УДК 004.056.5

Борисенко І.І., Кас'яненко М.М.

Національний університет «Одеська політехніка»

МАТЕМАТИЧНІ МЕТОДИ КОМБІНАТОРИКИ, ЯК ЗАСІБ СТВОРЕННЯ КРИПТОГРАФІЧНИХ ШИФРІВ

Вступ. Техніка транспозиції - це криптографічний прийом, який використовується для перетворення простого тексту в текст шифру. Це досягається шляхом перестановки положення символів у простому тексті. Є різні методи транспозиції такі як техніка залізничного паркану, прості методи стовпчастої транспозиції прості методи стовпчастої транспозиції - кілька раундів. На жаль, оскільки транспозиційний шифр не змінює частоту окремих літер, він все ще сприйнятливий до частотного аналізу, хоча транспозиція дійсно усуває інформацію з пар літер. Тому розробка подальшого розвитку цього виду шифру є актуальною. В роботі пропонується шифр, який базується на математичних методах обробки перестановок та дій з ними.

Мета: Розробка криптографічного шифру комбінаторними засобами та подальше його застосування для цілей сеганографії.

Основна частина.

Оскільки основою нового стеганографічного алгоритму є такий комбінаторний об'єкт як перестановки (позначимо літерою P), то введемо саме поняття перестановки та операції над перестановками, які будемо використовувати під час вбудовування повідомлення у контейнер. Перестановкою будемо називати бієкцію φ скінченої множини на себе. Отже, φ є перестановка на M тоді і тільки тоді, коли для довільних елементів $a,b\in M$, $a\neq b$, маємо $\varphi(a)\neq\varphi(b)$. А це означає, що перестановка визначається таблицею виду

$$\begin{pmatrix}1 & 2 & 3 & \dots & n-1 & n\\ a_1 & a_2 & a_3 & \dots & a_{n-1} & a_n\end{pmatrix},$$

де $a_1, a_2, ..., a_n$ - різні елементи з множини M .

Для будь-яких перестановок φ та ψ визначена операція добутку $\varphi\circ\psi$, який знаходиться за правилом: спочатку переставляють стовпці в таблиці ψ так, щоб її верхній рядок співпав з нижнім рядком таблиці φ, а потім будують нову таблицю, першим рядком якої є перший рядок таблиці φ, а другим – другий рядок таблиці ψ. Щоб побудувати перестановку обернену даній φ^{-1} треба поміняти рядки перестановки φ місцями, а потім стовпці переставити так, щоб числа першого рядка були розміщені у зростаючому порядку. Для реалізації алгоритму, що пропонується в роботі, потрібно вміти розв'язувати рівняння, елементами якого є перестановки. Розглянемо рівняння:

$$\varphi\circ x=\psi \qquad (1)$$

В роботі досліджується питання чи існує така перестановка x, для якої виконується рівність (1). Якщо така перестановка існує, то чи вона єдина? Оскільки φ - перестановка, то розв'язок рівняння (1) існує і він єдиний. Оскільки по означенню φ - бієкція, то для неї існує обернена перестановка φ^{-1}, тому можна

розглянути перетворення $\varphi^{-1}\circ\psi$. Щоб показати, що $\varphi^{-1}\circ\psi$ є розв'язком рівняння (1), треба обчислити добуток $\varphi\circ(\varphi^{-1}\circ\psi)$. Використовуючи властивість асоціативності добутку [1] та визначення оберненої перестановки, яке подано вище, одержимо $\varphi\circ(\varphi^{-1}\circ\psi)=(\varphi\circ\varphi^{-1})\circ\psi=\varepsilon\circ\psi=\psi$, де ε - тотожна перестановка, яка має вигляд $\begin{pmatrix}1 & 2 & 3 & .... & n\\ 1 & 2 & 3 & .... & n\end{pmatrix}$. А це означає, що $\varphi^{-1}\circ\psi$ - є розв'язком рівняння (1). Щоб показати, що розв'язок $\varphi^{-1}\circ\psi$ - єдиний, позначимо його літерою α, тоді рівняння (1) прийме вигляд $\varphi\circ\alpha=\psi$ помноживши одержане рівняння зліва на φ^{-1}, одержимо $\varphi^{-1}\circ(\varphi\circ\alpha)=\varphi^{-1}\circ\psi$, або $(\varphi^{-1}\circ\varphi)\circ\alpha=\varphi^{-1}\circ\psi$ і, остаточно $\varepsilon\circ\alpha=\varphi^{-1}\circ\psi$, $\alpha=\varphi^{-1}\circ\psi$. Ця рівність означає, що ніяких інших розв'язків рівність (1) не має. Ще одне питання, яке треба розглянути – це обчислення кількості перестановок, які можна побудувати з елементів множини M, яка має n елементів. Вирішення цього питання залежить від того, чи різні елементи становлять множину M, або ж вона має однакові елементи. Методи такого розділу математики, як комбінаторика, дають формули для підрахунку перестановок для різного складу множини M. Якщо всі елементи множини M різні, то кількість перестановок дорівнює:

$$P_n=n! \tag{2}$$

Якщо ж в множині M є k_1 елементів першого типу, k_2 - елементів другого типу і так далі, k_s елементів s-го типу, то кількість перестановок обчислюється за формулою:

$$P_{(n;k_1,\ldots,k_s)}=\frac{n!}{k_1!\cdot k_2!\cdot\ldots\cdot k_s!} \tag{3}$$

До безпосереднього процесу вбудовування повідомлення потрібно виконати препроцесінг і самого повідомлення і контейнера, в якості якого виступає цифрове зображення в градаціях сірого, або ж синя складова кольорового зображення [2], оскільки зорова система людини менш чутлива до синього кольору. Елементи повідомлення кодуються цифрами, які належать деякій множині $M=\{1,2,...,k\}$. Елементи контейнера послідовно групуються у блоки розміром $1\times n$. При вбудовуванні повідомлення використовується деякий допоміжний масив $masiv$, в якому знаходиться k перестановок довжини n. Всі перестановки занумеровані. При вбудовуванні елемента повідомлення з кодом i в масиві $masiv$ знаходимо перестановку з номером i, перемножуємо її на ключ φ, одержуємо перестановку ψ. Масив $masiv$ не містить перестановки, добуток якої з ключем φ дає тотожну перестановку. Блоки контейнера, які складаються з однакових елементів випускаються. Елементи інших блоків переставляються згідно перестановці ψ тільки в тому випадку, якщо для будь-якої пари елементів, які обмінюються місцями, різниця їх значень не перевищує деяке число d .Стеганографічний алгоритм, назвемо його Permut, в загальному вигляді представимо наступними кроками.

Крок 1. Розбиваємо матрицю контейнера – зображення на блоки заданого розміру $1\times n$.

Крок 2. Для елемента повідомлення з кодом i в масиві $masiv$ знаходимо

перестановку з номером i, множимо її на ключ φ, одержуємо перестановку ψ.

Крок 3. Якщо блок контейнера складається з однакових елементів переходимо до наступного блоку.

Якщо блок має хоча б два різні елементи виконуємо перестановку пікселів згідно перестановці ψ тільки в тому випадку, якщо для будь-якої пари елементів, які обмінюються місцями, різниця їх значень не перевищує деяке число d, інакше переходимо до наступного блоку. Алгоритм Permut не є «сліпим» тому для декодування повідомлення потрібна наявність контейнера. Щоб декодувати повідомлення, вбудоване повідомлення алгоритмом Permut треба розбити матрицю контейнера та стеганоконтейнера на блоки того самого розміру, що і при вбудовуванні. Порівняти відповідні блоки контейнера та стего, якщо вони співпали, то це означає, що в блок повідомлення не вбудовувалося. У іншому разі треба обчислити перестановку φ^{-1} обернену до ключа φ та обчислити добуток $\alpha = \varphi^{-1} \circ \psi$. Одержану перестановку α знай ти в масиві $masiv$, порядковий номер, який відповідає α є кодом елемента вбудованого повідомлення.

Із збільшенням довжини блоку складність алгоритму збільшується, оскільки збільшується кількість випадків стосовно складу блоків, які треба аналізувати. Продемонструємо сказане на конкретному прикладі. Нехай $n = 4$, розглянемо які випадки можуть бути стосовно складу блоків контейнера та визначимо, яку мінімальну кількість перестановок повинен містити масив $masiv$. Якщо всі елементи блоку різні, то кількість різних перестановок дорівнює 4!=24. В блоці 3 однакових елементи, тоді маємо $P_{(4;3)} = \frac{4!}{3!} = \frac{24}{6} = 4$ перестановки, в блоці 2 однакових елементи – маємо $P_{(4;2)} = \frac{4!}{2!} = \frac{24}{2} = 12$ перестановок, в блоці два елементи зі значенням $c1$ і два елементи зі значенням $c2$, тоді $P_{(4;2,2)} = \frac{4!}{2!2!} = \frac{24}{4} = 6$ перестановок. Таким чином мінімальна кількість перестановок, яка нам потрібна дорівнює чотирьом, тому повідомлення можна кодувати вже чотирма цифрами. Зрозуміло, що якщо довжину блоку контейнера ще збільшити на одиницю, то кількість випадків значно зросте і складність алгоритму збільшиться. Але, якщо будуть поставлені вимоги щодо зменшення викривлень контейнера, то розширити Permut завжди можливо, включивши додаткові перевірки складу блоків.

Висновок. Розроблено стеганографічний алгоритм просторової області вбудовування Permut, заснований на використанні такої комбінаторної конфігурації як перестановки та дій з ними. Подальший розвиток роботи – це дослідження Permut для різної довжини блоків, а саме $n = 3$ та $n = 4$ з метою вивчення їх властивостей.

Перелік використаних джерел

1. Нікольський Ю.В, Пасічник В.В, Щербина Ю.М. Дискретна математика. – К.: Видавнича група BHV, 2007. – 368 с.

2. Гонсалес Р. Цифровая обработка изображений / Р.Гонсалес, Р.Вудс; пер. с англ. под ред. П.А.Чочиа. - М.: Техносфера, 2005. - 1072 с.