

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ Г. С. СКОВОРОДИ



НАУКОВО-ДОСЛІДНА РОБОТА СТУДЕНТІВ ЯК ЧИННИК УДОСКОНАЛЕННЯ ПРОФЕСІЙНОЇ ПІДГОТОВКИ МАЙБУТНЬОГО ВЧИТЕЛЯ

Збірник наукових праць

Випуск 23

ХАРКІВ - 2024



Редін Микола, Андрієвська Віра Освітній потенціал соціальних мереж	103
Романько Анастасія, Винник Олександр Розробка комп'ютерного рефрактометра на основі програмного засобу ColorKit	111
Синицька Ярослава, Андрієвська Віра Цифрова компетентність вчителя Нової української школи	117
Слісаренко Микола, Андрієвська Віра Чат-бот: поняття, історія розвитку, перспективи застосування	124
Слісаренко Роман, Колгатіна Лариса Використання чат-ботів для взаємодії студентів із викладачами: виклики та можливості у контексті питань доступності	134
Талалай Віталій, Гайдусь Андрій Використання технологій дистанційного навчання в освітньому процесі профільної школи	145
Хвіц Вадим, Андрієвська Віра Організації самостійної роботи учнів базової середньої школи при вивченні програмування	154
Храмов Олексій, Гайдусь Андрій Методика навчання кодування даних у шкільному курсі інформатики	163
Чернишова Орина, Штонда Оксана Організація онлайн-навчання математики: виклики сучасності	173
Щербак Сергій, Гайдусь Андрій Розробка комп'ютерної гри для навчання школярів основ безпечної поведінки в Інтернеті	182

УДК 378:004

<https://doi.org/10.5281/zenodo.10812932>

Храмов Олексій

здобувач другого (магістерського) рівня вищої освіти
кафедра інформатики

Харківський національний педагогічний університет імені Г. С. Сковороди

Гайдусь Андрій

кандидат технічних наук, доцент кафедри інформатики

Харківський національний педагогічний університет імені Г.С. Сковороди

<https://orcid.org/0000-0001-8414-5765>

МЕТОДИКА НАВЧАННЯ КОДУВАННЯ ДАНИХ У ШКІЛЬНОМУ КУРСІ ІНФОРМАТИКИ

Анотація. У сучасному світі, де програмування можна зустріти будь-де і воно є найцікавішою професією, треба мати цікавий та зрозумілий спосіб зацікавити дитину у його вивченні. Стаття висвітлює значення стеганографії в шкільному курсі інформатики, покладаючи основний акцент на її актуальності та цікавості для учнів. Розглядаються сучасні підходи та методи викладання стеганографії, враховуючи переваги цього методу навчання кодування для дітей. Важливим аспектом є аналіз того, як стеганографія стає потужним інструментом для розвитку ключових навичок учнів у сфері програмування. Навчання програмуванню через стеганографію враховує сучасні технології та педагогічні тенденції. Закликаючи вчителів інформатики до використання стеганографії як засобу зацікавлення учнів у програмуванні, стаття сприяє розвитку та впровадженню ефективних методів навчання в шкільних програмах.

Ключові слова: стеганографія; навчання; програмування.

Постановка проблеми дослідження. У сучасному освітньому контексті, де важливість володіння комп'ютерно-технічними навичками стає дедалі актуальнішою, питання вивчення кодування у школі набуває особливого значення. Однак, незважаючи на загальний рух у напрямку інтеграції інформаційних технологій у навчання, виникає

питання ефективності та привабливості існуючих методів викладання програмування.

Серед сучасних підходів важливе місце займає стеганографія, яка, крім технічного аспекту, пропонує цікавий та захоплюючий контекст для вивчення кодування даних. Основною проблемою дослідження є необхідність визначення ефективності та придатності стеганографії як методу викладання кодування даних у шкільному курсі інформатики, а також вивчення її впливу на мотивацію та розвиток когнітивних навичок учнів. Розкриття цих аспектів сприятиме оптимізації навчального процесу та підвищенню якості інформатичної освіти в школах.

Аналіз останніх джерел і публікацій. Останні дослідження [9] та публікації [8] в галузі методики навчання програмування у школі визначають ключові тенденції, які визначають сучасний підхід до цього питання. Виділяється зростаючий інтерес до використання інтерактивних методів, спрямованих на створення цікавого та ефективного навчального середовища для учнів 8-9 класів. Також вони [9] надають увагу використанню практичних завдань, які не лише викладають основи кодування, але й заохочують учнів до креативного мислення та розвитку алгоритмічних навичок. Акцент робиться на розробці завдань, які релевантні для учнів, адаптованих до сучасних програм навчання інформатики.

Тенденція використання ігрових елементів у навчанні також визначається. Деякі джерела вказують на успішні приклади використання гри як засобу для залучення уваги та створення динамічного, захоплюючого середовища, сприяючи навчанню програмування.

Виділення невирішених раніше частин загальної проблеми. Існують проблеми в методиці навчання кодування даних у шкільному курсі інформатики, які включають адаптацію до індивідуальних потреб учнів, ефективне використання сучасних технологій, узгоджені методики оцінювання успішності, вплив на мотивацію та розвиток креативності, інтеграцію із загальношкільною системою освіти та подальший розвиток педагогічних методів. Розв'язання цих аспектів

сприятиме поліпшенню методики навчання кодуванню даних та підвищить ефективність навчання учнів в шкільному курсі інформатики.

Формування цілей статті. Мета даної роботи полягає у розробці та представленні ефективної методики навчання кодування даних у шкільному курсі інформатики для учнів 8-9 класів, використовуючи стеганографію. Робота спрямована на створення гнучкого та цікавого навчального середовища, яке враховує особливості розвитку та інтереси учнів цього вікового діапазону. Основний акцент робиться на практичних вправах, спрямованих на розвиток навичок програмування через стеганографію, що допомагатиме учням зробити обдуманий вибір та підняти рівень їхнього розуміння якості та функціональності кодування даних.

Виклад основного матеріалу дослідження. У сучасному світі, де високі технології стають неодмінною частиною нашого повсякденного життя, вивчення програмування в середній школі стає надзвичайно актуальним завданням. Подолати цей "цифровий рубікон" стає неминучістю для підготовки нового покоління до викликів і можливостей, що виникають у сфері інформаційних технологій.

Однак, вибір ефективного методу навчання, який не лише передасть ключові концепції програмування, але й зацікавить учнів, залишається важливим викликом для вчителів. В цьому контексті, стеганографія виступає як захопливий та інноваційний спосіб вивчення кодування даних, зокрема для учнів 8-9 класів.

В епоху загальної цифровізації та постійного зростання кількості електронної інформації, уміння ефективно працювати з даними стає ключовою навичкою. Вивчення кодування даних в шкільному віці сприяє розвитку не лише технічних, але і логічних та творчих здібностей. Інтеграція стеганографії в навчальний процес дозволяє створити зазначений баланс між розвитком навичок та зацікавленням учнів.

Стеганографія – це метод організації зв'язку, який власне приховує сама наявність зв'язку[1]. Методи стеганографії надає змоги вбудовувати секретні повідомлення в нешкідливі послання таким

чином, щоб неможливо було запідозрити існування вбудованого таємного послання, на відміну від криптографії, де ворог точно може визначити чи є передане повідомлення зашифрованим текстом.

Зараз з'явилися нові стеганографічні методи, в основі яких лежать особливості подання інформації в файлах, комп'ютерних мережах. При цьому, ми можемо казати, про появу нового напрямку — комп'ютерна стеганографія. Стеганографія, зокрема, відзначається своєю гнучкістю та невеликою складністю вивчення, що робить її ідеальним вибором для учнів середніх класів. Цей метод дозволяє здійснювати приховання інформації в різних медіа-файлах, таких як зображення чи аудіо, і стає доступним для учнів з різним рівнем підготовки.

Приклади використання. Наприклад, учні можуть створювати власні зашифровані повідомлення, вбачаючи результати своєї роботи через призму таємничості та розвиваючи при цьому свої алгоритмічні навички. Такий підхід дозволяє поглибити розуміння та зацікавлення учнів у світ програмування, використовуючи доступний та захоплюючий контекст стеганографії [2].

У якості моделі стеганографічної системи використовувалася запропонована у 1983 році Сіммонсом так звана "проблема ув'язнених". Зміст в тому, що два індивідуума (Аліса та Боб) хочуть обмінюватися секретними повідомленнями без втручання охоронця (Віллі), який контролює комунікаційний канал. Виникає ряд припущень, які роблять цю проблему більш-менш розв'язуваною. Відносно, першого припущення вирішення проблеми, вона полягає в тому, що учасники інформаційного обміну можуть розділяти секретне повідомлення (наприклад, це кодова клавіша) перед укладанням. Друге припущення, утрудняє вирішення проблеми, так як охоронець має право не тільки читати повідомлення, але і модифікувати (змінювати) їх.

У 1996 році було запропоновано використовувати єдину термінологію та обговорені основні терміни на конференції Information Hiding: First Information Workshop.

Стеганографічна система (стегосистеми) – це сукупність засобів і методів, які використовуються для формування прихованого каналу

передачі інформації. Стегосистеми повинні відповідати наступним вимогам:

- Щоб зміну неможливо було виявити при візуальному контролі, властивості контейнера повинні бути модифіковані. Ця вимога визначає якість приховування впроваджуваного повідомлення: для забезпечення безперешкодного проходження стегоповідомлення по каналу зв'язку, воно жодним чином не повинно привернути увагу атакуючого.
- Стегоповідомлення повинно бути стійким до спотворень. У процесі передачі зображення (звук або другий контейнер) повинен зазнавати різні трансформації: збільшуватися або зменшуватися, перетворюватися в інший формат. Крім того, воно може бути стисло, в тому числі і з використанням алгоритмів стиснення з втратою даних [5].
- Для підвищення надійності потрібно щоб повідомлення було продубльовано.
- Для збереження цілісності вбудованого повідомлення необхідно використання коду з виправленням помилки.

Приклади алгоритмів стеганографії [7].

Алгоритм Куттера

Алгоритм впровадження

Якщо 24-бітове зображення має RGB-кодування, то вбудовування виконується в канал синього кольору, тому що до синього кольору система людського зору найменш чутлива. Розглянемо алгоритм передачі одного біта секретної інформації. Нехай s_i - вбудований біт, $I = R, G, B$ - контейнер, $p = (x, y)$ - позиція, в якій виконується вкладення. Секретний біт вбудовується в канал синього кольору шляхом модифікації яскравості:

$$l(p) = 0.299r(p) + 0.587g(p) + 0.114b(p)$$

$$b_l(p) = \begin{cases} b(p) - ql(p), & \text{if } s_i = 1 \\ b(p) + ql(p), & \text{if } s_i = 0 \end{cases}$$

де q - константа, яка визначає енергію вбудованого сигналу.

Її величина залежить від призначення схеми. Чим більше q , тим вище робастної вкладення, але тим сильніше його помітність.

Алгоритм добування

Витяг біта одержувачем здійснюється без наявності у нього вихідного зображення, тобто наосліп. Далі виконується пророкування значення вихідного, немодифіцированого пікселя на підставі значень його сусідів. Для отримання оцінки пікселя можна використовувати значення декількох пікселів, розташованих в тому ж стовпці і в тому ж рядку, що утворюють «хрест» розміром 7×7 .

Оцінка b виходить у вигляді [3]:

$$\bar{b}_2(p) = \frac{1}{4c} \cdot \left(-2 \cdot b_2(p) \cdot \sum_{i=-c}^c b_2(x+i, y) + \sum_{k=-c}^c b_2(x, y+k) \right)$$

де c - число пікселів зверху (знизу, зліва, справа) від оцінюваного пікселя ($c = 3$).

Так як в процесі вбудовування ЦВЗ кожен біт був повторений cr раз, то ми отримаємо cr оцінок одного біта ЦВЗ. Секретний біт знаходиться після усереднення різниці оцінки пікселя і його реального значення:

$$\delta = \frac{1}{cr} \cdot \sum_{i=1}^c r \left(\bar{b}_i(p) - b_i(p) \right)$$

Алгоритм Patchwork

Алгоритм впровадження ЦВЗ

В основі алгоритму Patchwork лежить статистичний підхід. Patchwork впроваджує в вихідне зображення певну статистику, яка має гауссовське розподіл. Треба псевдовипадковим чином на основі ключа вибрати два пікселя зображення (A і B). Потім значення яскравості синій кольоровій компоненти одного з них збільшується на значення $\delta = 3$, а значення яскравості синій кольоровій компоненти іншого - зменшується на δ . Далі цей процес повторюється $n = 10000$ раз. Настільки унікальна статистика вказує присутність або відсутність підпису. Patchwork незалежний від змісту зображення-контейнера. Це забезпечує досить високий опір більшості негеометричних модифікацій зображення. Для аналізу необхідно зробити деякі припущення: сигнал кожної колірної компоненти кодується числом від

0 до 255, всі рівні яскравості однаково вірогідні, змінювані точки зображення вибираються випадковим чином. Алгоритм Patchwork виконується наступним чином: беруться будь-які дві точки, A і B , вибрані навмання в зображенні [9]. Нехай a - яскравості в точці A , b - яскравості в точці B . Тепер нехай $S = a - b$.

Очікуване значення S дорівнює 0, тобто середнє значення S після повторення цієї процедури велике число раз буде дорівнює 0. Хоча очікуване значення дорівнює 0, це не говорить нам нічого про те, яке значення S буде приймати в кожному конкретному випадку. Це пояснюється тим, що розсіювання вельми високо для цієї процедури. Дисперсія $\delta^2 S$ - міра того, як сильно значення S будуть згруповані навколо очікуваного значення 0. Щоб її обчислити, використовуємо припущення про незалежність вибору точок a і b . Так як $S = a - b$, і a і b прийняті незалежними, $\delta^2 S$ може бути обчислена в такий спосіб (це і всі інші рівняння ймовірності - по Дрейку):

$$\delta_S^2 = \delta_a^2 + \delta_b^2,$$

Очевидно, що $\delta_a^2 = \delta_b^2$, так як a і b - елементи одного і того ж безлічі значень яскравості. Таким чином:

$$\delta_S^2 = 2 \times \delta_a^2 \approx 2 \times \frac{(255 - 0)^2}{12} \approx 10836$$

тоді значення середньоквадратичного відхилення $\delta S \approx 104$. Це означає, що в більш ніж половині випадків значення S буде більше, ніж 43, або менше, ніж -43, що значно відрізняється від нуля. Беручи гауссовське розподіл, неприпустимо використовувати тільки одну ітерацію. Тому дану процедуру необхідно повторити велику кількість разів. Нехай процедура повторюється n раз, позначимо через a_i і b_i значення a і b на i -й ітерації, S_i - різниця цих значень. Тепер нехай S_n визначається як:

$$S_n = \sum_{i=1}^n S_i = \sum_{i=1}^n (a_i - b_i)$$

Математичне сподівання величини S_n є:

$$S_n = n \times S = n \times 0 = 0$$

Це інтуїтивно зрозуміло, так як кількість разів, коли a_i більше, ніж b_i відшкодовується кількістю раз, коли вірно зворотне. В такому випадку дисперсія є:

$$\delta_{S_n}^2 = n \times \delta_S^2,$$

а середньоквадратичне відхилення:

$$\delta_{S_n} = \sqrt{n} \times \delta_S \approx \sqrt{n} \times 104$$

Тепер для зображення можна обчислити S_{10000} , і якщо її значення перевищує середньоквадратичне відхилення в кілька разів, то можна з упевненістю робити висновок, що результат не випадковий, і зображення містить водяний знак. Алгоритм Patchwork штучно змінює значення S в зображенні таким чином, щоб воно відрізнялося від Мат.ожидание на кілька середньоквадратичних відхилень. Щоб закодувати зображення, необхідно:

1. Використовувати спеціальний ключ генератора псевдовипадкових чисел для вибору точок a_i і b_i . Це дуже важливо, тому що декодер повинен опрацювати ті ж самі точки, що і кодер.

2. Збільшити значення яскравості в точці a_i на величину δ , рівну 1 - 5 з 256.

3. Зменшити яскравість точки b_i на ту ж саму величину δ .

4. Повторити дії n раз (зазвичай $n = 10000$).

Алгоритм вилучення ЦВЗ

Для виявлення ЦВЗ необхідно відвідати ті ж точки, що і при кодуванні, обчисливши при цьому суму різниць яскравості в точках a_i і b_i :

$$S'_n = \sum_{i=1}^n [(a_i + \delta) - (b_i - \delta)] = 2\delta n + \sum_{i=1}^n (a_i - b_i)$$

Математичне очікування величини:

$$\sum_{i=1}^n (a_i - b_i)$$

суми різниці значень яскравості пікселів в незаповненому контейнері близько до нуля при досить великій кількості точок. На кожному повторенні мат.ожидание накопичує величину 2δ . Після n повторень $S'n$ перевищить середньоквадратичне відхилення в кілька разів:

$$\frac{2\delta n}{\delta_{S'n}} \approx 0.028\sqrt{n}$$

Чим більше значення n і δ , тим правіше зсувається графік розподілу величини $S'n$. Зрештою, може виникнути така ситуація, коли два розподілу ($S'n$ і S_n) практично не будуть перекриватися. Це призведе до того, що з високою часткою ймовірності можна буде визначити, чи містить сигнал ЦВЗ чи ні. При $\delta = 3$, а $n = 10000$ між Мат.ожидание величин $S'n$ і S_n вміщається 8.4 середньоквадратичних відхилення, що дозволяє однозначно судити про наявність водяного знаку в зображенні.

Висновки з дослідження і перспективи подальших розвідок. На основі проведеного аналізу та вивчення ефективності використання стеганографії в навчанні програмуванню для учнів середніх класів можна зробити кілька важливих висновків. Спочатку, стеганографія дійсно виявляється вдалим інструментом, який не лише надає можливість вивчення кодування даних, але й створює захопливий та цікавий контекст для учнів.

Підтримуючи невелику складність та гнучкість методу, стеганографія відкриває шлях до успішного впровадження в шкільний курс інформатики. Зазначена гнучкість дає можливість адаптувати завдання згідно із рівнем підготовки учнів, що допомагає забезпечити позитивний досвід вивчення.

Список використаної літератури

1. Wikipedia Стеганографія. URL:
<https://uk.wikipedia.org/wiki/%D0%A1%D1%82%D0%B5%D0%B3%D0%B0%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F>

2. Modern methods of computer steganography systematization. URL: https://www.researchgate.net/publication/311654964_Modern_methods_of_computer_steganography_systematization
3. Математична модель стегосистеми. URL: Математична модель стегосистеми: <https://studfile.net/preview/9650052/page:5/>
4. Стеганографія. Метод Коха Жао. URL: <http://um.co.ua/4/4-17/4-174333.html>
5. Особливості приховування інформації в зображеннях. URL: <https://journal.ldubgd.edu.ua/index.php/Visnuk/article/download/1585/1510/>
6. Cachin C. An Information-Theoretic Model for Steganography Proceeding of the Workshop on Information Hiding. 1998. DOI: 10.1145/3531536
7. Husrev T. Sencar ,Mahalingam Ramkumar, Ali N. Akansu. Data Hiding Fundamentals And Applications [Digital Multimedia] ELSEVIER science and technology books. 2004. 364 p. URL: <https://www.sciencedirect.com/book/9780120471447/data-hiding-fundamentals-and-applications>
8. Морзе Н. Стан та перспективи навчання інформатики в закладах освіти України. *Інформаційні технології і засоби навчання* 2022. DOI: 10.33407/itlt.v92i6.5138
9. Морзе Н.В., Проценко Г.О Концепція навчання учнів інформатики у 5-9 класах загальноосвітніх навчальних закладах. URL: https://elibrary.kubg.edu.ua/id/eprint/897/1/N_Morze_H_Protsenko_IITNZ_3.pdf

THE METHODOLOGY OF TEACHING DATA CODING IN THE SCHOOL COMPUTER SCIENCE COURSE

Khramov O., Gaidus A.

Abstract. In the modern world, where programming is ubiquitous and considered one of the most fascinating professions, it is essential to have an engaging and comprehensible way to spark a child's interest in learning it. This article highlights the significance of steganography in the school computer science curriculum, placing a primary emphasis on its relevance and appeal to students. Contemporary approaches and teaching methods of steganography are examined, considering the advantages of this coding education method for children. An important aspect is the analysis of how steganography becomes a powerful tool for developing key skills in programming. Teaching programming through steganography incorporates modern technologies and educational trends. By encouraging computer science teachers to use steganography as a means to captivate students in programming, the article contributes to the development and implementation of effective teaching methods in school programs.

Keywords: Steganography; Education; Programming.