УКРАЇНА

(19) UA (11) 153107 (13) U

(51) МПК (2023.01)
H04L 9/00

НАЦІОНАЛЬНИЙ ОРГАН ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ДЕРЖАВНА ОРГАНІЗАЦІЯ "УКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ОФІС ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ТА ІННОВАЦІЙ"

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2022 01970**

(22) Дата подання заявки: **10.06.2022**

(24) Дата, з якої є чинними права інтелектуальної власності: **25.05.2023**

(46) Публікація відомостей про державну реєстрацію: **24.05.2023, Бюл.№ 21**

(72) Винахідник(и):
Авраменко Віктор Васильович (UA),
Бондаренко Микита Олегович (UA)

(73) Володілець (володільці):
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ, вул. Римського-Корсакова, 2, м. Суми, 40007 (UA)

(74) Представник:
ГУДКОВ СЕРГІЙ МИКОЛАЙОВИЧ

(54) СПОСІБ ШИФРУВАННЯ ГРАФІЧНИХ ЗОБРАЖЕНЬ

(57) Реферат:

Спосіб шифрування графічних зображень полягає в використанні інтегральної непропорційності першого порядку. Для шифрування зображення як ключ застосовують інше графічне зображення такого ж або більшого розміру, при цьому обчислюють і передають по відкритому каналу зв'язку інтегральні непропорційності першого порядку I_{ai}, I_{ri}, I_{gi}, I_{bi} послідовностей чисел, які відповідно описують прозорість a_i, червону r_i, зелену g_i та блакитну b_i складові яскравостей пікселів, які шифруються, за відповідними складовими A_i, R_i, G_i, B_i пікселів ключового зображення.

UA 153107 U

Корисна модель належить до систем захисту інформації із використанням симетричного ключа і являє собою спосіб шифрування і дешифрування графічної інформації за допомогою іншого графічного зображення як ключа із застосуванням інтегральної функції непропорційності першого порядку.

В основному алгоритмі криптографії із закритими ключами використовують функції перестановок та підстановок на множині цілих чисел. Використання ключів на множині простих цілих чисел має ряд суттєвих недоліків, що примушує розробляти системи на основі дійсних чисел.

Найбільш близьким до корисної моделі є "Спосіб шифрування даних із використанням функції дійсної змінної" [UA H04L 9/00 №143734, 10.08.2020, бюл. № 15, Україна].

Недоліком способу є необхідність непомітної передачі приймаючій стороні ключової функції дійсної змінної, для якої потрібно також передати інтервал, в якому змінюється аргумент функції і крок, з яким це відбувається. Передача такого ключа може привернути увагу на відміну, коли сторони обмінюються, наприклад, фотографіями або альбомами репродукцій картин, серед яких є ключове зображення.

В основу корисної моделі поставлена задача розробки криптосистеми, яка потребує лише одне кольорове графічне зображення як ключ і при цьому забезпечує стійкість системи.

Поставлена задача вирішується тим, що у способі шифрування графічних зображень, який полягає в використанні інтегральної непропорційності першого порядку, згідно з корисною моделлю, для шифрування зображення як ключ застосовують інше графічне зображення такого ж або більшого розміру, при цьому обчислюють і передають по відкритому каналу зв'язку інтегральні непропорційності першого порядку I_{ai}, I_{ri}, I_{gi}, I_{bi} послідовностей чисел, які відповідно описують прозорість a_i, червону r_i, зелену g_i та блакитну b_i складові яскравостей пікселів, які шифруються, за відповідними складовими A_i, R_i, G_i, B_i пікселів ключового зображення за формулами:

$$I_{ai}=\frac{a_{i-1}+a_i}{A_{i-1}+A_i}-\frac{a_i}{A_i}, \quad (1)$$

$$I_{ri}=\frac{r_{i-1}+r_i}{R_{i-1}+R_i}-\frac{r_i}{R_i}, \quad (2)$$

$$I_{gi}=\frac{g_{i-1}+g_i}{G_{i-1}+G_i}-\frac{g_i}{G_i}, \quad (3)$$

$$I_{bi}=\frac{b_{i-1}+b_i}{R_{i-1}+R_i}-\frac{b_i}{B_i}, \quad (4)$$

де і - порядковий номер пікселя в зображенні, яке шифрується, і також відповідний порядковий номер пікселя в ключовому зображенні, i=1, 2 …N,

N - кількість пікселів, що шифруються,

I - значення інтегральної непропорційності першого порядку;

a - прозорість;

r - червона складова пікселів;

g - зелена складова пікселів;

b - блакитна складова пікселів, які шифруються,

A - прозорість;

R - червона;

G - зелена;

B - блакитна

складові пікселів ключового зображення, при цьому при шифруванні на початку повідомлення завжди повинен знаходитися певний відомий приймальній стороні піксель, прозорість і складові яскравості якого a_0, r_0, g_0, b_0 і який використовується також при дешифруванні за формулами:

$$a_i=\frac{\left(a_{i-1}-I_{ai}*\left(A_{i-1}+A_i\right)\right)*A_i}{A_{i-1}}, \quad (5)$$

$$r_i=\frac{\left(r_{i-1}-I_{ri}*\left(R_{i-1}+R_i\right)\right)*R_i}{R_{i-1}}, \quad (6)$$

$$g_i = \frac{\left(g_{i-1} - I_{gi} * \left(G_{i-1} + G_i\right)\right) * G_i}{G_{i-1}}, \quad (7)$$

$$b_i = \frac{\left(b_{i-1} - I_{bi} * \left(B_{i-1} + B_i\right)\right) * B_i}{B_{i-1}}, \quad (8)$$

які дозволяють отримати розрахункові значення складових яскравостей пікселів, що округляються до найближчих цілих чисел, в результаті стають відомими пікселі графічного зображення, що передається.

Завдяки такому рішенню зникає необхідність передавати як ключ функцію дійсної змінної, інтервал, в якому повинен змінюватися аргумент функції і крок, з яким це відбувається. Передача як ключа, наприклад, фотографії або малюнка серед багатьох інших привертає меншу увагу.

Ще одним елементом захисту є обумовлені обома сторонами прозорість і складові яскравості пікселя, з якого повинно починається шифрування і дешифрування. Все це забезпечує високу крипостійкість системи. Високій крипостійкості також сприяє те, що одні і ті ж складові яскравостей пікселів шифрується по-різному залежно від порядкового номера пікселя в повідомленні.

Спосіб здійснюється таким чином.

Вибирають кольорове графічне зображення як ключ, яке повинно бути не меншим від графічного зображення, яке передається. Також домовляються про значення прозорості і складових яскравості пікселя під номером нуль.

Шифрування повідомлення.

1. Прочитати із файлу послідовність пікселів зображення, яке передається і визначити числові значення прозорості і складових яскравостей a_i, r_i, g_i, b_i, де i=1,2,…,N.

Теж саме повторити для зображення, яке використовується як ключ і отримати відповідні значення прозорості і складових яскравостей A_i, R_i, G_i, B_i (i=1,2,…,N).

2. Обчислити непропорційності I_{ai}, I_{ri}, I_{gi}, I_{bi} (i=1,2,…,N) за формулами (1-4). При обчисленнях використовуються секретні, домовлені із обома сторонами, значення прозорості і складових яскравостей A_0, R_0,G_0, B_0.

3. Передати по відкритому каналу зв'язку послідовності I_{ai}, I_{ri}, I_{gi}, I_{bi}.

4. За відомими A_0, R_0,G_0 B_0 і отриманими значеннями непропорційностей I_{ai}, I_{ri}, I_{gi}, I_{bi} за формулами (5-8) обчислити розрахункові значення прозорості і складових яскравостей пікселів.

5. Отримані розрахункові значення округлити до цілих чисел і отримати кінцеві значення пікселів зображення, яке передається.

Обмеження на ключові зображення.

1. Складові яскравостей пікселів зображення не повинні бути нульовими.

2. Ключове зображення не повинне бути меншим, ніж зображення, яке передається.

3. Перед відправленням зашифрованого повідомлення попередньо перевірити, як виглядає дешифроване, щоб уникнути помилок, які можуть трапитися внаслідок неврахування попередніх пунктів.

Спосіб шифрування графічних зображень, де як ключ використовується інше кольорове графічне зображення з однаковими або більшими розмірами, дозволяє урізноманітнити непомітну передачу приймаючій стороні симетричного ключа. Застосування як ключів графічних зображень у вигляді фотографій, малюнків, карт, текстів, в тому числі написаних від руки, значно розширює поле можливих ключів і ускладнює можливість їх підбору.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Спосіб шифрування графічних зображень, який полягає в використанні інтегральної непропорційності першого порядку, який **відрізняється** тим, що для шифрування зображення як ключ застосовують інше графічне зображення такого ж або більшого розміру, при цьому обчислюють і передають по відкритому каналу зв'язку інтегральні непропорційності першого порядку I_{ai}, I_{ri}, I_{gi}, I_{bi} послідовностей чисел, які відповідно описують прозорість a_i, червону r_i, зелену g_i та блакитну b_i складові яскравостей пікселів, які шифруються, за відповідними складовими A_i, R_i,G_i, B_i пікселів ключового зображення за формулами:

$$I_{ai} = \frac{a_{i-1} + A_i}{A_{i-1} + A_i} - \frac{R_{i-1}}{A_i},$$

$$I_{ri} = \frac{r_{i-1} + r_i}{R_{i-1} + R_i} - \frac{r_i}{R_i},$$

$$I_{gi} = \frac{g_{i-1} + g_i}{G_{i-1} + G_i} - \frac{g_i}{G_i},$$

$$I_{bi} = \frac{b_{i-1} + b_i}{R_{i-1} + R_i} - \frac{b_i}{B_i},$$

де i - порядковий номер пікселя в зображенні, яке шифрується, і також відповідний порядковий номер пікселя в ключовому зображенні, i=1, 2 … N,
N - кількість пікселів, що шифруються,
I - значення інтегральної непропорційності першого порядку;
a - прозорість;
r - червона складова пікселів;
g - зелена складова пікселів;
b - блакитна складова пікселів, які шифруються,
A - прозорість;
R - червона;
G - зелена;
B - блакитна
складові пікселів ключового зображення, при цьому при шифруванні на початку повідомлення завжди повинен знаходитися певний відомий приймальній стороні піксель, прозорість і складові яскравості якого (a$_0$, r$_0$, g$_0$, b$_0$) і який використовується також при дешифруванні за формулами:

$$a_i = \frac{(a_{i-1} - a_{di} * (A_{i-1} + A_i)) * A_i}{A_{i-1}},$$

$$r_i = \frac{(r_{i-1} - I_{ri} * (R_{i-1} + R_i)) * R_i}{R_{i-1}},$$

$$g_i = \frac{(g_{i-1} - I_{gi} * (G_{i-1} + G_i)) * G_i}{G_{i-1}},$$

$$b_i = \frac{(b_{i-1} - I_{bi} * (B_{i-1} + B_i)) * B_i}{B_{i-1}},$$

які дозволяють отримати розрахункові значення складових яскравостей пікселів, що округляються до найближчих цілих чисел, в результаті стають відомими пікселі графічного зображення, що передається.

Комп'ютерна верстка В. Мацело

ДО "Український національний офіс інтелектуальної власності та інновацій", вул. Глазунова, 1, м. Київ – 42, 01601