



УКРАЇНА

(19) **UA**

(11) **107657**

(13) **U**

(51) МПК

H03M 13/09 (2006.01)

H04K 1/06 (2006.01)

G09C 1/06 (2006.01)

ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **а 2015 08148**

(22) Дата подання заявки: **17.08.2015**

(24) Дата, з якої є чинними
права на корисну
модель: **24.06.2016**

(46) Публікація відомостей
про видачу патенту: **24.06.2016, Бюл.№ 12**

(72) Винахідник(и):

Рудницький Володимир Миколайович
(UA),

Фауре Еміль Віталійович (UA),

Швидкий Валерій Васильович (UA),

Щерба Анатолій Іванович (UA)

(73) Власник(и):

ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ

ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ,

бул. Шевченка, 460, м. Черкаси, 18006 (UA)

(54) СПОСІБ КОМБІНОВАНОГО КОДУВАННЯ ІНФОРМАЦІЇ

(57) Реферат:

Спосіб комбінованого кодування інформації включає виявлення факту модифікації інформації внаслідок впливу природних або штучних завад і використовує для цих цілей залежну від кожного символу інформаційної частини блока перевірну частину, яка вводиться в блок даних. Для підвищення стійкості до несанкціонованої модифікації інформації перевірна частина завадостійкого коду формується для образу інформаційної частини, параметри формування цього образу зберігаються в секреті і є ключем перетворення.

UA 107657 U

Корисна модель належить до техніки передавання даних каналами зв'язку і може бути використана для виявлення помилок, що виникають у каналі зв'язку під час передавання цих даних, захисту інформації від нав'язування хибних даних, а також захисту від навмисних спроб несанкціонованого читання. Це досягається шляхом доповнення переданого блока даних перевіркою частиною, що формується для образу інформаційної частини за деяким правилом (ключем), яке тримається в таємниці.

Відомі способи кодування інформації, що забезпечують виявлення факту модифікації переданих даних внаслідок навмисних дій злоумисника або впливу помилок у каналі зв'язку [1, 2, 3].

Зокрема, таким способом контролю є завадостійкий код умовних лишків, що використовує систему числення в лишкових класах [3]. Цей спосіб кодування найбільш близький за сукупністю ознак до способу, що заявляється. Спосіб-аналог включає:

- формування стійких до розкриття контрольних ознак на основі теорії лишкових класів;
- формування контрольної суми, яка ставиться у відповідність укрупненому символу

(складеному числу π , що складається з m символів даних) і записується в системі лишкових класів. Базис системи лишкових класів ω вибирають з умови $\omega = \prod_{i=1}^b \sigma_i$, де σ_i - набір основ, що утворюють базис перетворення.

Сформований блок даних, доповнений спеціальним символом-прапором, що позначає початок блока і служить для циклової синхронізації, виводиться в канал зв'язку.

Спільними ознаками способу кодування інформації, що заявляється, та способу-аналога є наступне:

- обидва способи використовують механізми формування контрольних ознак, стійких до несанкціонованої модифікації інформаційних об'єктів;
- блок даних, який передається каналом зв'язку, містить інформаційну та перевірку частини; перевірна частина обчислюється за сукупністю всіх символів інформаційної частини;
- ключ формування перевірки частини тримається в секреті і відомий відправнику і одержувачу.

Недоліком способу-аналога є невисока швидкість роботи алгоритму, що особливо проявляється під час збільшення довжини блока та кількості контрольних ознак, а також необхідність виконання обчислень у лишкових класах по модулю, відмінному від ступеня числа 2, що ускладнює роботу алгоритму.

В основу корисної моделі поставлена задача виявлення факту несанкціонованої модифікації інформації, виявлення внесених каналом зв'язку помилок, а також блокування несанкціонованого доступу до інформації за рахунок комбінації позитивних властивостей методів факторіального кодування і методів завадостійкого кодування. При цьому блокування несанкціонованого доступу до інформації і виявлення факту несанкціонованої модифікації інформації обумовлені властивостями факторіального кодування, а висока достовірність передавання - властивостями завадостійкого кодування.

Поставлена задача вирішується наступним:

- образ інформаційної частини блока даних формується у вигляді однієї перестановки порядку M (або відповідного їй синдрому) на основі прихованої залежності від кожного символу інформаційної частини блока даних; отримана перестановка (синдром) не підлягає передаванню приймачу;

- представлена в двійковому вигляді перестановка (або її синдром) кодується завадостійким кодом (наприклад, БЧХ-кодом шляхом ділення багаточлена, що відповідає образу інформаційної частини блока, на утворюючий поліном); отримана перевірна частина вводиться в блок даних;

- блок даних, що містить інформаційну частину (з m двійкових символів) і перевірку частину (з k двійкових символів (для БЧХ-коду k - порядок утворюючого код багаточлена)), доповнюється кодовою комбінацією "прапор" і передається приймачу.

Примітка. Під перестановкою мається на увазі послідовність з M чисел натурального ряду $0, 1, 2, \dots, (M-1)$, розташованих у деякому порядку. Загальне число можливих перестановок дорівнює $M!$, при цьому колона з цих перестановок може бути пронумерована числами відрізка $[0, M!-1]$.

Для формування перестановки використовується позиційна система числення з факторіальною основою, яка забезпечує взаємно однозначний зв'язок довільного числа $B(n)$,

що належить числовому відрізку $[0, M!-1]$ і визначає номер перестановки $P(n)$ у дискретний момент часу $n \geq 0$, з перестановкою $P(n)$. Номер $B(n)$ перестановки $P(n)$ у факторіальній системі числення записується наступним чином:

$$B(n) = \sum_{i=0}^{M-1} b_{M-1-i}(n) \cdot (M-1-i)!, \text{ де } i \in [0, M-1] - \text{номер факторіального коефіцієнта в}$$

запису числа $B(n)$, а $0 \leq b_i(n) \leq i$.

Послідовність символів $b_i(n)$ будемо називати синдромом $S(n)$ і записувати у вигляді $S(n) = b_{M-1}(n), b_{M-2}(n), \dots, b_0(n)$.

За синдромом $S(n)$ легко обчислюється перестановка $P(n)$. Закон перетворення синдрому в перестановку може бути відкритим і прихованим. У випадку прихованого перетворення таблиця перетворення тримається в секреті і є ключем перетворення. Зазначена послідовність дій може бути записана у вигляді: $B(n) \rightarrow S(n) \rightarrow P(n)$, причому ця послідовність може бути розділена на дві: $B(n) \rightarrow S(n)$ і $S(n) \rightarrow P(n)$.

Синдром перестановки обчислюється за інформаційною частиною шляхом послідовного аналізу всіх її символів. Таким чином, спосіб, що заявляється, передбачає виконання операції $S(n) \rightarrow P(n)$ та операції зчеплення синдромів $S(n) = g[S(n-1)]$, $n \in \overline{1, m}$ (це означає, що наступний синдром є деякою функцією від попереднього). За останнім синдромом блока $S(n=m)$, який пов'язаний з усіма попередніми, обчислюється перестановка $P(m)$. Ця перестановка записується у вигляді двійкової послідовності (наприклад, у вигляді коефіцієнтів багаточлена ступеня $M \cdot \lceil \log_{2M} \rceil$, де $\lceil A \rceil$ означає функцію "стеля" ("ceiling") від числа A).

Зчеплення синдромів (і, отже, всіх символів інформаційної частини блока) досягається операцією $S(n) = f[S(n-1) \oplus t_r(n)]$, де t_r - r -розрядний символ даних, \oplus - символ підсумовування двох доданків, представлених у різних системах числення. Вираз $f[S(n-1)]$ означає модифікацію попереднього синдрому перестановки - його зміщення на числовій осі на деяку, яка визначається ключем, величину.

Образом інформаційної частини блока, що використовується для формування його перевірної частини, може бути як останній синдром блока $S(n=m)$ (який зчеплений з усіма попередніми синдромами), так і перестановка $P(m)$, сформована за останнім синдромом (що відповідає операції $S(m) \rightarrow P(m)$). Цей образ записується у вигляді багаточлена над полем:

$GF(2^{m'}) : A(x) = a_{m'-1} \cdot x^{m'-1} + a_{m'-2} \cdot x^{m'-2} + \dots + a_1 \cdot x^1 + a_0 \cdot x^0$, де $m' = M \cdot \lceil \log_2(M) \rceil$ (у разі використання для формування перевірної частини безпосередньо синдрому перестановки $m' \leq M \cdot \lceil \log_2(M) \rceil$).

Значення M може вибиратися виходячи з вимог до імітостійкості. Далі представлені в двійковому вигляді перестановка або її синдром кодується завадостійким кодом.

Досягнутий технічний результат - виявлення факту модифікації інформації внаслідок впливу природних або штучних завад - обумовлений застосуванням завадостійкого кодування до образу (синдрому перестановки або самої перестановки), обчисленому за інформаційною частиною блока. При цьому ключ перетворення інформаційної частини в синдром (а також синдрому в перестановку) тримається в секреті, забезпечуючи статистичну незалежність перевірної частини блока від його інформаційної частини і роблячи неможливим несанкціоновану модифікацію будь-якого символу інформаційної частини блока.

Крім того, такий підхід виключає можливість отримання даних користувачем, який не має ключа формування перевірної частини блока. Це обумовлено тим, що приймач несанкціонованого споживача без знання секретного ключа не має можливості увійти в синхронізм з передавачем внаслідок того, що в системі з вирішальним зворотним зв'язком один і той же блок буде кілька разів перепитуватися без його виведення споживачеві, після чого сформується сигнал "аварія каналу"; у системі без зворотного зв'язку приймач, розмножуючи помилки внаслідок невірної декодування, також сформує сигнал "аварія каналу".

Зауважимо, що в природі не існує кодів, що виявляють усі можливі помилки. Спосіб кодування, що заявляється, не виявляє помилки, які виникають у випадку виконання наступних умов: помилка в блоці призвела до того, що перевірна послідовність, сформована приймачем з

інформаційної частини прийнятого з помилками блока, збіглася з перевіркою частиною цього блоку. Імовірність такої події порівнянна з імовірністю залишкової помилки декодування використовуваного завадостійкого коду.

Заявлений технічний результат від застосування цього способу контролю цілісності інформації досягається за допомогою пристрою, спрощена структурна схема якого (адаптована для реалізації на однокристальній ЕОМ) показана на кресленні.

Пристрій містить блок (1) обчислення синдрому $S(n)$ за заданим значенням $S(n-1)$ і $t(n)$ для $n \in \overline{1, m}$, блок (2) обчислення перестановки $P(m)$ за заданим $S(m)$, блок завадостійкого кодування (3), формувач блока даних (4), джерело інформації (формувач числа $t(n)$) (5) і пристрій керування (6). Зауважимо, що у разі формування перевіркою частини блока безпосередньо на основі синдрому перестановки в ланцюгу блоків (1)-(2)-(3)-(4) блок (2) є відсутнім.

У початковий момент часу з зовнішнього пристрою (наприклад, клавіатури ЕОМ) у блок (1) обчислення синдрому $S(n)$ завантажується послідовність $S(0)$ з M чисел, яка є вектором початкового завантаження і може бути частиною ключа. Одночасно в цей же блок (1) завантажується ключ модифікації попереднього синдрому перестановки. У той же час в блок (2) перетворення синдрому в перестановку завантажується ключ перетворення (синдрому в перестановку), а джерело інформації (5) видає перший символ блока даних - r -розрядне число $t_r(1)$, - який також завантажується в блок (1).

Блок обчислення синдрому (1) за заданим $S(0)$ і $t_r(1)$ обчислює значення першого синдрому $S(1) = f[S(0)] \oplus t_r(1)$. Усі наступні синдроми (до $S(n=m)$ включно) обчислюються як $S(n) = f[S(n-1)] \oplus t_r(n)$ у режимі прихованого перетворення. Після цього блок формування перестановки (2) обчислює перестановку $P(m)$. Завадостійкий кодер (3) за послідовністю $P(m)$ (або $S(m)$) обчислює перевірку частину блока. Формувач блока даних (4) об'єднує символи інформаційної та перевіркою частин у блок даних, додає символ-прапор і видає його в канал зв'язку.

Джерела інформації:

1. Пат. 75935 Україна, МПК H03M13/31 (2006.01). Спосіб забезпечення цілісності інформації на базі коду умовних лишків /Василенко В.С, Чунарьова А.В., Василенко М.Ю, Чунарьов А.В.; заявник та патентовласник Національний авіаційний університет. - № u2012103515; заявл. 26.03.2012; опубл. 25.12.2012, Бюл. № 24. - 4 с.

2. Пат. 75938 Україна, МПК H03M13/31 (2006.01). Спосіб забезпечення цілісності інформації на базі лишково-хеммінгового коду /Василенко В.С, Чунарьова А.В., Василенко М.Ю, Чунарьов А.В.; заявник та патентовласник Національний авіаційний університет. - № u2012103518; заявл. 26.03.2012; опубл. 25.12.2012, Бюл. № 24. - 4 с.

3. Пат. 67988 Україна, МПК H03M13/31 (2006.01). Спосіб забезпечення цілісності інформації на базі завадостійкого коду умовних лишків /Василенко М.Ю, Василенко В.С, Чунарьов А.В.; заявник та патентовласник Національний авіаційний університет. - № u201110207; заявл. 19.08.2011; опубл. 12.03.2012, Бюл. № 5. - 5 с.

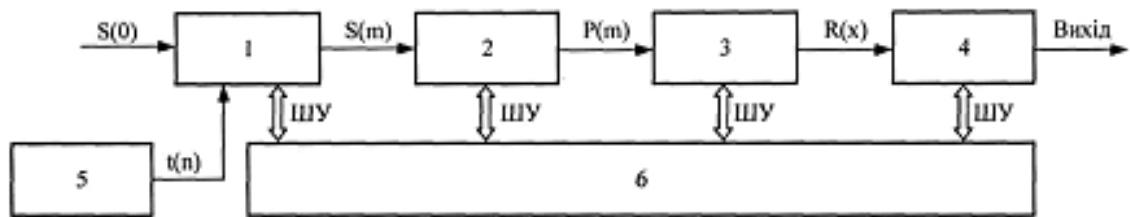
ФОРМУЛА КОРИСНОЇ МОДЕЛІ

1. Спосіб комбінованого кодування інформації, який включає виявлення факту модифікації інформації внаслідок впливу природних або штучних завад і використовує для цих цілей залежну від кожного символу інформаційної частини блока перевірку частину, яка вводиться в блок даних, який **відрізняється** тим, що для підвищення стійкості до несанкціонованої модифікації інформації перевірна частина завадостійкого коду формується для образу інформаційної частини, параметри формування цього образу зберігаються в секреті і є ключем перетворення.

2. Спосіб за п. 1, який **відрізняється** тим, що як образ інформаційної частини використовують синдром перестановки, який обчислюється шляхом перетворення символів інформаційної частини в послідовність взаємопов'язаних чисел у факторіальній системі числення.

3. Спосіб за п. 2, який **відрізняється** тим, що для додаткового підвищення стійкості до несанкціонованої модифікації інформації синдром перестановки перетворюється в перестановку і використовується як образ інформаційної частини для формування перевіркою

частини завадостійкого коду, ключ перетворення синдрому перестановки в перестановку зберігається в таємниці та є елементом ключа перетворення.



Комп'ютерна верстка О. Рябо

Державна служба інтелектуальної власності України, вул. Василя Липківського, 45, м. Київ, МСП, 03680, Україна

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