Винахід 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 [Авторське свідоцтво СРСР №1164892, МКІ Н03М13/00, бюлетень "Изобретения стран мира" №18, 1985].

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.

Відомий також спосіб кодування та передавання інформації [Авторське свідоцтво СРСР №1432788, МКІ Н03М13/00, бюлетень "Открытия. Изобретения" №39, 1988].

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 загортковим 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.

Вказані способи мають той недолік, що не використовують стискання інформації і не забезпечують її захист від несанкціонованого використання.

Найбільш близьким по технічній суті є спосіб кодування і передавання інформації із захистом та пристрій для його реалізації [Патент України на винахід №23491 А, МПК6 Н03М13/00, бюлетень "Промислова власність" №4, 1998].

Спосіб вміщує в собі моделювання послідовності елементарних двійкових сигналів і передавання їх каналом зв'язку у вигляді стандартного блока даних. На передавальному боці числовими методами розраховуються коефіцієнти ряду Фур'є, отримані гармоніки по черзі відкидають, починаючи з кінця, до тих пір, поки похибка відновлення не 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 розрахований на відновлення сигналу, що формується на передавальному пункті, із завданою похибкою. При цьому не враховуються особливості передавання.

Головним недоліком вказаного способу є те, що для апроксимації прямокутних сигналів використовуються синусоподібні коливання, що в окремих випадках збільшує похибку відновлення і кількість складових, тобто обсяг даних, що передаються. При цьому збільшується завантаженість каналу зв'язку і час передавання.

В основу винаходу покладено задачу створення способу кодування та передачі інформації, в якому за рахунок введення нових операцій забезпечується мінімізація інформації, що передається, знижується час, який витрачається на передавання інформації, і підвищується ефективність використання каналу.

Задача вирішується наступним чином: на передавальному боці дискретна інформація зчитується з носія у вигляді стандартного блока, довжина якого встановлюється в діалоговому режимі. Числовими методами розраховуються поліноми Лежандра. Після чого здійснюють апроксимацію цього блока в базисі поліномів Лежандра, які описують дану послідовність дискретних значень (байт). Отримані номери поліномів за допомогою модему передаються до каналу зв'язку. На приймальному боці отримують передані номери поліномів Лежандра, відновлюють базис поліномів і за допомогою зворотного перетворення відновлюють інформацію.

Функції Лежандра $P_n(x)$ визначаються диференціальним рівнянням:

$$P_n(x) = \frac{1}{2^n \cdot n!} \cdot \frac{d_n}{dx^n}\left(\left(x^2 - 1\right)^n\right) \quad (1)$$

і являють собою поліноми степені n із коефіцієнтом $\frac{(2n)!}{2_n \cdot n!}$, при членах старшої степені.

В описуваному вище випадку апроксимація всіх неперервних та дискретних сигналів здійснюється в класичному базисі синусоїдних функцій. Для пропонованого випадку використовуються поліноміальні ортогональні функції Лежандра, тому для певного класу функцій сходимість ряду буде значно вищою, ніж в першому випадку [Бронштейн И.Н., Семендяев К.А. Справочник по математике для инженеров и студентов ВТУЗов. - М: Наука, 1980. – С. 885].

Розв'язок рівняння (1) дозволяє отримати ряд ортогональних функцій, обмежених інтервалом $x \in [-1,1]$ і описуваних виразами (2).

$P_0(x) = 1$,

$P_1(x) = x$,

$$P_2(x) = \frac{1}{2}\left(3x^2 - 1\right),$$

$$P_3(x) = \frac{1}{2}\left(5x^3 - 3x\right),$$

$$P_4(x) = \frac{1}{8}\left(35x^4 - 30x^2 + 3\right),$$

$$P_5(x) = \frac{1}{8}\left(63x^5 - 70x^3 + 15x\right),$$

$$P_6(x) = \frac{1}{16}\left(231x^6 - 315x^4 + 105x^2 - 5\right),$$

$$P_7(x) = \frac{1}{16}\left(429x^7 - 693x^5 + 315x^3 - 35x\right),$$

Краща сходимість ряду означає, що для апроксимації вихідної послідовності необхідно значно менше членів рівняння і кінцевий обсяг даних буде меншим без втрат інформації. При цьому алгоритм оброблювання даних спрощується, тобто до каналу зв'язку необхідно передавати меншу кількість даних, за рахунок чого скорочується час передавання і підвищується ефективність використання каналу. Крім цього, оскільки до каналу зв'язку передається не сама інформація, а номери функцій Лежандра, то без знання умов перетворення відновити інформацію неможливо, то функція захисту конфіденційної інформації зберігається повністю.

Відомий пристрій для приймання дискретних сигналів з кореляційним кодуванням по рівню [Авторське свідоцтво СРСР № 1164892, МКІ H03M13/00, бюлетень "Изобретения стран мира" №18, 1985], який вміщує в себе блок кодування і формувач сигналів на передавальному боці, а також формувач вхідного сигналу, блок вирішення, регістр зсуву, блок передбачення знаку, блок порівняння, елемент спів падання та інвертор.

Відомий також пристрій для реєстрації способу кодування і передавання інформації [Авторське свідоцтво СРСР №1432788, МКІ H03M13/00, бюлетень "Открытия. Изобретения" №39, 1988], який вміщує в собі комутатори, блок загорткового кодування, блок модуляції та канал зв'язку.

Недоліком даних пристроїв є те, що вони займають дуже широку смугу частот для організації обміну інформацією. Крім того, інформація, що передається не є захищеною.

Найбільш близьким за технічною суттю є пристрій для реалізації способу кодування і передавання інформації із захистом [Патент України на винахід №23491А, МПК6 H03M13/00, бюлетень "Промислова власність" №4, 1998], який вміщує персональний комп'ютер у складі центрального процесора, оперативного запам'ятовувального пристрою, монітора, клавіатури та носія інформації, арифметичного співпроцесора, друкувального пристрою та системного каналу, канал передавання інформації, модем, програмований контролер переривань та послідовний порт, причому модем зв'язаний з каналом передавання інформації, по двонаправленій шині зв'язаний з інформаційним каналом послідовного порту, виходи запитів переривань якого підключені до входів програмованого контролера переривань, а за допомогою системного каналу центральний процесор зв'язаний з арифметичним співпроцесором, постійним та оперативним запам'ятовувальними пристроями, монітором, клавіатурою, друкувальним пристроєм та носієм інформації.

Недоліком цього пристрою є те, що для апроксимації сигналів використовуються лише синусоподібні коливання, що не завжди є оптимальним, за рахунок чого збільшується кількість складових, тобто обсяг даних, що передаються. При цьому збільшується завантаженість каналу зв'язку і час передавання.

В основу винаходу поставлена задача створення пристрою кодування та передавання інформації, в якому за рахунок введення нових блоків та зв'язків зменшується надлишковість інформації, що передається, та підвищується швидкість передавання. Це відбувається за рахунок розділення в часі процесів кодування і передавання інформації, а також змінення принципу кодування. З цією метою до складу пристрою вводиться персональний комп'ютер. За рахунок об'єднання модулятора і демодулятора в єдиний блок (модем) та використання одних і тих самих технічних засобів як для передавання, так і для приймання інформації, виконується розширення функціональних можливостей. Крім того, інформація змінює вигляд, тобто відрізняється від початкового вигляду і у випадку несанкціонованого зчитування з каналу зв'язку не може бути відновлена без знання алгоритму отримання істинних значень, тобто зберігається її конфіденційність, а пристрій виконує функцію захисту.

Поставлена задача досягається тим, що до пристрою, який вміщує канал зв'язку, модулятор і демодулятор, об'єднані під назвою "модем", персональний комп'ютер, який вміщує в собі центральний процесор, оперативний запам'ятовувальний пристрій, монітор, системний канал, клавіатуру та носій інформації додатково введений постійний запам'ятовувальний пристрій, послідовний інтерфейс і нові зв'язки.

На Фіг.1 представлена схема, яка реалізує спосіб кодування та передавання інформації; на Фіг.2 - схема програмного забезпечення для режиму передавання інформації; на Фіг.3 - схема програмного забезпечення для режиму приймання інформації.

Пристрій для кодування та приймання-передавання дискретної інформації із захистом вміщує канал зв'язку 1, зв'язаний з модемом 2, персональний комп'ютер 3, до складу якого входять носій інформації 4, клавіатура 5, системний канал 6, послідовний інтерфейс 7, двонаправлений інформаційний канал якого зв'язаний з двонаправленим каналом модему 2, центральний процесор 8, оперативний запам'ятовувальний пристрій 9, постійний запам'ятовувальний пристрій 10 та монітор 11, причому за допомогою системного каналу 6 центральний процесор 8 зв'язаний з блоками, які входять до складу персонального комп'ютера 3.

Спосіб полягає в наступному.

На передавальному боці дискретну інформацію зчитують з носія інформації 4 у розмірі стандартного блока, числовими методами розраховують функції Лежандра, після чого програмним шляхом здійснюється апроксимація і підбираються відповідні номери поліномів. Отримані номери функцій Лежандра передають до каналу зв'язку за допомогою модему, на приймальному боці отримують відповідні номери поліномів, за якими відновлюють самі функції і за допомогою звичайного зворотного перетворення відновлюють початкову інформацію.

Описаний спосіб включає дії в такій послідовності:

На передавальному боці:

зчитування масиву дискретної інформації у розмірі стандартного блока з носія 4;

розрахунок поліномів Лежандра за допомогою персонального комп'ютера 3;

отримання номерів функцій Лежандра в результаті апроксимації початкового повідомлення за допомогою персонального комп'ютера 3;

передавання каналом зв'язку 1 розміру блока та номерів поліномів Лежандра.

На приймальному боці:

приймання з каналу зв'язку 1 розміру блока;

приймання номерів функцій Лежандра та відновлення самих функцій за допомогою персонального комп'ютера 3;

зворотне перетворення поліномів Лежандра та відновлення інформації за допомогою персонального комп'ютера 3;

зберігання отриманих даних на носію інформації 4.

Пристрій працює у відповідності з наведеним алгоритмом. При увімкненні живлення центральний процесор 8 виводить на монітор 11 повідомлення про початковий розмір стандартного блока інформації і очікує повідомлення, введеного з клавіатури 5 персонального комп'ютера 3. Після цього центральний процесор 8 виконує зчитування даних з носія інформації 4 у розмірі стандартного блока даних у оперативний запам'ятовувальний пристрій 9.

Після цього центральний процесор 8 виконує розрахунок поліномів Лежандра, апроксимацію початкової функції і визначення номерів функцій Лежандра, які відповідають даній інформації. Далі визначається найменша комбінація функцій Лежандра, яка дозволить швидко відновити інформацію із завданою похибкою. Оскільки початкові значення являють собою байти (цілі значення в діапазоні 0...255), то похибка результату округлення не повинна перевищувати 0,5, що і є максимальною похибкою зворотного перетворення для кожного випадку.

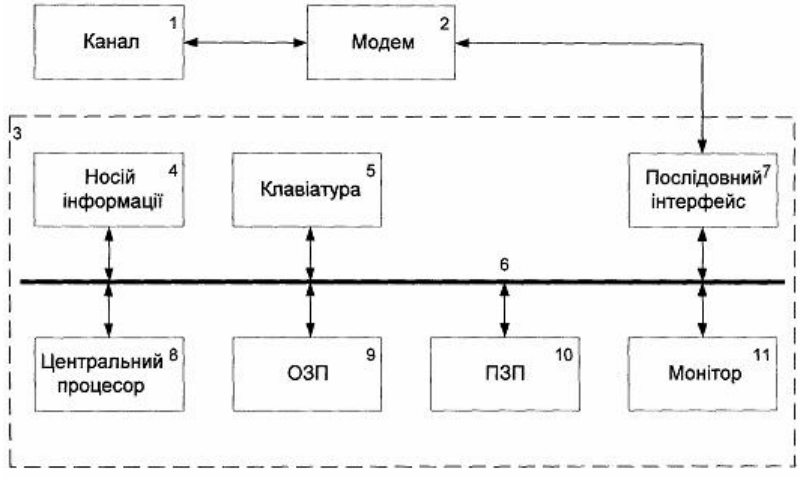
Передавання розміру блока і номерів функцій Лежандра відбувається з допомогою послідовного інтерфейсу 7 і модему 2. Центральний процесор 8 пересилає байт інформації в послідовний порт 7, який перетворює його на послідовний код і по бітах передає до модему 2. Програмним шляхом здійснюється опитування регістра прапорців доки не буде встановлений прапорець кінця передавання байту, що свідчить про те, що байт даних перетворений на послідовний код і переданий до каналу зв'язку. Після цього може передаватися наступний байт. Процес повторюється до тих пір, поки вся інформація, що міститься на носії інформації 4, не буде оброблена і передана до каналу зв'язку.

В режимі приймання інформації послідовний код, що поступає з каналу 1 через модем 2 демодулюється, після чого центральний процесор 8 зчитує передані байти і розташовує їх у відповідних місцях оперативного запам'ятовувального пристрою 9. Процес відбувається до тих пір, поки вся інформація не буде прийнята і розміщена у відповідних місцях оперативного запам'ятовувального пристрою 9. Після цього центральний процесор 8 виконує розрахунок функцій Лежандра та виконує їх зворотне перетворення, тобто відновлює початковий вигляд інформації, яка записується на носій інформації 4. Одночасно з цим вона може бути виведена на монітор 11.

Оскільки до каналу зв'язку надходить не сам файл, а лише номери функцій ряду Лежандра, якими цей файл апроксимується, то обсяг даних, що передаються, є значно меншим від початкового.

За рахунок того, що до каналу зв'язку передається не сама інформація, а номери апроксимуючої функції, без знання вигляду та всіх параметрів якої відновити інформацію не можливо, то виконується і функція захисту конфіденційної інформації.

Даний спосіб та пристрій доцільно виконувати на базі персонального комп'ютера IBM-PC, модеми випускаються серійно.



Фіг. 1


Початок
Ініціалізація
Встановлення розміру блоку
2
Зчитування блоку даних з носія
Розрахунок поліномів Лежандра
Апроксимація блоку даних
Визначення мінімальної комбінації поліномів
Перетворення їх номерів на байти
Передавання байта номера
Байт переданий?
0
1
Всі байти передані?
0
1
1
Збільшення вказівника номера
Всі номери передані?
0
1
1
Всі дані передані?
0
2
1
Кінець

Фіг. 2


Початок
Ініціалізація
Встановлення розміру блоку
Зчитування блоку даних з носія
Розрахунок поліномів Лежандра
Зворотне перетворення даних
Всі дані прийняті?
0
1
Кінець

Фіг. 3