бути реалізований, наприклад, за допомогою пристрою, структурна схема якого наведена на фіг. 2. Пристрій включає: вхід 1 "Вхідні дані"; вхід 2 "Старт"; вхід 3 "Стоп"; вхід 4 "Синхросигнал"; блок керування 5; сигнатурні аналізатори 6_{1-6_m} ; блоки множення 7_{1-7_m} сигнатури на матрицю зв'язків ступеня, яка дорівнює розрядності частині інформаційної послілки, для якої обчислюється ця сигнатура; блоки 8_{1-8_m} дозволу запису результуючої сигнатури у вихідні регістри каналів 9_{1-9_m} ; кодові посилки з сигнатурним контролем 10_{1-10_m} , які для кожного каналу складаються з вхідних даних та сигнатур; сигнали керування 11_{1-11_m} блоками 8_{7-8_m} ; сигнали 12_{1-12_m} , передавання даних до m каналів 13_{1-13_m} формування сигнатурного контролю.

Пристрій працює наступним чином.

З приходом сигналу 2 "Старт" на блок керування 5 починають проходити в схему вхідні дані 1, які синхронізуються синхросигналами за входом 4. Блок керування ділить вхідну послідовність на блоки довжиною k - розрядів та послідовно видає їх, з початку, до каналу 13_1 формування сигнатурного контролю. Регістри 9_{1-9_m} являють собою регістри зсуву з можливістю паралельного запису. За синхросигналами (на схемі не показано) дані поступово записуються до регістра 9_1 каналу 13_1 та оброблюються в сигнатурному аналізаторі 6_1 . Після подачі останнього розряду даних зі входу 12_1 за сигналом керування 11_1 сформована сигнатура каналу 13_1 записується в вільну частину регістра 9_1 . Після цього, блок керування 5 зупиняє подачу даних до першого каналу 13_1 та починає обробку даних в другому каналі 13_2 . Блоки множення 7_{1-7_m} сигнатури на матрицю зв'язків відповідного ступеня необхідні для обчислення сигнатури з урахуванням ваги кожного розряду. Матриця зв'язків S описує зв'язки входів та виходів класичного одноканального сигнатурного аналізатора, у відповідності до вибраного утворюючого поліному, та в загальному випадку має вигляд:

$$S = \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_{r-1} & \alpha_r \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 \dots & 0 & 0 \\ \dots & & & & \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix},$$

де α_i - значення i -го коефіцієнта при показнику ступеня утворюючого поліному.

Процес закінчення обробки даних завершується при подачі сигнала "Стоп" на вході 3. При цьо-

му, на виходах $10_1, 10_m$ встановлюється кодова посилка з сигнатурним контролем.

Джерела інформації

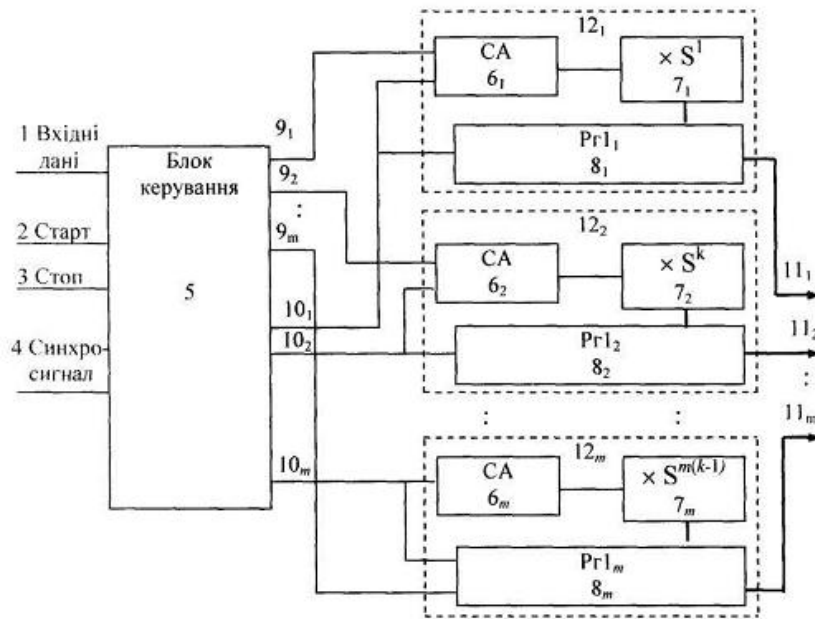
1. Патент України на корисну модель №5440, М. кл. Н03М 13/00, Бюл. №3, 2005.

2. Кириллов С.Н., Семин Д.С. Модифицированный помехозащищенный кодер на основе БИХ-фильтра //Вестник РГРТУ. Рязань - 2009. - №2 (выпуск 28). -с. 27-30 (прототип).

1000011111 | 00101
1000001000 | 11010
1010001001 | 11101

Інформаційні Сигнатури
розряди

Фиг. 1



Фиг. 2