

Винахід відноситься до техніки передавання інформації і може використовуватися в інформаційно-вимірвальних 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", 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.

Відомий також спосіб кодування та передавання інформації (Авторське свідоцтво СРСР №1432788, МКІ Н03М13/00, 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 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, МПКБ Н03М13/00, бюлетень "Промислова власність", 1998, №4).

Спосіб вміщує в собі моделювання послідовності елементарних двійкових сигналів і передавання їх каналом зв'язку у вигляді стандартного блока даних. На передавальному боці чисельними 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 синусоїдні коливання, що збільшує похибку відновлення і кількість складових, тобто обсяг даних, що передаються. При цьому збільшується завантаженість каналу зв'язку і час передавання даних.

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, чисельними методами розраховуються функції Хаара. Після цього здійснюють спектральний аналіз в базисі функцій Хаара, які апроксимують дану послідовність дискретних значень (байтів). Визначені номери функцій Хаара за допомогою модему передаються до каналу зв'язку. На приймальному боці отримують передані номери функцій Хаара, відновлюють функції Хаара і з допомогою зворотного перетворення відновлюють інформацію.

Функція Хаара $H_1^n(\theta)$ визначається рівнянням:

$$H_1^n(\theta) = \begin{cases} 2^{1/2}, & \frac{n-1}{2^l} \leq \theta < \frac{n-1/2}{2^l} \\ -2^{1/2}, & \frac{n-1/2}{2^l} \leq \theta < \frac{n}{2^l} \\ 0, & \text{інші } \theta \end{cases} \quad (1)$$

де $0 \leq l < \log_2 N$;

N - кількість формованих функцій;

$1 \leq n \leq 2^l$.

При розкладанні функції $\Phi(x)$ в ряд Хаара коефіцієнти при членах визначаються у відповідності з формулою:

$$C_1^{(n)} = 2^{-\log_2 N+1} \cdot \sum_{x=0}^{N-1} \varphi(x) \cdot H_1^{(n)}(x) \quad (2)$$

Оскільки для апроксимації прямокутних сигналів в даному випадку використовуються не синусоїдні функції, а прямокутні ортогональні, то сходиність ряду буде значно вищою, ніж в першому випадку (Залманзон Л.А. Преобразования Фурье, Уол-ша, Хаара и их применение в управлении, связи и других областях. - М.: Наука, 1989. -496с.). Це 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 Хаара, 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 Н03М13/00, бюлетень "Изобретения стран мира", 1985, №18), який вміщує в себе блок кодування і формувач сигналів на передавальному боці, а також формувач вхідного сигналу, блок вирішення, реєстр 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 Н03М13/00, бюлетень "Открытие. Изобретения", 1988, №39), 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 № 23491 А, МПК6 Н03М 13/00, бюлетень "Промислова власність", 1998, № 4), 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 прямокутних сигналів використовуються синусоїдні коливання, що за рахунок ефекту Гіббса збільшує похибку відновлення і 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 зміни принципу кодування. З цієї метою зі складу персонального комп'ютера виводяться зайві блоки (арифметичний співпроцесор, монітор, клавіатура та принтер), а вводиться постійний запам'ятовувальний пристрій. 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", програмований контролер переривань, послідовний інтерфейс, персональний комп'ютер у складі центрального процесора, оперативного запам'ятовувального пристрою, системного каналу та носія інформації додатково введений постійний запам'ятовувальний пристрій, що вводиться до складу персонального комп'ютера із новими зв'язками.

На фіг.1 подана 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, послідовний інтерфейс 3, двонаправленою шиною приймання-передавання даних RxD та TxD підключений до модему 2, а виходами формування сигналів переривання INT - до відповідних входів програмованого контролера переривань 4, персональний комп'ютер 5, за допомогою системного каналу 6 якого, центральний процесор 7 зв'язаний з оперативним запам'ятовувальним 8, постійним запам'ятовувальним 9 пристроями та носієм інформації 10, що входять до складу персонального комп'ютера 5, а також послідовним інтерфейсом 3 і програмованим контролером переривань 4.

Спосіб полягає в наступному.

На передавальному боці дискретну інформацію зчитують з носія інформації 10 персонального комп'ютера 5 в розмірі стандартного блока, чисельними методами розраховують функції Хаара, після чого програмним шляхом здійснюють апроксимацію початкових даних в базисі вказаних функцій. Після цього отримані номери функцій Хаара передають до каналу зв'язку 1 через послідовний інтерфейс 3 за допомогою модему 2, на приймальному боці з каналу зв'язку 1 за допомогою модему 2 через послідовний інтерфейс 3 отримують відповідні номери функцій Хаара, відновлюють самі функції Хаара і з допомогою 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 інформації 10 персонального комп'ютера 5;
- розрахунок функцій Хаара за допомогою персонального комп'ютера 5;
- отримання номерів функцій Хаара при апроксимації початкового повідомлення за допомогою персонального комп'ютера 5;
- передавання каналом зв'язку 1 за допомогою модему 2 та послідовного інтерфейсу 3 розміру блока та номерів функцій Хаара. На приймальному боці:
 - приймання з каналу зв'язку 1 за допомогою модему 2 та послідовного інтерфейсу 3 розміру блока;
 - приймання номерів функцій Хаара та відновлення самих функцій Хаара за допомогою персонального комп'ютера 5;
 - зворотне перетворення функцій Хаара та відновлення інформації за допомогою персонального комп'ютера 5;
- зберігання отриманих даних на носій інформації 10 персонального комп'ютера 5.

Пристрій працює у відповідності з наведеним алгоритмом.

При увімкненні живлення центральний процесор 7 персонального комп'ютера 5 здійснює ініціалізацію пристроїв і, у відповідності з повідомленням про початковий розмір стандартного блока інформації, виконує зчитування даних з носія інформації 10 в розмірі стандартного блока даних до оперативного запам'ятовувального пристрою 8.

Після цього центральний процесор 7 виконує розрахунок функцій Хаара, здійснює апроксимацію початкової інформації. Далі визначається найменша комбінація функцій Хаара, яка дозволить швидко відновити інформацію.

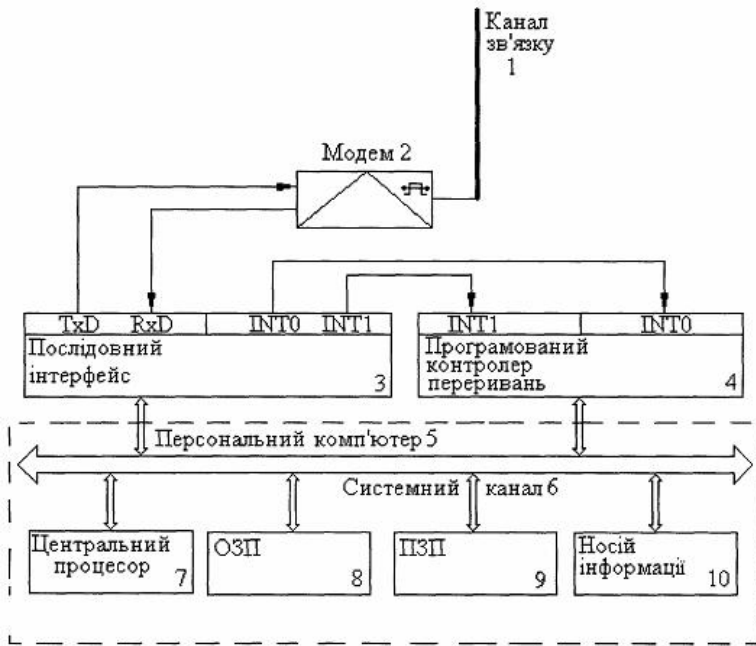
Передавання розміру блока і номерів функцій Хаара до каналу зв'язку 1 здійснюється за допомогою послідовного інтерфейсу 3 і модему 2. Центральний процесор 7 пересилає байт інформації до послідовного інтерфейсу 3, який перетворює його на послідовний код і по бітах передає в модем 2. Передача кожного байту інформації по шині TxD супроводжується формуванням сигналу переривання INT0. За допомогою програмованого контролера переривань 4, на вхід якого попадає цей сигнал, центральний процесор 7 персонального комп'ютера 6 синхронізує передавання байтів до послідовного інтерфейсу 3, уникаючи постійного відслідковування програмним шляхом завершення циклу передавання байта. Процес повторюється до тих пір, поки вся інформація, що міститься на носії інформації 10, не буде оброблена і передана до каналу зв'язку.

В режимі приймання інформації послідовний код, що поступає з каналу 1 через модем 2 демодулюється і поступає шину приймання RxD послідовного інтерфейсу 3. Перетворення паралельним інтерфейсом 3 кожного байту даних на паралельний код супроводжується сигналом переривання INT1, який поступає на відповідний вхід програмованого контролера переривань 4. Згідно з цим сигналом центральний процесор 7 зчитує спочатку розмір переданого блоку, а потім передані байти і розміщує їх у відповідних місцях оперативного запам'ятовувального пристрою 8. Процес відбувається до тих пір, поки вся інформація не буде прийнята і розміщена на відповідних місцях оперативного запам'ятовувального пристрою 8. Після цього центральний процесор 7 виконує розрахунок функцій Хаара та виконує їх зворотне перетворення, тобто відновлює початковий вигляд інформації, яка записується на носій інформації 10 персонального комп'ютера 5. Формування сигналів переривання за допомогою програмованого контролера 4 дозволяє вивільнити центральний процесор 7 від постійного контролю надходження байта з каналу зв'язку 1 на вхід RxD послідовного інтерфейсу 3 і використати його для операцій відновлення інформації.

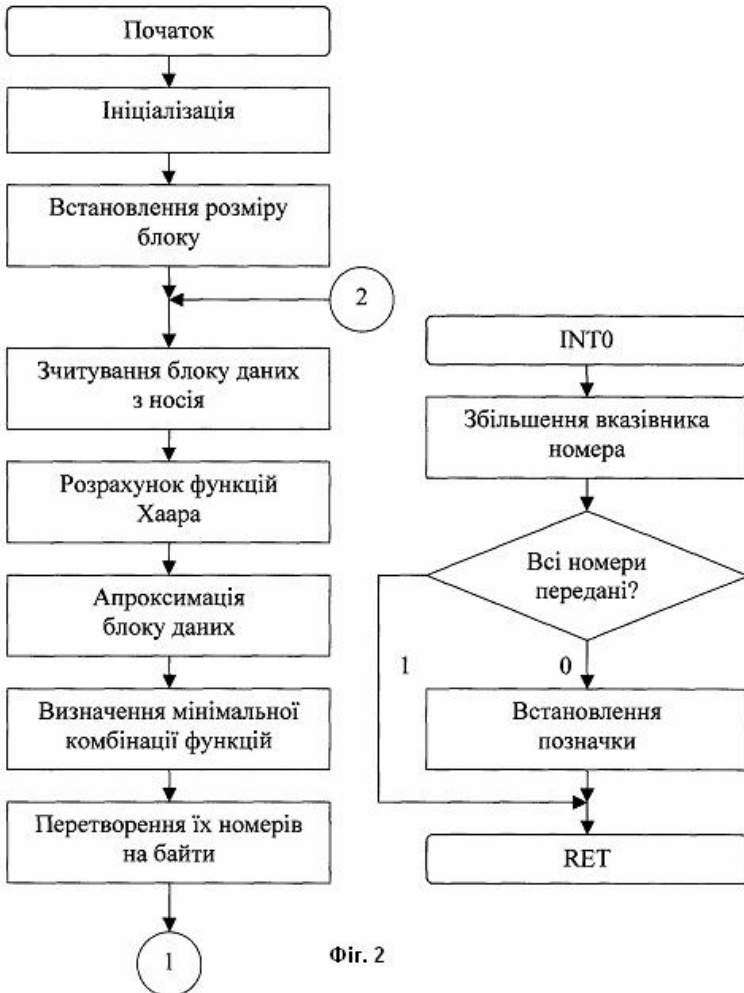
Оскільки до каналу зв'язку надходить не сам файл, а лише номери функцій ряду Хаара, якими цей файл апроксимується, то обсяг даних, що передаються, є значно меншим від початкового.

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

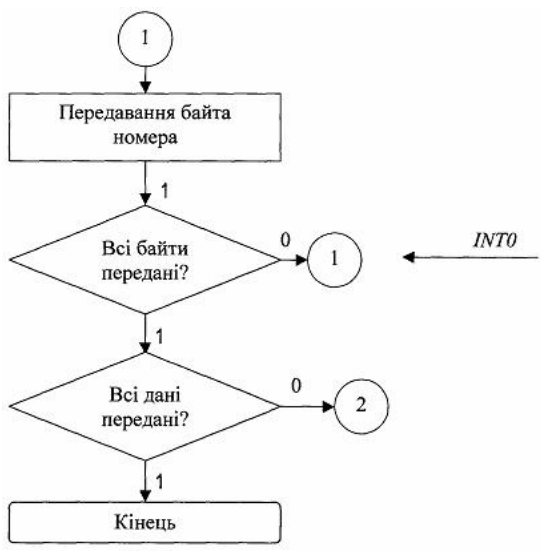
Даний спосіб та пристрій доцільно виконувати на базі персонального комп'ютера IBM-PC, модеми випускаються серійно.



Фіг. 1



Фіг. 2



Фіг. 2



Фіг. 3



Фіг. 3