

Винахід стосується криптографії, зокрема засекречування конфіденційної візуальної інформації від несанкціонованого доступу.

Відомий спосіб засекречування візуальної інформації, у якому кодування (засекречування) реалізується шляхом використання шумового зображення, сформованого генератором випадкових функцій, яке служить ключем для декодування зображення на приймальній стороні [1].

Однак цей спосіб має низький рівень надійності засекречування, низьку стійкість засекречування щодо впливу завад та має лише один засіб захисту від розсекречування.

Відомий також спосіб засекречування візуальної інформації, в якому кодування реалізується за допомогою трансформаційних перетворень зображення на основі унітарних математичних перетворень [2].

Цей спосіб має вищий рівень надійності захисту, оскільки в ньому використано перетворення зображень в їх спектральні образи. Проте і в цьому випадку обмежена кількість спектральних перетворень обумовлює низьку захищеність інформації щодо розсекречування. Шумові похибки в каналі зв'язку помітно знижують якість відтворюваного зображення.

Найбільш близьким до запропонованого винаходу і вибраним за прототип є спосіб кодування зображень на основі перетворень, де зображення піддається унітарному математичному перетворенню (перетворення Фур'є), а отримані коефіцієнти перетворення кодуються шляхом додавання маски-ключа, яка має випадкову фазову характеристику [3].

Однак і цей спосіб має недоліки. При використанні запропонованих квазіперіодичних фазових масок існує можливість несанкціонованого розсекречування зображення методами послідовного перебору можливих комбінацій. Спосіб має порівняно низьку завадостійкість до шумових завад та збоїв у каналі зв'язку, яка проявляється в додатковому розмитті відтворюваного зображення.

В основу винаходу поставлено завдання підвищити надійність та завадостійкість засекречування візуальної інформації, вводячи додаткове кодування амплітудної характеристики зображення, що також знизить ймовірність несанкціонованого розсекречування візуальної інформації та усуне загрозу зниження якості зображення при наявності комунікаційних завад.

Поставлене завдання вирішується тим, що в способі засекречування візуальної інформації, який включає оцифровування зображення, пряме Фур'є-перетворення, зміну фаз складових отриманого спектру за допомогою ключа-перетворювача та обернене перетворення Фур'є на передавальній стороні, а також зворотні вказаним перетворення на приймальній стороні згідно з винаходом ключ-перетворювач фаз складових спектру реалізують у вигляді фазових складових спектру, отриманого з зображення, сформованого випадковою шумовою функцією, вводять на передавальній стороні ключ-перетворювач амплітудних складових спектру і відповідний йому ключ-перетворювач амплітудних складових спектру на приймальній стороні, який реалізують у вигляді фільтра з певною амплітудно-частотною характеристикою.

Реалізація ключа-перетворювача фаз із використанням зображення, сформованого саме випадковою шумовою функцією, фактично повністю виключає можливість підбору ключа. Використання ключа-перетворювача амплітудних складових спектру додатково зменшує ймовірність розсекречування інформації і у зв'язку зі згладженням даних на приймальній стороні зменшує помітність комунікаційних завад, які можуть виникати у каналі зв'язку.

На фігурах зображено функціональну схему реалізації способу, на фіг. 1 - схема засекречування; на фіг. 2 - схема розсекречування.

Схема засекречування складається з блоку оцифровування зображення 1, блоку прямого перетворення Фур'є 2, блоку встановлення початкового стану 3, блоку генерування випадкового поля 4, блоку прямого перетворення Фур'є 5, блоку зберігання амплітудної характеристики фільтра-ключа 6, блоку оберненого перетворення Фур'є 9, блоку додавання 7 та блоку множення 8 (фіг. 1). Вихід блоку оцифровування зображення 1 під'єднаний до блоку прямого перетворення Фур'є 2, де вихід "ФАЗА" якого, під'єднаний до блоку додавання 7, а вихід "МОДУЛЬ" - до блоку множення 8, куди відповідно під'єднані вихід "ФАЗА" блоку прямого перетворення Фур'є 5 та блок зберігання амплітудної характеристики ключа 6. Вихід блоку встановлення початкового стану 3 під'єднаний до блоку генерування випадкового поля 4, який під'єднаний до блоку прямого перетворення Фур'є 5. Виходи блоку додавання 7 і блоку множення 8 під'єднані до блоку оберненого перетворення Фур'є 9, який є вихідним блоком схеми засекречування.

Блок оцифровування зображення 1 призначений для перетворення зображення з аналогової форми або носія візуальної інформації у цифрову форму. Блок прямого перетворення Фур'є 2 призначений для формування фази і модуля зображення, яке підлягає засекречуванню. Блок встановлення початкового стану 3 призначений для встановлення початкового стану генератора випадкового двомірного поля за допомогою відповідного ключа, що задається користувачем. Блок генерування випадкового поля 4 призначений для генерування випадкового двомірного поля. Блок прямого перетворення Фур'є 5 призначений для формування випадкової шумової функції, тобто випадкової фазової складової спектру на основі згенерованого випадкового поля. Блок зберігання амплітудної характеристики 6 призначений для зберігання апріорно заданих характеристик фільтра-ключа з певною смуговою амплітудною характеристикою в області середніх частот. Блоки 7 і 8 виконують операції додавання і множення. Блок оберненого перетворення Фур'є 9 призначений для формування вихідного зображення з заданих відліків модуля і фази.

Схема розсекречування складається з блоку прямого перетворення Фур'є 10, блоку встановлення початкового стану 11, блоку генерування випадкового поля 12, блоку прямого перетворення Фур'є 13, блоку зберігання амплітудної характеристики фільтра-ключа 14, блоку додавання 15, блоку множення 16, блоку оберненого перетворення Фур'є 17 та блоку цифро-аналогового перетворення 18 (фіг. 2). Вихід блоку прямого перетворення Фур'є 10 під'єднаний виходом "ФАЗА" до блоку додавання 15, а виходом "МОДУЛЬ" - до

блоку множення 16, куди відповідно під'єднані вихід "ФАЗА" блоку прямого перетворення Фур'є 13 та блок зберігання амплітудної характеристики ключа 14. Вихід блоку встановлення початкового стану 11 під'єднаний до блоку генерування випадкового поля 12, який під'єднаний до блоку прямого перетворення Фур'є 13. Виходи блоку додавання 15 і блоку множення 16 під'єднані до блоку оберненого перетворення Фур'є 17, вихід якого під'єднаний до блоку цифро-аналогового перетворення 18, який є вихідним, блоком схеми розсекречування.

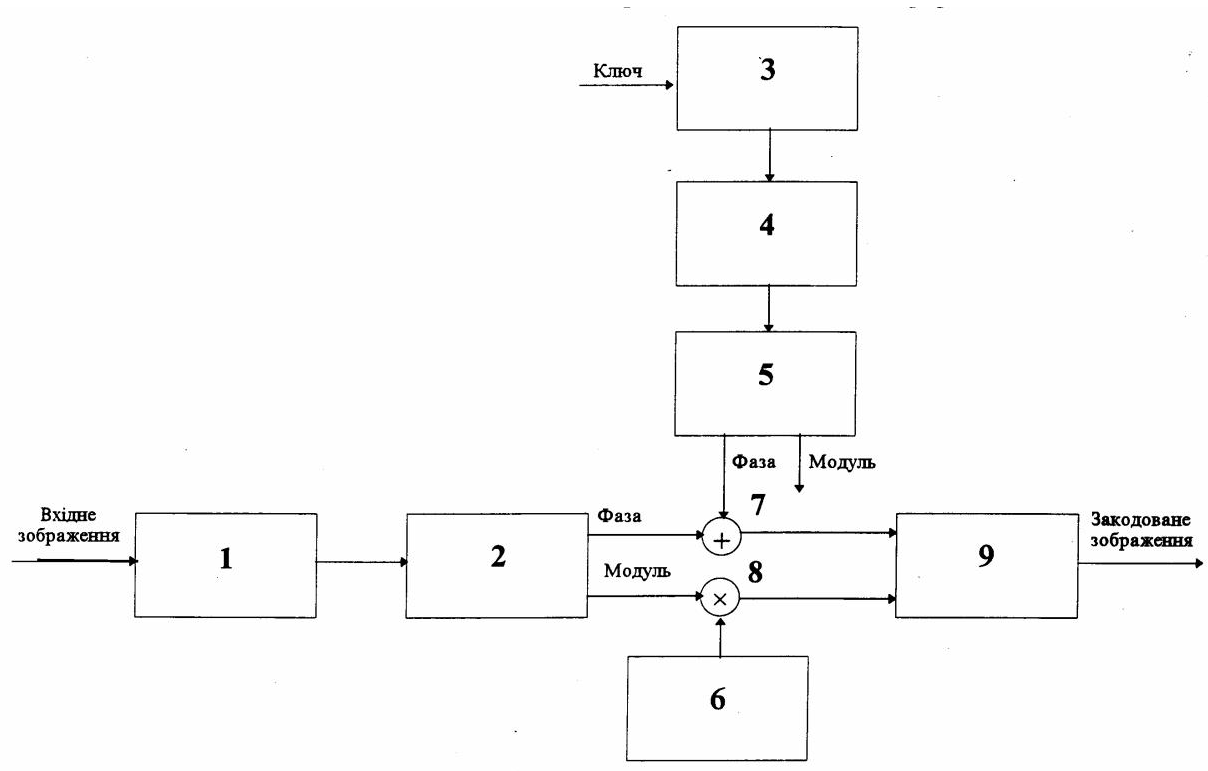
Призначення блоків 10,11,12,13,14 та 17 є аналогічним до призначення блоків 2,3,4,5, 6 та 9. Блоки 15 і 16 виконують операції віднімання і ділення відповідно. Блок 18 виконує перетворення цифрового зображення в аналогову форму.

Спосіб реалізується наступним чином.

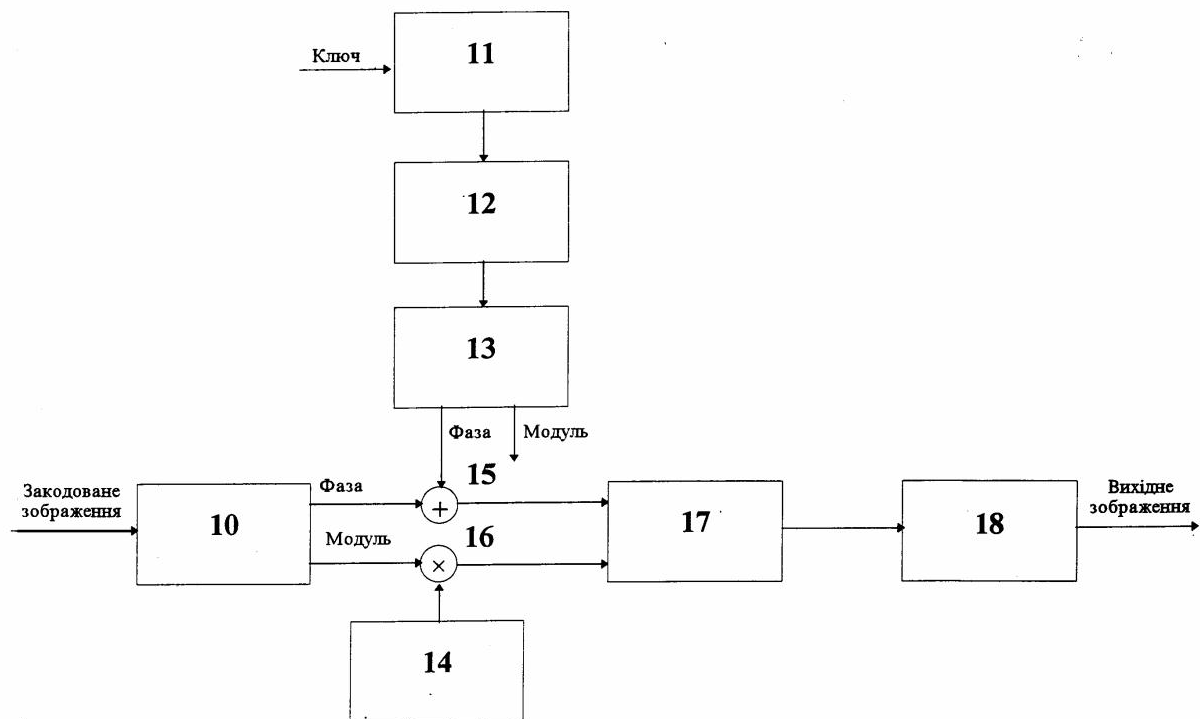
При засекречуванні інформації (використовується схема фіг. 1) зображення, яке підлягає засекречуванню, подають через блок оцифровування зображення 1 у блок прямого перетворення Фур'є 2, який формує його модуль та фазу на виходах "МОДУЛЬ" та "ФАЗА", відповідно. За допомогою ключа, введеного користувачем, у блоці встановлення початкового стану 3 встановлюють початковий стан генератора випадкового двовимірного поля за допомогою одного з стандартних генераторів гаусівського або рівномірного закону розподілу ймовірності. Під ключем розуміють введену користувачем певну послідовність символів - цифр і/або букв, перетворену у двійкову послідовність або ASCII код, на основі якого автоматично генерується випадкова шумова функція. Згенероване випадкове двовимірне поле трансформують у Фур'є область у блоці прямого перетворення Фур'є 5, де для подальшого засекречування використовують лише його фазову складову спектру, що алгебраїчно додають за допомогою блоку додавання 7 до фазової складової спектру зображення, яке підлягає засекречуванню. Описана процедура модифікації фазового спектру зображення на основі заданого користувачем ключа означена у патенті як ключ-перетворювач фаз складових спектру

(блоки 3,4,5 і 7 на фіг.1 та 11,12,13 і 15 на фіг.2). Тобто, це поняття включає формування випадкової шумової функції за допомогою ключа та операцію додавання (віднімання) її з фазовим спектром зображення. Отриманий модуль сигналу перемножують з заданою амплітудною характеристикою фільтра ключа, яка зберігається у блоці 6, за допомогою блоку множення 8. Процедура модифікації амплітудного спектру зображення на основі заданого користувачем ключа означена у патенті як ключ-перетворювач амплітудних складових спектру (блоки 6 і 8 на фіг. 1 та 14 і 16 на фіг. 2). Тобто, це поняття включає формування фільтра-ключа з певною смуговою амплітудною характеристикою в області середніх частот і операцію множення сформованої амплітудної характеристики на амплітудну характеристику зображення. Отримана фаза сигналу зображення має випадковий характер і вже не відображає характеристичних ознак вхідного зображення, а амплітудна характеристика має виражений низькочастотний або смуговий характер, що приведе до додаткового "розмиття" вхідного зображення, що обумовлено втратою високочастотних складових спектра, які визначають деталізованість зображення. Фільтрація за допомогою фільтра-ключа з смуговою амплітудною характеристикою в області середніх частот дозволяє усунути контури та текстури об'єктів зі зображення, які є визначальними факторами при розпізнаванні образів. Вибір смугової амплітудної характеристики пояснюється особливостями просторової передавальної характеристики системи сприйняття людиною візуальної інформації, яка має максимальне значення на просторовій частоті 8 циклів/градус. Таким чином, нелінійне зменшення інтенсивності спектральних складових у ділянці середніх частот у відповідності зі заданою за допомогою ключа амплітудною характеристикою погіршує чіткість та однозначність візуальної інформації. У блоці оберненого перетворення Фур'є 9 формується вихідне закодоване зображення з заданих відліків модуля і фази.

При розсекречуванні інформації використовується схема фіг. 2. Відмінність такої обробки у порівнянні зі схемою фіг. 1 полягає в усуненні внесених при засекречуванні спотворень у зображення-оригінал шляхом віднімання випадкової фазової складової, сформованої за допомогою ключа, введеного користувачем, який відомий на приймальній стороні, та інверсії спотворень амплітудної характеристики фільтра-ключа, що реалізується в блоках 15 і 16, відповідно. Крім того, у блоці 18 виконується цифро-аналогове перетворення зображення для переведення його в аналогову форму.



Фіг. 1



Фіг. 2

Тираж 50 екз.

Відкрите акціонерне товариство «Патент»
Україна, 88000, м. Ужгород, вул. Гагаріна, 101
(03122) 3 – 72 – 89 (03122) 2 – 57 – 03
