Корисна модель відноситься до техніки передавання інформації і може використовуватися в інформаційно-вимірювальних системах, комп'ютерних мережах та системах обміну інформацією.

Відомий спосіб передавання та приймання двійкових сигналів та пристрій для його реалізації [А. с. СРСР № 1164892, МКІ Н03М 13/00, бюлетень "Изобретения стран мира", 1985, № 18].

Спосіб полягає в тому, що під час передавання перед кожним імпульсом перетворюваної послідовності формують додатковий, полярність якого встановлюють у відповідності з кореляційним перетворенням полярності імпульсів початкової двійкової послідовності, а під час приймання перед порівнянням кожного сигналу, отриманого після стробування із завданим порогом, визначають його полярність і формують сигнал, що відповідає полярності даного сигналу, отриманого після стробування і сигнал передбачення полярності наступного сигналу, що отримується після стробування в наступний відліковий момент часу у відповідності з кореляційним перетворенням, що здійснюється під час передавання, який порівнюється з сигналом, що відповідає полярності наступного сигналу, отриманого після стробування, а при їх невідповідності збільшують завданий поріг.

Вказаний спосіб має той недолік, що він призначений лише для фіксації помилок, що виникають під час передавання, а не для їх виправлення.

Відомий також спосіб кодування та передавання інформації [А. с. СРСР № 1432788, МКІ НОЗМ 13/00, бюлетень "Открытия. Изобретения", 1988, № 39],

Спосіб вміщує в собі кодування інформаційної послідовності елементарних бінарних сигналів за допомогою частотної маніпуляції з неперервною фазою і наступне передавання модульованого сигналу каналом зв'язку. Завдяки передаванню кожних $n(n \geq 1)$, кодованих згортковим кодом елементарних двійкових сигналів інформаційної послідовності з некодованим елементарним двійковим сигналом цієї самої послідовності, після чого здійснюють частотну модуляцію з неперервною фазою. При цьому забезпечується підвищення швидкості передавання. Кодова відстань лишається незмінною.

Вказаний спосіб має той самий недолік, оскільки він теж призначений лише для фіксації помилок, що виникають під час передавання, а не для їх виправлення.

Найбільш близьким по технічній суті е спосіб кодування і передавання інформації із захистом та пристрій для його реалізації [Патент України на винахід № 23491 А, МКІ Н03М 13/00, бюлетень "Промислова власність", 1998, № 4].

Спосіб вміщує в собі моделювання послідовності елементарних двійкових сигналів і передавання їх каналом зв'язку у вигляді стандартного блока. На передавальному боці чисельними методами розраховуються коефіцієнти ряду Фур'є, отримані гармоніки по черзі відкидають, починаючи з кінця, до тих пір, поки похибка відновлення буде в межах 0,5, досягаючи мінімального складу ряду Фур'є, Отримані коефіцієнти розбивають на байти за правилами комп'ютерного адресування, перетворюють на послідовний код і передають до каналу зв'язку. На приймальному боці елементарні двійкові сигнали зчитують з каналу зв'язку, демодулюють, перетворюють на паралельний код по байтах, вводять до персонального комп'ютера, де за правилами комп'ютерного адресування з них формують коефіцієнти ряду Фур'є довжиною у стандартне машинне слово, розраховують значення функції для аргументу, що дорівнює 1, 2,... , n, де n - довжина стандартного блока інформації, а отримані значення округлюють до найближчого цілого числа.

Вказаний спосіб, як і попередні, розрахований на відновлення сигналу, що формується на передавальному пункті, із завданою похибкою. При цьому не враховуються завади, що діють у каналі зв'язку.

У відповідності із правилами побудови завадозахищених кодів, кодова відстань d визначає:

$$d \geq r + s + 1 \quad (1)$$

де r - кількість помилок, що виправляються;

s - кількість помилок, що виявляються.

Більшість завадозахищених кодів розрахована на виявлення чи виправлення однієї помилки. Причому перші є здебільшого вбудованими до засобів перетворення паралельного коду на послідовний (код з перевіркою на парність), а другі додатково реалізуються у пристроях обміну інформацією (циклічний, Хеммінга тощо). Але на практиці канали зв'язку здебільшого характеризуються наявністю помилок пакетного характеру.

Оскільки практично всі технічні засоби передавання інформації будуються зараз на базі мікропроцесорної техніки, то передавання інформації здійснюється в байтовому форматі (по вісім двійкових розрядів). Виходячи з цього, доцільно будувати такий формат коду, щоб загальна кількість його розрядів була кратною восьми, а кодова відстань була максимальною. При цьому код повинен бути нероздільним, тобто у посиланні неможливо було б визначити інформаційні та контрольні розряди, що надасть йому умови захищеності від несанкціонованого проникнення.

Перераховані заходи дозволять уникнути недоліків, які властиві прототипові.

Таким чином, суттєвий ефект може дати побудова завадозахищеного коду з ознаками додаткового захисту від несанкціонованого проникнення.

В основу корисної моделі покладена задача створення способу кодування інформації, при якому за рахунок введення нових операцій забезпечується захист від завад у лінії зв'язку за рахунок виправлення помилок і захист від несанкціонованого проникнення за рахунок нероздільності коду.

Вказана задача вирішується тим, що на передавальному боці формують кодові послідовності у відповідності із принципом формування коду, визначають таблицю відповідності інформаційних посилань кодовим послідовностям, дискретну інформацію зчитують з носія, розбивають за довжиною на інформаційні повідомлення, перетворюють на кодові послідовності у відповідності із визначеною таблицею, перетворюють на послідовний код і передають до каналу зв'язку. На приймальному боці сигнал приймають з каналу зв'язку, відновлюють імпульсну послідовність за амплітудою та тривалістю, ідентифікують кодову

комбінацію, у випадку необхідності виправляють помилки передавання, за допомогою таблиці відповідності кодові комбінації перетворюють на інформаційні повідомлення і записують на носій.

Суть способу полягає в тому, що за рахунок використання алгоритму побудови коду із максимальною кодовою відстанню для фіксованої кількості розрядів досягається його максимальна завадозахищеність (кількість помилок, що виправляють), а за рахунок операцій розбиття даних з носія на інформаційні повідомлення і побудови таблиці відповідності між інформаційними повідомленнями і кодовими послідовностями з повідомлення вилучається явна інформація, за рахунок чого йому надаються ознаки захищеності від несанкціонованого проникнення.

На кресленні наведена схема, що ілюструє принципи формування функцій Хаара.

Як видно з креслення функції Хаара природно мають кодову відстань, яка дорівнює 4. Виходячи з виразу (1), це означає, що їх використання без усяких додаткових заходів дозволяє не лише виявляти, але й виправляти помилки. Крім цього, вони реалізуються біполярним сигналом, що само собою виключає наявність постійної складової у канальному сигналі і, як наслідок, виключення між символьних завад першого та другого роду.

У відповідності із правилами побудови складається матриця Хаара, яка має вигляд (2).

$$H_8 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & -1 & -1 \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix} \quad (2)$$

$$H_8 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & -1 & -1 & -1 \\ 0 & 0 & -1 & -1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & -1 & -1 \\ 0 & -1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & -1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & -1 \end{bmatrix} \quad (3)$$

Об'єднавши ці дві матриці, можна отримати шістнадцять кодових комбінацій із кодовою відстанню d = 4. їм у відповідність можна поставити шістнадцять інформаційних кодових комбінацій, наприклад як це подано у таблиці 1. Таблиця відповідності може складатися випадково, що дозволяє досягти однозначності між інформаційними повідомленнями та кодовими комбінаціями лише для того, хто цю таблицю складав і для того сеансу обміну інформацією, де вона використовується. Кількість можливих варіантів перестановок комбінацій визначається формулою (4).

Таблиця

Приклад таблиці відповідності між кодовими комбінаціями та інформаційними повідомленнями

Інформаційне повідомлення	Кодова комбінація
0000	11111111
0001	1-1000000
0010	11110-111
ООН	111100-1-1
0100	11-1-10000
0101	1111-1-1-1-1
ОНО	0000-1-1-1-1
0111	110-11111
1000	000011-1-1
1001	10101010
1010	00-1-11111
1011	00000000
1100	1111110-1
1101	0-1111111
1110	001-10000
1111	0000001-1

$$N_k = k_k! \quad (4)$$

де k_k - кількість кодових комбінацій.

$$N_n = C_{8 \cdot N}^4 \quad (5)$$

де N - об'єм файла, що має передаватися, байт.

Складена таблиця визначає відповідність між п'ятьма двійковими інформаційними розрядами та кодовими комбінаціями. Виходячи з цього, зчитану з носія інформацію, що має передаватися, необхідно розбити на інформаційні повідомлення по чотири двійкових розрядів. Кількість можливих варіантів таких сполучень буде визначатися формулою (5).

Описаний спосіб вміщує дії у такій послідовності:

на передавальному боці:

- формування кодових комбінацій з використанням матриць;
- формування таблиці відповідності між інформаційними повідомленнями та кодовими комбінаціями;
- зчитування дискретної інформації;
- перетворення інформації на кодові комбінації;
- побітове передавання кодових комбінацій до каналу зв'язку;

на приймальному боці:

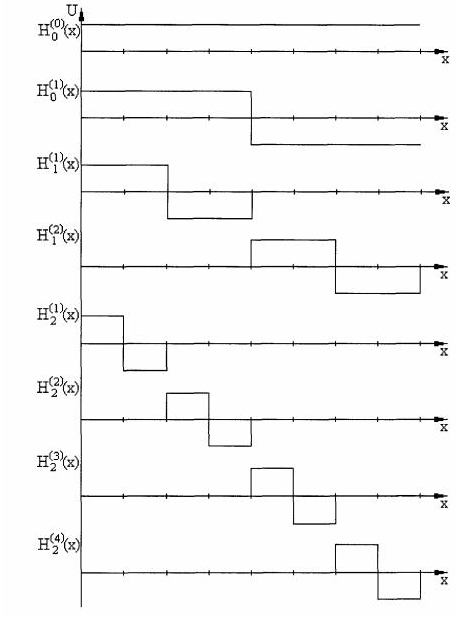
- побітове приймання кодових комбінацій з каналу;
- виправлення помилок у випадку необхідності шляхом підбирання найбільш близької кодової комбінації;
- перетворення кодових комбінацій на інформаційні повідомлення;
- формування вихідного файла і записування його на носій.

Оскільки для передавання інформації використано код із кодовою відстанню 4, то він може виправляти одну помилку у кожній кодовій комбінації. Отже завадозахищеність обміну інформацією підвищується.

Крім цього формування таблиць відповідності і перекодування інформації, що передається сприяє її захищеності від несанкціонованого доступу. Повна кількість можливих варіантів перекодування складає:

$$N_\Sigma = N_k \cdot N_n = k_k! \cdot C_{8 \cdot N}^4 = \frac{k_k! \cdot (8 \cdot N)!}{4! \cdot (8 \cdot N - 4)!} \quad (6)$$

Навіть передавання 100 байт інформації за цим принципом для дешифрування вимагає перебору 10^{47} можливих варіантів, що показує досить високу криптостій-кість даного способу.



Фіг. 1