УКРАЇНА

(19) UA (11) 50203 (13) U

(51) МПК (2009)
H03M 13/00

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ

ОПИС
ДО ПАТЕНТУ
НА КОРИСНУ МОДЕЛЬ

видається під
відповідальність
власника
патенту

(54) СПОСІБ ЗАВАДОСТІЙКОГО КОДУВАННЯ ДИСКРЕТНОЇ ІНФОРМАЦІЇ ІЗ ЗАХИСТОМ

(21) u200913294
(22) 21.12.2009
(24) 25.05.2010
(46) 25.05.2010, Бюл.№ 10, 2010 р.
(72) СЕМЕРЕНКО ВАСИЛЬ ПЕТРОВИЧ, ДУБРОВ ОЛЕКСАНДР ФЕДОРОВИЧ
(73) ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
(57) Спосіб завадостійкого кодування дискретної інформації із захистом, в якому на боці передавача кодують k-розрядні інформаційні вектори множенням на (n-k)-розрядний породжувальний поліном циклічного (n,k)-коду і шифрують їх, а на боці приймача декодують отримані з каналу зв'язку n-розрядні кодові вектори діленням на (n-k)-розрядний породжувальний поліном циклічного (n,k)-коду і дешифрують їх, який **відрізняється** тим, що після кодування шифрують n-розрядні кодові вектори порозрядним додаванням по модулю два до них секретного n-розрядного вектора пароля, а перед декодуванням дешифрують порозрядним додаванням по модулю два до отриманих з каналу зв'язку n-розрядних кодових векторів цього ж n-розрядного вектора пароля.

1

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

Відомий спосіб кодування дискретної інформації із захистом, 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 [Патент України на корисну модель №5440, М. кл. H03M 13/00, Бюл. №3, 2005].

Недоліками цього способу є складність математичних перетворень з використанням функцій Хаара та низька завадостійкість (виправляється лише одна помилка в кодовій комбінації) 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 завадостійкого кодування на основі БІХ-фільтрів [Кириллов С.Н., Семин Д.С. Модифицированный помехозащищеиный кодер на основе БИХ-фильтра //Вестник РГРТУ. Рязань - 2009. - №2(выпуск 28). - с. 27-30], в якому на стороні передавача на тактах від 1 до k одночасно кодують k-розрядні інформаційні вектори множенням на r-розрядний породжувальний поліном циклічного (n,k)-коду і шифрують їх діленням 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 r-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.

2

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 створення способу завадостійкого кодування дискретної інформації із захистом, в якому, за рахунок того, що на стороні передавача спочатку кодують, а потім шифрують, а на стороні приймача спочатку дешифрують, а потім декодують, що сприяє збільшенню ступеню захисту та зменшенню загальних витрат часу на виконання операцій декодування і дешифрування.

Поставлена задача досягається тим, що на боці передавача кодують k-розрядні інформаційні

(19) UA (11) 50203 (13) U

вектори множенням на (n-k)-розрядний породжувальний поліном циклічного (n,k)-коду і шифрують їх, а на боці приймача декодують отримані з каналу зв'язку n-розрядні кодові вектори діленням на (n-k)-розрядний породжувальний поліном циклічного (n,k)-коду і дешифрують їх, причому після кодування шифрують n-розрядні кодові вектори порозрядним додаванням по модулю два до них секретного n-розрядного вектора паролю, а перед декодуванням дешифрують порозрядним додаванням по модулю два до отриманих з каналу зв'язку n-розрядних кодових векторів цього ж n-розрядного вектора паролю.

Спосіб здійснюється наступним чином. Спочатку на боці передавача виконується завадостійке кодування заданих інформаційних векторів I(x). Для завадостійкого кодування дискретної інформації використовується циклічний (n,k)-код, над полем Галуа GF(2) з мінімальною кодовою відстанню d_{min}, який задається r-розрядним породжувальним поліномом

$g(x)=g_0+g_1x+g_2x^2+... +g_{r-1}x^{x-1}+g_rx^r$, r=n-k.

Кодовий вектор $C(x)=(c_1,c_2,...,c_n)$ циклічного коду має довжину n, інформаційну розмірність k і дозволяє виправляти всі випадкові помилки кратності $1,2,...,\tau_{min}$ ($\tau_{min}=\frac{d_{min}-1}{2}$).

Для завадостійкого кодування використовується несистематичне кодування циклічних кодів, тобто для отримання n-розрядного кодового вектора C(x) необхідно протягом n тактів часу заданий k-озрядний інформаційний вектор I(x) перемножити на породжувальний поліном g(x):

$$C(x)=I(x)\times g(x). \quad (1)$$

Перевагою несистематичного кодування в циклічних кодах є нероздільність інформаційних і контрольних розрядів, що забезпечує одночасно і захист даних в каналі зв'язку.

Секретність переданих даних буде забезпечена лише при умові збереженні у секреті породжувального полінома. Якщо зловмиснику стане відома ця інформація, йому стануть відомими закодовані інформаційні вектори. Тому для практичного використання захисту інформації на основі циклічних кодів необхідні додаткові заходи підвищення криптостійкості.

Після кодування виконується шифрування за допомогою додавання до n-розрядного кодового вектора C(x) секретного n-розрядного вектора паролю P(x) і в канал зв'язку передається n-розрядний захищений кодовий вектор T(x):

$$T(x)=C(x)\oplus P(x), \quad (2)$$

де $\oplus$ позначає порозрядну логічну операцію по модулю два.

Порозрядна логічна операцію по модулю два виконується послідовно, починаючи із тих розрядів вектора T(x), які першими передаються в канал зв'язку. Тому операція (2) вимагає додатково лише один такт часу.

На боці приймача отриманий із каналу зв'язку вектор $T_{ch}(x)$ спочатку дешифрується, тобто з нього виділяється кодовий вектор $C_{ch}(x)$ за допомогою додавання до n-розрядного вектора T(x) секретного n-розрядного вектора паролю P(x):

$$C_{ch}(x)=T_{ch}(x)\oplus P(x). \quad (3)$$

Операція (3) виконується послідовно, починаючи з тих розрядів вектора $T_{ch}(x)$, які першими надходять із каналу зв'язку. Операція (3) вимагає додатково лише один такт часу, на відміну від відомого способу, в якому операція дешифрування вимагає додатково k тактів часу.

При декодуванні із кодового вектору $C_{ch}(x)$ виділяється початковий інформаційний вектор I(x) діленням кодового вектора $C_{ch}(x)$ на породжувальний поліном g(x):

$$I(x)=\frac{C_{ch}(x)}{g(x)}+R(x). \quad (4)$$

Якщо в результаті ділення (4) буде отримано нульовий вектор синдрому R(x), це буде свідчити, що передача даних по каналу зв'язку виконана без τ_{min} помилок, тобто $C_{ch}(x)=C(x)$. При отриманні ненульового вектора синдрому R(x) далі виконується процедура пошуку помилок в кодовому векторі в межах коректуючої здатності вибраного коду.

Якщо операція (3) не буде виконана, тоді результатом декодування вектора $T_{ch}(x)$ буде завжди ненульовий вектор синдрому R(x), що не дасть можливості а ні визначити правильність передачі даних по каналу зв'язку, а ні відновити інформаційний вектор I(x).

Оскільки n-розрядний вектор паролю P(x) може бути вибрано довільним, існує 2^n варіантів такого вибору. Для одного кодового вектора C(x) шифрування за допомогою операції (2) забезпечує вищий ступінь захисту, оскільки важче підібрати n-розрядний вектор паролю P(x), ніж k-розрядний допоміжний поліном псевдовипадкової гами у відомому способі (n>k). Можна також періодично змінювати вектор паролю P(x) для кожного кодового вектора C(x), як і у відомому способі змінюються допоміжні поліноми.

У відомому способі зменшується завадостійкість коду саме тому, що на боці приймача першою здійснюється операція декодування, внаслідок чого невиявлені декодером помилки спричиняють додаткові спотворення інформації під час дешифрування. У запропонованому способі такі ситуації неможливі і тому зберігається початкова завадостійкість кодування.

Розглянемо спосіб завадостійкого кодування дискретної інформації із захистом на прикладі циклічного (15,11)-коду з породжувальним поліномом

$g(x)=1+x+x^4=11001$.

Нехай задано 11-розрядний інформаційний вектор I(x)=11110001010. Виконаємо несистематичне кодування для отримання 15-розрядного кодового вектора C(x) згідно (1):

$C(x)=(11110001010)\times(11001)=100001101111010$.

Далі виберемо 15-розрядний вектор паролю P(x)=001101110001001, обчислимо 15-розрядний захищений кодовий вектор T(x) згідно (3):

$T(x)=(100001101111010)\oplus(001101110001001)=101100011110011$

Нехай після передачі даних отримано вектор $T_{ch}(x)=101100011110011$ і знайдемо кодовий вектор $C_{ch}(x)$ згідно (4):

$C_{ch}(x)=(101100011110011)\oplus(001101110001001)$ $=100001101111010$ Виконаємо декодування отриманого кодового вектора згідно (2):

$$I(x)=\frac{C_{ch}(x)}{g(x)}=\frac{100001101\mathbf{1}11010}{11001}=111100010\mathbf{1}0\cdot$$

Ми отримали також нульовий вектор остачі (R(x)=00000), що свідчить про відсутність помилок передачі.

Якщо виконати декодування вектора $T_{ch}(x)$, тоді буде отримано такий результат:

$$\frac{T_{ch}(x)}{g(x)}=\frac{101100011\mathbf{1}0011}{11001}=1101011100\cdot$$

Ми отримаємо також ненульовий вектор остачі (R(x)=01011), що не дасть змоги перевірити правильність передачі кодового вектора.

Комп'ютерна верстка М. Ломалова Підписне Тираж 26 прим.

Міністерство освіти і науки України

Державний департамент інтелектуальної власності, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

ДП "Український інститут промислової власності", вул. Глазунова, 1, м. Київ – 42, 01601