УДК 004.056.5

О.О. КУЗНЕЦОВ, д-р техн. наук, О.О. СТЕФАНОВИЧ,
Д.І. ПРОКОПОВИЧ-ТКАЧЕНКО, канд. техн. наук, К.О. КУЗНЕЦОВА

3D СТЕГАНОГРАФІЧНЕ ПРИХОВУВАННЯ ІНФОРМАЦІЇ

Вступ

Стеганографія, у широкому сенсі, це такий спосіб передачі закодованого інформаційного повідомлення, при якому приховується сам факт його існування [1, 2]. На відміну від криптографії, методи стеганографії дають можливість замінити несуттєві частки даних на конфіденційну інформацію так, щоб неможливо було запідозрити існування вбудованого таємного послання [1].

На сьогодні у зв'язку з розвитком обчислювальної техніки і нових каналів передачі інформації з'являються нові стеганографічні методи, в основі яких лежить приховування інформації в комп'ютерних файлах – контейнерах, які володіють високим рівнем природньої надмірності (фото- та відеозображення, аудіо-файли, текстові документи, тощо). Сутність приховування полягає в скритній заміні надмірних даних інформаційними повідомленнями, вилучити або навіть встановити факт наявності яких може тільки вповноважена особа, що має секретний стеганографічний ключ [1, 2].

Останніми роками з'явився та отримав розвиток новий напрям комп'ютерної стеганографії, який пов'язаний із приховуванням інформаційних повідомлень в штучно створених контейнерах, надмірність в який породжена технічними особливостями зберігання, обробки та/або передачі даних [3 – 14]. Такі методи «технічної» стеганографії набули поширення при приховуванні інформаційних повідомлень в різних за своєю природою штучних контейнерах. Зокрема, методи мережевої стеганографії у якості носія (контейнеру) використовують переданий по мережі пакет або сукупність пакетів даних, процедури приховування та вилучення інформаційних даних засновані на використанні особливостей функціонування мережевого стеку протоколів передачі даних [3 – 6]. Побудову прихованих кластерних каналів засновано на використанні особливостей зберігання даних у сучасних файлових системах [7 – 9]. Існують і інші напрямки розвитку технічної стеганографії, зокрема, які засновані на використанні штучної надмірності тривимірних (3D) моделей об'єктів [10 – 14]. Останніми роками тривимірні моделі набули значного поширення та розповсюдження в різних застосуваннях, зокрема при обробці медичних даних, музейних експонатів та зразків культурної спадщини, імітаційних моделей промислових зразків та виробничих процесів, комп'ютерних ігор, тощо. При цьому стеганографічні методи застосовують для захисту авторського права тривимірних моделей, скритого приховування певної інформації, захисту від випадкових викривлень або певних похибок, тощо. Отже дослідження нових методів приховування даних із використанням 3D-технологій є перспективним напрямком сучасних досліджень.

В цій роботі розвивається новий підхід, запропонований в [15 – 17], щодо стеганографічного приховування даних в твердотільних об'єктах за допомогою технології 3D-друку. Сутність цього підходу полягає в перетворенні інформаційного повідомлення на 3D-модель, яку розміщують всередині 3D-моделі контейнеру із подальшим роздрукуванням (створенням, вирощуванням). Зовнішній вигляд отриманого твердотільного об'єкту, його експлуатаційні та естетичні властивості не змінюються в процесі вбудовування інформаційного повідомлення. Крім того, видалити або спотворити приховане повідомлення без руйнування або значного пошкодження виробу неможливо, отже маємо нову технологію стеганографічного захисту інформації як для скритної її передачі, так і для забезпечення авторського права, тощо.

1. Приховування інформаційних даних

В роботах [15 – 17] було запропоновано прототип комплексу стеганографічного захисту, в якому інформаційні дані приховуються в процесі пошарового створення (вирощування)

твердотільного об'єкта при використанні різних технологій 3D-друку. Основна ідея полягає у вбудовуванні (стеганографічному кодуванні) інформаційних даних в цифрову 3D-модель, за якої в подальшому пошарово створюється (роздруковується) твердий об'єкт (готовий виріб або прототип для подальшого доведення). Процес вбудовування реалізується з використанням секретних ключових даних, що виключає несанкціонований доступ до інформації, що захищається, порушення її цілісності, автентичності та конфіденційності. Крім того, застосовані методи стеганографічного захисту не повинні знижувати експлуатаційних, естетичних та будь-яких інших властивостей готового виробу, оскільки технології, що застосовуються для нанесення шарів, не модифікуються. Отже, пропонований комплекс інваріантний способу пошарового вирощування, тобто може комплектуватися довільними периферійними пристроями 3D-друку різних фірм виробників з будь-якими матеріалами і принципами пошарового створення [15 – 17].

Головна ідея приховування даних полягає в розміщенні інформаційного повідомлення у середині довільної комп'ютерної моделі фізичного об'єкту, яку можна роздрукувати на 3D принтері – іграшці, статуетці, сувенірі тощо. Інформаційне повідомлення подається у двійковому вигляді і кожен біт перетворюється на певний фрагмент фізичної моделі. Як приклад (рис. 1), кожен біт може кодуватися тривимірним кубом встановленого розміру, причому наповненість куба відповідає вмісту відповідного біту: «0» відповідає пустому (не заповненому) кубу, «1» – заповненому. Інформативний признак може бути і іншим, наприклад заповнення різними матеріалами, або одним матеріалом але із різною щільністю, орієнтованістю, формою елементарних «бітових» фізичних моделей, тощо.

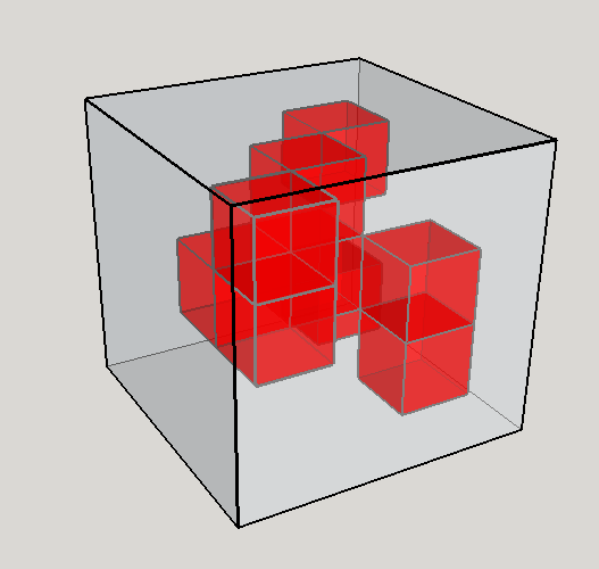


Рис. 1. Схематичне подання стеганографічного кодування – перетворення інформаційного повідомлення на фрагмент комп'ютерної моделі фізичного об'єкту

Для автоматизованого кодування було застосовано спеціалізоване програмне забезпечення OpenSCAD, яке призначене для створення твердотільних тривимірних САПР-об'єктів. Воно є вільним і доступним під операційними системами Linux / UNIX, Microsoft Windows і Apple Mac OS X.

На рис. 2 продемонстровано кодування інформаційного повідомлення «Tomorrow never comes until it's too late». Кожен символ повідомлення подається у бінарному вигляді за допомогою коду ASCII. Далі, для обраної кубічної форми «бітових» моделей та розміру 3x3x3 міліметри виконується кодування кожного інформаційного біту. Для цього було розроблено програмне забезпечення, яке формує відповідний вихідний код, що розміщується у робочому

полі програми OpenSCAD. На рис. 2 всі елементарні фізичні моделі згруповано у контейнер розміром 11x3x10 відповідних кубів (ці налаштування додатково встановлюються у розробленому програмному забезпеченні).

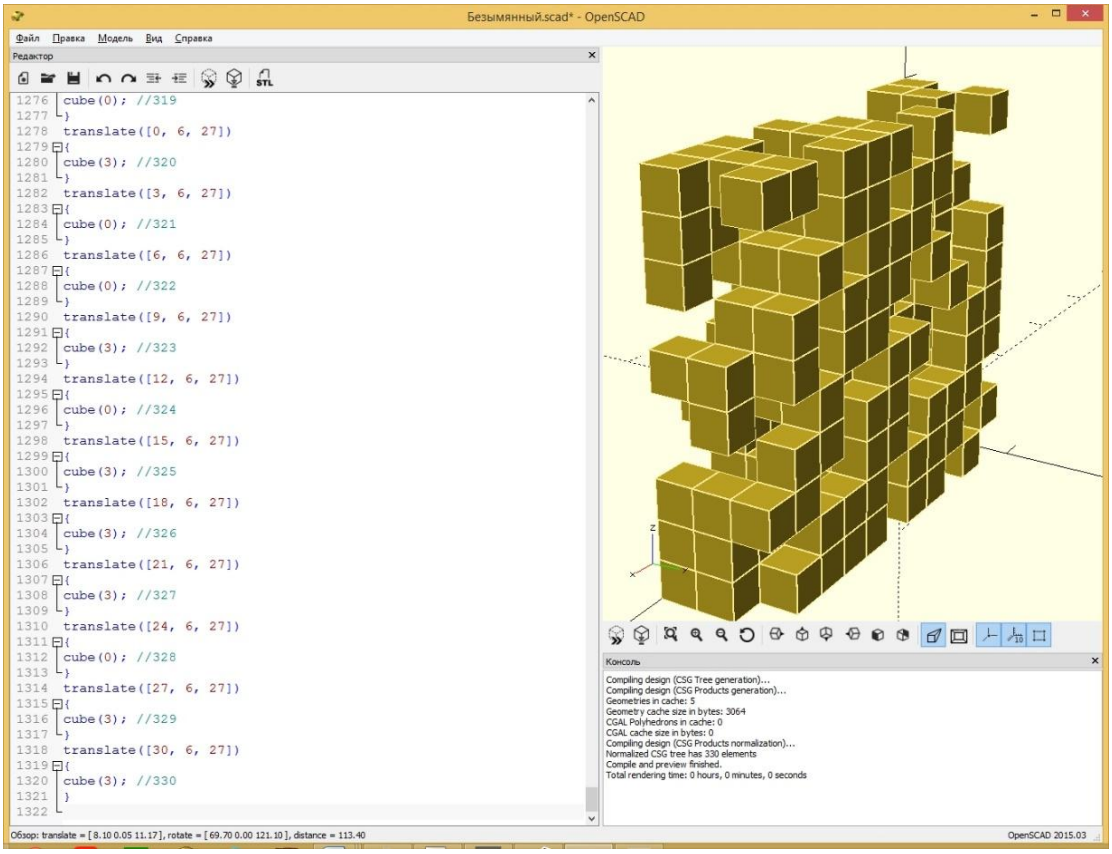


Рис. 2. Приклад стеганографічного кодування за допомогою програми OpenSCAD

На рис. 2 зліва можна побачити вихідний код, в якому задаються координати та розмір тривимірних кубів – носіїв інформаційних бітів. Праворуч наведено створену тривимірну модель інформаційного повідомлення, яка відповідає всім заданим вхідним параметрам.

Таким чином, в результаті стеганографічного кодування інформаційне повідомлення спочатку перетворюється у трьохвимірну булеву матрицю, яка, в свою чергу, перетворюється в комп'ютерну модель фізичного об'єкту. Сформована комп'ютерна модель булевої матриці розміщується у середині основної моделі контейнеру так, щоб її краї не виходили за межі зовнішнього тіла, як це схематично наведено на рис. 3. При цьому застосовувалося спеціалізоване програмне забезпечення MakerBot Desktop з технологій 3D-друку.

Розмістити таку матрицю в середині іншої моделі можна різними способами, наприклад:

- всі заповнені куби під час друку на 3D принтері заповнювати іншим кольором;
- всі заповнені куби під час друку на 3D принтері залишати порожніми.

Недоліком другого способу є зменшення кінцевої ваги тіла, що при детальному аналізі може видати факт наявності таємного повідомлення. Заповнення бітів іншим кольором (або, наприклад, іншим матеріалом) зменшує ймовірність виявлення прихованого повідомлення, але збільшує складність його зчитування.

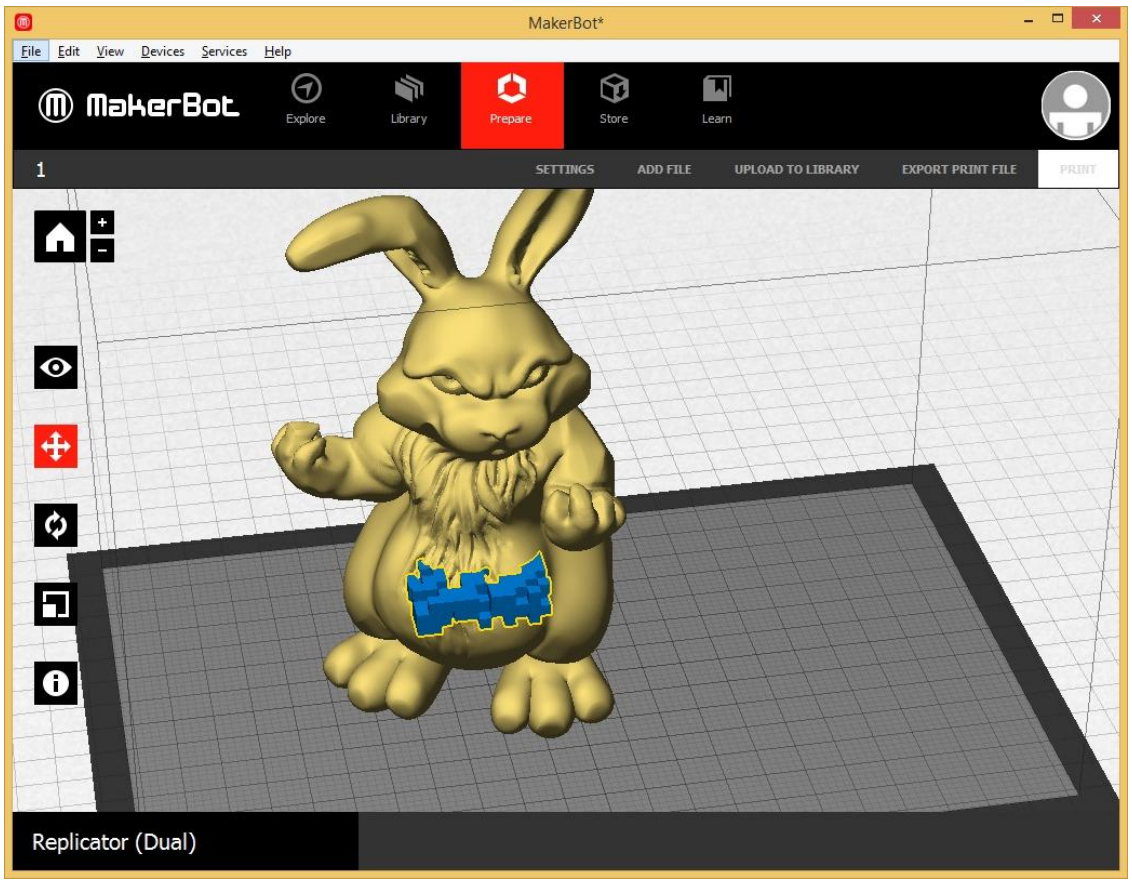


Рис. 3. Розміщення тривимірної моделі інформаційного повідомлення
у середині основної моделі контейнеру

На рис. 4 показаний процес пошарового створення твердотільного об’єкту-контейнеру із вбудованим інформаційним повідомленням. Ліворуч на рисунку показана схематична візуалізація процесу друку, праворуч – фотографія реального процесу на 68 шарі 3D-друку, який було виконано із застосуванням 3D принтеру «Flashforge Creator Dual». На рис. 5 показано завершення друку 3D-моделі та готовий виріб із вбудованим повідомленням.

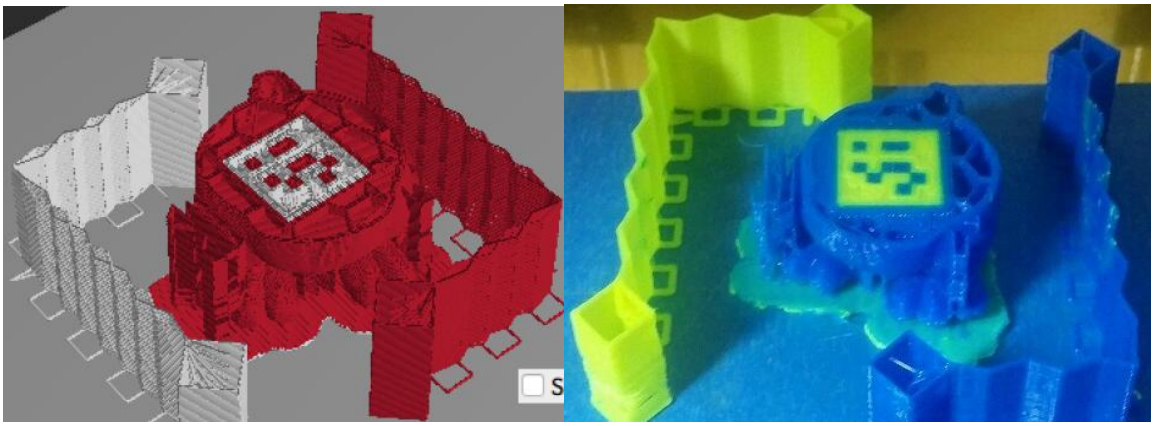


Рис. 4. Пошарове створення твердотільного об’єкту-контейнеру
із вбудованим інформаційним повідомленням

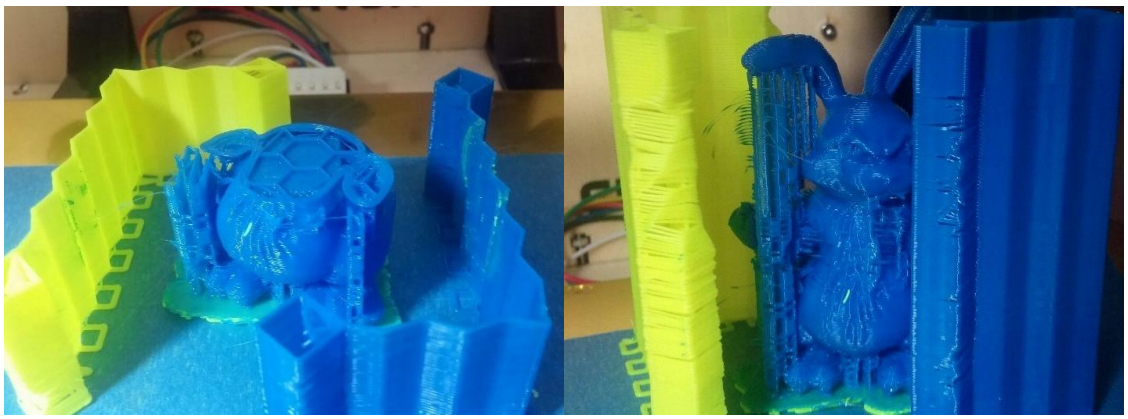


Рис. 5. Завершення друку та готовий виріб із вбудованим повідомленням

2. Вилучення інформаційних даних

Процес вилучення вбудованих даних здійснюється за допомогою сканування отриманого твердотільного об'єкту. Витягнуті сканером дані піддаються стеганографічному декодуванню з використанням секретних ключових даних. На цьому етапі забезпечуються різні послуги безпеки, наприклад, цілісність, автентичність, причетність, конфіденційність, тощо. Для підвищення достовірності (завадостійкості) вбудовані дані додатково піддаються надмірному кодуванню, яке дозволяє з заданою вірогідністю виявляти і/або виправляти помилки, що виникли в процесі пошарового друку/сканування. Пропонований комплекс може використовувати в різних областях: для прихованої передачі інформаційних повідомлень із забезпеченням різних послуг безпеки (цілісності, автентичності, причетності, конфіденційності та ін.). Видалення, спотворення або модифікація вбудованих даних неможливі без фізичного руйнування готового виробу, тобто пропонований комплекс ідеально підходить для забезпечення достовірності пошарово вирощених виробів, захисту їх від несанкціонованого копіювання та недобросовісних підробок, забезпечення авторського права, тощо [1, 2].

Слід відмітити, що на сьогодні день ще не розроблено надійних засобів вилучення інформаційних даних [15 – 17]. Саме невизначеність конкретної процедури вилучення вбудованих даних за допомогою сканування отриманого твердого тіла є головним невирішеним питанням з приводу практичного застосування запропонованого комплексу 3D-стеганографії. Зокрема, система може комплектуватися різними периферійними пристроями 3D-друку, які застосовують різні технології пошарового вирощування та різний за своїми фізичними властивостями вихідній матеріал. Відповідні процедури сканування отриманого твердого тіла повинні враховувати ці особливості і, по можливісті, забезпечувати надійне та безпомилкове вилучення прихованих даних.

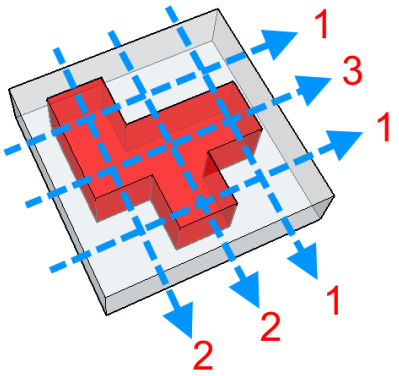
Одним із можливих напрямків у вирішенні зазначених проблем є застосування лазерних сканерів, в яких потік когерентного, монохроматичного, поляризованого і вузьконаправленого потоку випромінювання, що утворює паралельний пучок, зменшується в результаті поглинання в середовищі в деяку заздалегідь обумовлену кількість разів. Для встановлення принципової можливості зчитування прихованого повідомлення з 3D-моделі, що пошарово створена (надрукована) на 3D-принтері без пошкодження самої моделі або повідомлення, було проведено наступні експериментальні дослідження.

2.1. Опис лабораторної установки та умов проведення експериментальних досліджень

Головна ідея проведення експерименту полягає в вузьконаправленому опромінюванні готового виробу (із вбудованим повідомленням) за різними кутами та напрямками, достатніми для однозначного визначення внутрішньої структури виробу. При цьому як вихідні дані

враховуються значення інтенсивності випромінювання, що зменшуються в результаті поглинання.

При кодуванні інформаційних бітів пустими та заповненими кубами схема опромінення готового виробу може бути подана у спрощеному вигляді як на рис. 6 (ліворуч). В кінці стрілок вказане умовне значення результату вимірювання зменшення інтенсивності випромінювання (пропорційно до товщини заповненого матеріалом об'єкту). Праворуч на цьому ж рисунку подано значення інформаційних бітів, які, як очікується, буде вилучено із твердотільного об'єкту.



1	0	0
1	1	1
0	1	0

Рис. 6. Спрощена схема опромінення готового виробу (ліворуч)
та очікуваний результат вилучення даних (праворуч)

Оскільки ніяких інших відомостей щодо внутрішньої структури виробу немає, розміщення заповнених фрагментів (і відповідних бітів) повинне враховувати однозначність вилучення тільки за результатами вимірювання (зображені на рисунку ліворуч результати вимірювання мають два можливі рішення, одне з яких не співпадає із наведеним праворуч). Таке розміщення, фактично, є номограмою, яку застосовують при формуванні японських кросвордів.

Для спрощення умов проведення експерименту було виготовлено просту фізичну модель у формі сходинок із ABS-пластика жовтого та синього кольорів. Така форма дозволяє швидко змінювати товщину заповненого матеріалом об'єкту (рис. 7). Фактично, маємо шість різних значень, які умовно відповідають наступним інформаційним бітовим послідовностям:

- без заповнення – бітова послідовність (00000);
- одне заповнення (перша сходинка) – бітова послідовність (10000);
- два заповнення (друга сходинка) – бітова послідовність (11000);
- три заповнення (третя сходинка) – бітова послідовність (11100);
- чотири заповнення (четверта сходинка) – бітова послідовність (11110);
- п'ять заповнень (п'ята сходинка) – бітова послідовність (11111).

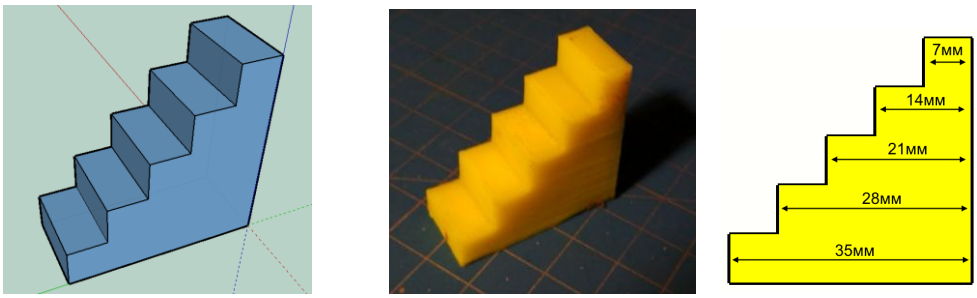


Рис. 7. Спрощена фізична модель інформаційних даних

Для проведення досліджень було застосовано оптичні прилади з лабораторії кафедри фізичної оптики фізичного факультету. Відомо, що кожен матеріал має свій показник

поглинання – величина, зворотня відстані, на якому потік монохроматичного випромінювання, що утворює паралельний пучок, зменшується в результаті поглинання в середовищі в деяку заздалегідь обумовлену кількість разів. Показник поглинання визначається властивостями речовини і в загальному випадку залежить від довжини хвилі λ світла, що поглинається. Ця залежність є спектром поглинання речовини.

В якості монохроматичного випромінювання використовувалися наявні у лабораторії лазери видимого спектру, що відрізнялися довжиною хвилі та потужністю випромінювання. Пучок лазерного світла проходив через досліджуване тіло. Випромінювання, що не поглиналося пластиком, потрапляло на закріплений з іншої сторони фоторезистор – фотоелектричний напівпровідниковий приймач випромінювання, принцип дії якого ґрунтується на ефекті фотопровідності (явищі зменшення опору напівпровідника у разі збудження носіїв заряду світлом). Для зчитування і подальшої обробки даних був використаний мікроконтролер «Arduino UNO». На фоторезистор подавалася напруга 5 В. В залежності від степені збудження фотоелементу змінювався його опір. Мікроконтролер робив заміри зміни напруги кожні 40 мс, оцифровував їх та відправляв на персональний комп’ютер.

Схематично лабораторну установку зображено на рис. 8. Вона включає досліджуване тіло із пластику у вигляді сходинок (рис. 7), лазер як джерело вузьконаправленого опромінювання готового виробу, фоторезистор та мікроконтролер, для зчитування розсіяного випромінювання. На рис. 9 наведено фотографію зібраної лабораторної установки та збільшену фотографію процесу оптичного опромінювання.

Для прийому та відображення поточного значення фоторезистора, а також розрахунку середнього арифметичного із виконаних замірів застосовувалося розроблене програмне забезпечення. Оскільки спектр поглинання речовини був невідомий для виготовленого зразка, у досліді використовувалися всі наявні в лабораторії лазери із різними характеристиками (див. табл. 1).

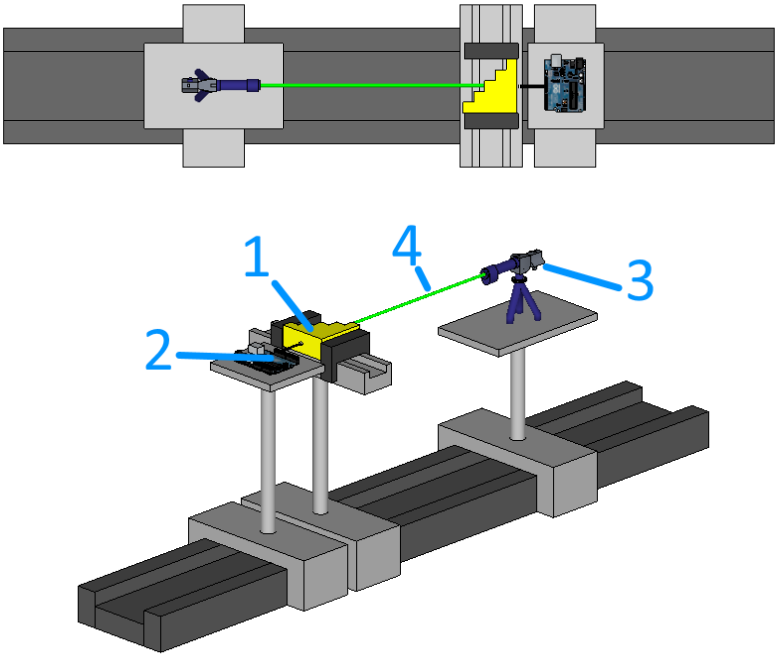


Рис. 8. Схема лабораторної установка: 1 – досліджуване тіло із пластику у вигляді сходинок; 2 – фоторезистор та мікроконтролер, що зчитує дані; 3 – лазер; 4 – лазерне випромінювання

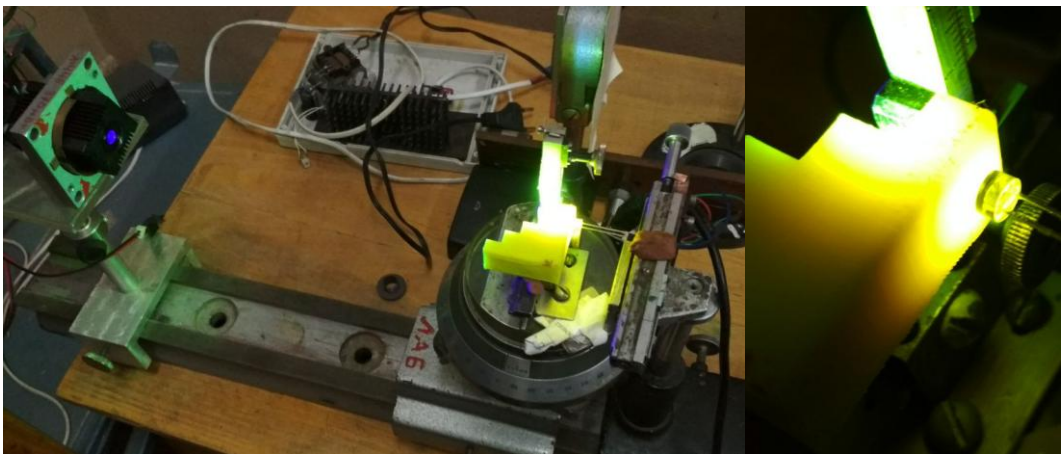


Рис. 9. Фотографія зібраної лабораторної установки (ліворуч)
та збільшена фотографія процесу опромінювання (праворуч)

Таблиця 1

Характеристики лазерів, які застосовувалися в експерименті

Номер	Довжина хвилі, нм	Потужність, мВт	Видимий колір
1	532	100	Зелений
2	650	25	Червоний
3	405	90	Фіолетовий
4	445	160	Синій
5	650	25	Червоний

Кожним лазером просвічувалися різні товщини досліджуваного тіла та робились заміри відсотку світла, що пройшов крізь дану ділянку тіла. Експеримент проводився за відсутності будь-яких інших ввімкнених джерел світла, тобто у темряві. Крок зміни товщини досліджуваного тіла 7 мм був обраний враховуючи товщину лазерного пучка, товщина якого знаходиться у межах 5-6 мм. Для коректності досліду, пучок лазерного випромінювання повинен повністю потрапляти на ділянку із однією товщиною. Мікроконтролер має вольтметр, що виявляє зміну напруги з кроком 5/1024 вольта, тому під час оцифровки аналогового значення отримуємо число від 0 (світло не потрапляє взагалі) до 1024 (максимальна кількість світла, яку може розпізнати фоторезистор).

2.2. Результати експерименту та їх інтерпретація

Отримані результати експериментальних досліджень (усереднені за виконаними вимірюваннями) зведено у табл. 2.

За наведеними у таблиці даними можна зробити висновок, що зразок із жовтого пластику найменше поглинає зелене лазерне випромінювання із довжиною хвилі λ=532 нм. Хоч обидва зразки виготовлені з однакового виду пластику, із-за різниці кольору вони мають зовсім різні показники поглинання. Тіло, що виготовлено з синього пластику, має значно більший показник поглинання. Навіть на мінімальній товщині тіло з синього пластику поглинуло світло з кожного лазера, якого б вистачило для визначення найменшої товщини.

Таблиця 2

Результати вимірювань

Зразок жовтого кольору						
Номер лазера	Товщина ділянки, мм					
	0	7	14	21	28	35
1	1024	1001	775	162	33	4
2	1024	995	426	65	6	0
3	1024	995	97	5	1	0
4	1024	998	500	59	5	0
5	1024	995	336	57	4	0
Зразок синього кольору						
Номер лазера	Товщина ділянки, мм					
	0	7	14	21	28	35
1	1024	0	0	0	0	0
2	1024	0	0	0	0	0
3	1024	0	0	0	0	0
4	1024	0	0	0	0	0
5	1024	0	0	0	0	0

Отримані результати для зразка матеріалу жовтого кольору свідчать, що для різної товщини матеріалу маємо різні значення інтенсивності випромінюванні і ці різниці досить суттєві. Отже, за результатами вимірювань принципово можливо встановити товщину матеріалу, та, відповідно, визначити вміст прихованих інформаційних бітів.

Висновки

В роботі досліджено новий напрямок технічної стеганографії, який пов'язаний із приховуванням інформаційних даних в процесі пошарового створення (вирощування) твердотільного об'єкта при використанні різних технологій 3D-друку. Інформаційні дані перетворюються в цифрову 3D-модель елементарних фізичних об’єктів, які розміщуються всередині 3D-моделі виробу-контейнеру. Після роздрукування твердий об'єкт фізично містить приховану інформацію, яку неможливо видалити або спотворити без пошкодження контейнеру. Крім того, застосовані методи не знижують експлуатаційних, естетичних та будь-яких інших властивостей готового виробу, оскільки технології, що застосовуються для нанесення шарів, не модифікуються, приховування є інваріантним способу пошарового вирощування, тобто можуть застосовуватися різні пристрої 3D-друку з будь-якими матеріалами і принципами пошарового створення.

Процес вилучення вбудованих даних здійснюється за допомогою сканування отриманого твердотільного об’єкту. Саме невизначеність конкретної процедури сканування отриманого твердого тіла є головним невирішеним питанням з приводу практичного застосування запропонованого комплексу 3D-стеганографії.

За результатами експериментальних досліджень встановлено принципову можливість зчитування прихованого повідомлення з 3D-моделі із застосуванням лазерних сканерів, в яких потік когерентного, монохроматичного, поляризованого і вузьконаправленого потоку випромінювання, що утворює паралельний пучок, зменшується в результаті поглинання в середовищі в деяку заздалегідь обумовлену кількість разів. Отримані результати для зразка матеріалу жовтого кольору свідчать, що для різної товщини маємо різні значення інтенсивності випромінюванні і ці різниці досить суттєві. Отже, за результатами вимірювань принципово можливо встановити товщину матеріалу, та, відповідно, визначити вміст прихованих інформаційних бітів.

Наведені результати експериментальних досліджень не є остаточними та потребують подальшого уточнення та відтворення. Зокрема, невирішеними є питання обрання типу і характеристик лазеру, погодженість цих характеристик із властивостями матеріалів

твердотільного об’єкту, налаштування фоторезисторів, тощо. Крім того, перспективним, на нашу думку, є проведення експериментальних досліджень із іншими видами випромінювання, видами та кольорами пластику.

Список літератури:

1. Katzenbeisser S., Petitcolas F. A. Information Hiding Techniques for Steganography and Digital Watermarking. – Norwood, MA, USA: Artech House, 2000. – 220 p.

2. Petitcolas F. A. P., Anderson R. J. and Kuhn M. G. Information hiding-a survey // Proceedings of the IEEE. – vol. 87, no. 7. – pp. 1062-1078. – Jul 1999.

3. Mazurczyk W., Smolarczyk M., Szczypiorski K. Retransmission steganography and its detection // Soft Computing, vol. 15, no. 3, pp. 505-515, 2011.

4. Nair A. S., Kumar A., Sur A. and Nandi S. Length based network steganography using UDP protocol // IEEE 3rd International Conference on Communication Software and Networks, Xi'an, 2011, pp. 726-730.

5. Ahsan K. and Kundur D. Practical data hiding in TCP Lip // ACM Workshop on Multimedia and Security, 2002, [On-line]. Internet: http://ee.tamu.edu/deepalpdf/ acm02.pdf.

6. S. H. Sellke, C. Wang, S. Bagchi and N. B. Shroff, "TCP/IP Timing Channels: Theory to Implementation", pp. 2204-2212, 2009.

7. Khan H., Javed M., Khayam S.A., Mirza F. Designing a cluster-based covert channel to evade disk investigation and forensics // Computers & Security. – Volume 30, Issue 1. – January 2011. [On-line]. Internet: https://www.sciencedirect.com/science/article/pii/ S016740481000088X

8. Khan H., Javed M., Khayam S.A., Mirza F. Evading Disk Investigation and Forensics using a Cluster-Based Covert Channel / National University of Science & Technology (NUST). – Islamabad 44000, Pakistan. [On-line]. Internet: https://www.sigsac.org/ccs/CCS2009/pd/abstract_17.pdf

9. Morkevičius N., Petraitis G., Venčkauskas A., Čeponis J. Covert Channel for Cluster-based File Systems Using Multiple Cover Files // Information Technology and Control, 2013, Vol.42, No.3. pp. 32. [On-line]. Internet: http://itc.ktu.lt/index.php/ITC/article/ view/3328

10. Rani R. and Deep G. Digital 3D barcode image as a container for data hiding using steganography // 4th International Conference on Signal Processing, Computing and Control (ISPCC), Solan, 2017. – P. 325-330.

11. Sun Z. , Z. m. Lu and Z. Li. Reversible Data Hiding for 3D Meshes in the PVQ-Compressed Domain // International Conference on Intelligent Information Hiding and Multimedia, Pasadena, CA, USA, 2006, pp. 593-596.

12. Wang K., Lavoué G., Denis F., Baskurt A. and He X. A Benchmark for 3D Mesh Watermarking // Shape Modeling International Conference, Aix-en-Provence, 2010. – P. 231-235.

13. Motwani M. C., Bryant B. D., Dascalu S. M. and F. C. Harris Jr. 3D Multimedia Protection Using Artificial Neural Network // 7th IEEE Consumer Communications and Networking Conference, Las Vegas, NV, 2010. – P. 1-5.

14. Vasić B. Annotation of cultural heritage 3-D models by robust data embedding in the object mesh // 22nd Telecommunications Forum Telfor (TELFOR), Belgrade, 2014. – P. 842-849.

15. Кузнецов А.А., Коваленко О.Ю. Стеганографическая защита информации с использованием 3D-печати // Інформаційна безпека держави, суспільства та особистості : зб. тез доповідей Всеукр. наук.-практ. конф., 16 квітня 2015 р. – Кіровоград : КНТУ, 2015. – С. 91-92.

16. Кузнецов О.О. Лекція 12: Технічна стеганографія. Приховування даних в твердотільних об'єктах за допомогою 3D-друку : Електронний конспект лекцій за дисципліною «Стеганографія». – Харків : Харк. нац. ун-т ім. Каразіна, 2016. – 14 с.

17. Коваленко О.Ю. Розробка лабораторного комплексу технічної стеганографії з використанням тривимірного друку : Пояснювальна записка до дипломної роботи бакалавра (Керівник О.О. Кузнецов). – Харків : Харк. нац. ун-т ім. Каразіна, 2015. – 47 с.

Харківський національний
університет імені В.Н. Каразіна;
АТ «Інститут інформаційних технологій», Харків

Надійшла до редколегії 09.11.2018