Methods of information systems protection

УДК 004.07 **doi:** https://doi.org/10.20998/2522-9052.2022.1.15

Д. Г. Волошин, С. С. Бульба

Національний технічний університет “Харківський політехнічний інститут”, Харків, Україна

ІНТЕЛЕКТУАЛЬНИЙ МЕТОД ВИЗНАЧЕННЯ СПУФІНГУ БПЛА

Анотація. У роботі представлений інтелектуальний метод виявлення спуфінгу БПЛА. Відмінною особливістю методу є використання технології розрахунку субтраєкторії на основі субтраєкторій візуальної одометрії та GPS-положень у ковзаючому вікні з урахуванням інтелектуальної оцінки оптичного потоку та формування дескрипторів «Его-переміщення» БПЛА. У ході дослідження проведено аналіз та порівняльні дослідження широкого спектру методів спуфінгу БПЛА, виявлено найчастіше рекомендовані та практично використовувані методи. Зроблено висновок про актуальність проблематики GPS спуфінгу. Проведено аналіз методів захисту від GPS спуфінгу БПЛА. Виявлено перспективні напрямки інтелектуального виявлення спуфінгу БПЛА з використанням методів та засобів візуальної одометрії. У ході дослідження методів фіксації вхідних даних запропоновано підхід оцінки оптичного потоку з використанням ковзного вікна. При цьому аргументовано доведено необхідність інтелектуальної обробки вхідних даних. Оцінку оптичного потоку та формування дескрипторів проводилася з використанням рекурентних згорткових нейронних мереж. В результаті розроблено структурну схему методу виявлення спуфінгу БПЛА. Це дало змогу провести дослідження розробленого методу. Результати експерименту для двох сценаріїв спуфінгу показали ефективність оцінки положень не менше двох з трьох показників в умовах використання ковзаючих вікон розміром від 15 і вище, з годинною затримкою, що становить половину розміру вікна.

Ключові слова: спуфінг; БПЛА; ковзаюче вікно; оптичний потік; дескріптор.

Постановка проблеми

У сучасних умовах використання безпілотних літальних апаратів (БПЛА) в більшості випадків їхнє управління виконується з використанням глобальних навігаційних супутникових систем (*GNSS*), а також з використанням глобальної системи позиціонування (*GPS*). Однак, в умовах зон підвищеного ризику, використанні системи навігації піддаються ряду ризиків. Наприклад, з деяких джерел [1, 2] відомо, що *GPS* схильна до ризику навмисних і ненавмисних атак і перешкод. Серед навмисних атак можна відзначити глушіння і різноманітні підміни. Оскільки підміни виконуються, як правило, непомітно, а також викликають найбільші втрати саме вони є найбільш серйозною загрозою. Проведений аналіз частіших випадків кібератак на БПЛА дозволив зробити висновок про підвищення числа зловмисних підмін шляхом спуфінгу *GPS*. Пов'язано це з тим, що за допомогою спуфінгу *GPS* можна успішно перехопити БПЛА, змінивши траєкторію польоту і пункт призначення без сповіщення користувачів БПЛА.

Ряд результатів досліджень показав успішність проведення подібних атак на БПЛА. Так, наприклад, у роботі [3] представлені результати експерименту з успішного спуфінгу *GPS*, змінами розташування БПЛА і прив'язки до часу. В [4] аргументовано описані можливі умови успішного спуфінгу та практичні рекомендації. В [5] описані результати практичного експерименту перехоплення БПЛА та його проведення у зазначену точку. У [6] представлені результати дослідження методу прихованого спуфінгу БПЛА, що забезпечують аргументоване теоретичне обґрунтування задач спуфінгу в інтегрованих середовищах глобальної системи *GPS*-позиціонування та інерційної навігаційної системи *INS*. Слід зазначити, що наведені приклади є лише незначною частиною доказів зростання популярності атак спуфінгу БПЛА, а також активного використання кібератак спуфінгу *GPS* БПЛА.

Проведені дослідження дозволили класифікувати основні технології спуфінгу *GPS* БПЛА та виділити з них основні методи: імітатори сигналів *GPS*, спуфери на основі простих приймачів, а також спуфери на основі складних приймачів.

До першої категорії можна віднести види імітаторів *GPS* сигналу, об'єднані інтерфейсом різної частоти. Цей вид спуфінгу дає змогу імітувати справжній сигнал *GPS*. Синхронізація помилкових сигналів із реальними у цьому методі не потрібна. Цей метод спуфінгу не складний у реалізації. Проте такі атаки виявляються штатними засобами захисту. Другий вид спуфінгу складніший. Вимагає, щоб *GPS*-приймач був пов'язаний з передавачем підробки. Це дозволяє виявити показники розташування, часу та координат супутників та синхронізує підроблені сигнали *GPS* із реальними. Цей вид спуфінгу порівняно з першим (імітатором сигналу *GPS*) виявити складніше. Третя категорія передбачає, що положення та швидкість фазового центру приймальної антени БПЛА-жертви точно відомі. І саме цей тип спуфінгу найнебезпечніший з погляду його виявлення. Для виявлення цього виду кіберзлочинів необхідно проведення додаткових досліджень та удосконалення методів захисту БПЛА від спуфінгу *GSM*.

Аналіз літератури [7-13] показав, що в даний час методи захисту від спуфінгу *GSM* можна розділити на методи автономного приймача глобальної супутникової навігаційної системи (*GRS*) і методи гібридного приймача позиціонування (*HPR*).

У методах *GRS* отриманий сигнал обробляється для визначення справжності (автентичності). Ці методи засновані на просторовій [7] та часовій [8] обробці, аналізі розподілу вихідних сигналів корелятора [9], захисті

від вторинних сигналів [10] та автономному контролі цілісності [11]. Одним із основних недоліків перерахованих методів є велика ймовірність помилки результуючого рішення у випадках використання зловмисниками сучасних методів обробки та обфускації сигналів, а також використання сучаснішого обладнання. У методах *HPR* для виявлення і запобігання спуфінгу *GPS* використовуються допоміжні дані про місцезнаходження БПЛА від додаткових систем і служб, таких як інерціальна навігаційна система (*INS*) [11], система стільникового зв'язку або *Wi-Fi* [11], а також систем позиціонування на основі візуальної одометрії [12].

Незважаючи на перспективність перелічених підходів та методів захисту, недоліки пов'язані з необхідністю постійного калібрування в інерційних навігаційних системах, складністю оцінки підроблених фреймів на об'єднаних виходах *GPS/INS*, а також можливою відсутністю засобів стільникового зв'язку та *Wi-Fi* у віддалених або важкодоступних місцях істотно знижують точність оцінки ситуації при виявленні спуфінгу. Крім того, зазначені допоміжні системи позиціонування синхронізуються за часом з використанням *GPS*, що також потребує резервування даних про час.

Окремо слід зазначити методи, які використовують у комплексі додаткові дані від засобів у системах позиціонування на основі візуальної одометрії та засобів візуальної картографії. У роботі [13] детально описані можливості використання даного підходу при отриманні даних від вимірювальних блоків, висотоміра і радара при навігації БПЛА. Водночас високі вимоги до обчислювальної потужності та вартості значною мірою звужують область використання зазначеного підходу на практиці.

У той же час, технічні засоби візуальної одометрії використовуються як допоміжні в процесі захисту від спуфінгу. Їхня робота не залежить від сигналів *GPS* та інших радіочастотних перешкод. Цей факт підтверджується авторами роботи [12], в якій запропоновано методику аналізу місцезнаходження при виявленні спуфінгу БПЛА.

Враховуючи представлені результати аналізу, доцільно вдосконалити методи гібридного приймача позиціонування (*HPR*) на основі аргументованого вибору вхідних даних візуальної одометрії, а також розвитку методів їх обробки. Зокрема пропонується використовувати дані щодо відносної траєкторії БПЛА для порівняння з абсолютною траєкторією, яку можна контролювати за допомогою *GPS*. У запропонованому методі відсутня залежність від низки засобів отримання вхідних даних (наприклад, інерційний вимірювальний блок, радар, висотомір та інші), що спрощує процес збирання та обробки даних. Також не розглядаються вхідні дані цифрової моделі рельєфу, супутникового зображення та інше, що знижує обчислювальне навантаження у системі.

1. Виявлення спуфінгу GSM з урахуванням методів візуальної одометрії

При формалізації методу виявлення спуфінгу БПЛА, що розробляється, важливими є обмеження на дані, відомі кіберзлочинцю, і використовуються ним для виконання деструктивних дій. У разі заміни *GSM* спуфер володіє даними про миттєве місце розташування об'єкта атаки, заздалегідь заданої траєкторії та пункт призначення БПЛА. Крім того, спуфер може генерувати і транслювати підроблені сигнали *GPS*, так, що траєкторія польоту БПЛА, що моделюється з підроблених даних про місцезнаходження *GPS*, збігається із заздалегідь заданою траєкторією. В результаті, коли позиції, отримані з підроблених сигналів *GPS*, показують заздалегідь задану траєкторію руху, атакований БПЛА слідує іншою, хибною, траєкторією, і прямує до помилкового пункту призначення. Таким чином, фактична траєкторія руху БПЛА, що прототипується на основі отриманих даних візуальної одометрії, не збігається із заздалегідь визначеною траєкторією.

Назвемо надалі фактичну траєкторію, якою перенаправляється атакований БПЛА істинною траєкторією атакованого БПЛА.

Пропонований метод виявлення спуфінгу БПЛА з використанням технологій візуальної одометрії заснований на можливостях отримання даних за допомогою штатних одометричних засобів (камери БПЛА, пасивних датчиків та ін.). У більшості практичних випадків це зображення, які включають до свого складу геотеги координат *GPS*. У разі підміни *GPS* фальшиві *GPS*-координати використовуються для геотегування зображень БПЛА. Також однією з можливостей запропонованого методу є удосконалений підхід порівняння двох траєкторій польоту, які одночасно визначаються для руху БПЛА за допомогою двох різних способів позиціонування. Перша траєкторія формується на основі *GPS*-координат, друга прототипується на основі зображень БПЛА, отриманих за допомогою візуальної одометрії.

Продемонструємо подане завдання у вигляді рис. 1. Припустимо, лінії *ABC* рис. 1 це наперед визначені траєкторії руху БПЛА, точка *A* – точка початку виконання польотного завдання, а точка *C* – точка призначення. Також припустимо, що в момент досягнення БПЛА точки *B*, кіберзлочинці проводять атаку спуфінгу *GPS*. Внаслідок цього БПЛА відхиляється від заданої траєкторії та входить у лінію *BC*' замість лінії *BC*. Як уже згадувалося, при використанні методу спуфінгу на основі складних приймачів, підроблені *GPS* положення продовжують вказувати на те, що БПЛА слідує заданій траєкторії (лінії *BC*). Проте, насправді, справжня траєкторія атакованого БПЛА відповідає лінії *BC*'. Отже, на рис. 1 лінія *ABC* є справжньою траєкторією атакованого БПЛА.

Порівняння цих траєкторій використовують для виявлення спуфінгу. Однак це порівняння не відповідає на питання про час та місце проведення атаки спуфінгу. Щоб усунути цей недолік замість порівняння повної істинної траєкторії БПЛА з реальною, пропонується використовувати зіставлення на основі ковзаючого вікна. Це дозволить локалізувати місце порівняння траєкторій у межах одного вікна і знаходити відхилення в заданих межах. Для цього вікно вздовж траєкторії руху БПЛА зсувається від позиції до позиції і в кожній позиції відбувається відбір *R*-зображень з геотегами (*R* – розмір вікна).

На рис. 1 ковзаючі вікна зображені у вигляді чотирикутників, що фіксують напрям траєкторії.

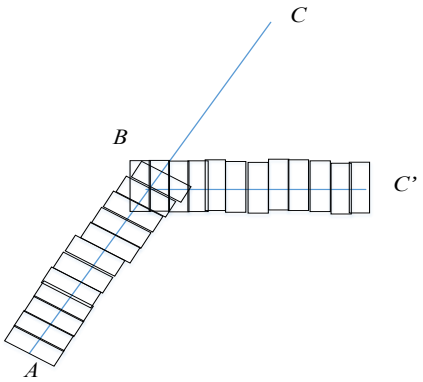


Рис. 1. Приклад заданих траєкторій руху БПЛА з хибною траєкторією (**Fig. 1.** Example of given UAV trajectories with the wrong trajectory)

У кожному вікні можна виділити дві субтраєкторії БПЛА. Перша – вилучена з позиції *GPS*, друга – із зображень, отриманих за допомогою засобів візуальної одометрії. У разі відсутності спуфінгу ці субтраєкторії співпадатимуть. Шляхом порівняння цих субтраєкторій можна визначити час та місце спуфінгу БПЛА. Ці субтраєкторії можна порівняти безпосередньо, використовуючи метричну відстань, або опосередковано, використовуючи дескриптор траєкторії, який описує траєкторію вектором ознак, що відображає різні характеристики траєкторії.

1.1. Розрахунок траєкторії з використанням даних візуальної одометрії. Траєкторія об'єкта що рухається T, являє собою послідовність упорядкованих пар (t_i, P_i)

$$T = \{(t_1, P_1)\ldots(t_n, P_n)\}, \quad (1)$$

де P_i – вектор положення точки в момент часу; n – кількість позицій в T чи довжина T.

У i-му положенні БПЛА та в межах W_i ковзаючого вікна БПЛА можуть бути призначені дві траєкторії завдовжки R (R – розмір вікна). Це вікно переміщається вздовж траєкторії руху БПЛА, і в кожній i-й позиції БПЛА будуть обрані R зображень з геотегами числа зображень від $i-(R-1)/2$ до $i+(R-1)/2$. Всередині W_i перша субтраєкторія вилучається з *GPS*-положень від $GPS_{i-(R-1)/2}$ до $GPS_{i+(R-1)/2}$, які використовуються при геотегуванні зображень БпЛА:

$$GPST_i = \{(t_j, GPS_j)\ldots(t_{j+k-1}, GPS_{j+k-1})\}; \quad j = i-(k-1)/2. \quad (2)$$

Позначимо траєкторію як $GPST_i$. Крім того, друга субтраєкторія розраховується на основі даних, отриманих із засобів візуальної одометрії, зокрема з використанням положення камери від $CAM_{i-(R-1)/2}$ до $CANM_{i+(R-1)/2}$. В межах ковзаючого вікна:

$$CAMT_i = \{(t_j, CAM_j)\ldots(t_{j+k-1}, CAM_{j+k-1})\}; \quad j = i-(k-1)/2, \quad (3)$$

де $CAMT_i$ – траєкторія камери.

Слід зазначити, що формалізація траєкторії $GPST_i$ у кожному ковзаючому вікні є не складним технічним завданням, яке виконується з використанням штатних засобів моделювання.

Однак розрахунок траєкторії $CAMT_i$ з використанням даних візуальної одометрії потребує використання додаткових знань. Візуальна одометрія це процес збору та оцінки даних про тривимірну зміну положення об'єкта в просторі з використанням необхідного обладнання (камер, датчиків та ін.).

Так само слід зауважити, що у випадку візуальної одометрії відносне положення камери можна оцінити або за допомогою характеристик зображення або на основі функціонально-орієнтованого методу.

Оцінюючи положення камери на основі характеристик зображення найчастіше використовуються значення інтенсивності оптичного потоку [14]. Оцінюючи з урахуванням функціонально-орієнтованого методу окремі особливості зображення виділяються і фіксуються описом. Потім цей опис використовується для порівняння точок та оцінки відносного положення між двома зображеннями [15]. У методі, що розробляється, пропонується за основу взяти дані про відносну субтраєкторію польоту БПЛА. При цьому для їх розрахунку використати підхід монокулярної візуальної одометрії. Для розрахунку та опису точкових об'єктів зображення, а також їх зіставлення з відповідними точками пропонується використовувати оператор масштабно-інваріантного перетворення елемента. Для обчислення $CAMT_i$ всередині кожного ковзаючого вікна необхідно оцінити відносну орієнтацію $R_{j,j+1}, B_{j,j+1}$, а також параметри між послідовними зображеннями I_j та I_{j+1}, $R_{j,j+1}$ представляє собою матрицю відносного повороту камери з позиції $j+1$ в позицію j, а $B_{j,j+1}$ – вектор відносного положення камери від позиції $j+1$ в позицію j. На рис. 2 представлена структура векторів, що описують положення БпЛА у просторі.

Після закінчення зазначених дій відносні положення камери в межах ковзаючого вікна фіксуються і перетворюються на систему координат моделі зображення відповідно до виразів:

$$\begin{aligned} &CAM_j = 0;\ j = p = i-(k-1)/2;\\ &CAM_j = B_{j-1,j};\ j = p+1;\\ &CAM_j = CAM_{j-1} + Y_{p,j-2}X_{p,j-2}B_{j-1,j};\\ &p+2 \le j \le i+(k-1)/2;\\ &Y_{p,j-2} = \varphi_{p,p+1}\ldots\varphi_{j-2,j-1};\\ &X_{p,j-2} = R_{p,p+1}\ldots R_{j-2,j-1}. \end{aligned} \quad (4)$$

де CAM_j – вектор положення j-го зображення в ковзному вікні; $\varphi_{j-2,j-1}$ – коефіцієнт масштабування перетворення відстані з тривимірної моделі $j-1$ в тривимірну модель $j-2$; $R_{j-2,j-1}$ – матриця відносного повороту камери з позиції $j-1$ у позицію $j-2$; $Y_{p,j-2}$ – коефіцієнт масштабування перетворення відстані з

тривимірної моделі $j-2$ в першу тривимірну модель $j=p$; $X_{p,j-2}$ – матриця відносного повороту камери з позиції $j-2$ на першу позицію $j=p$.

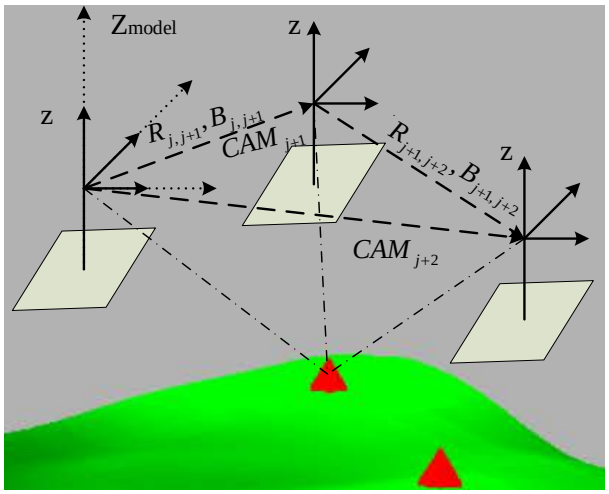


Рис. 2. Структура векторів, що описують положення БПЛА у просторі (**Fig. 2.** The structure of vectors describing the position of the UAV in space)

Одним з основних недоліків використання даних візуальної одометрії (особливо отриманих протягом тривалого часу) це сукупна похибка в оцінці положення камери. Ця похибка призводить до відхилення розрахункової траєкторії від реальної. Ця похибка збільшується зі збільшенням довжини траєкторії. Використання підходу ковзаючого вікна при оцінці основних показників зображення та розрахунку субтраєкторій БПЛА $CAMT_i$ дозволяє зменшити цю похибку.

1.2. Перетворення координат. Використовуючи для виявлення атаки спуфінгу БПЛА даних порівняння, $GPST_i$ і $CAMT_i$ необхідно враховувати фактор відмінності систем координат цих субтраєкторій. Відповідно перед їх порівнянням виникає необхідність в узгодженні даних про ці субтраєкторії та переведення їх в одну систему координат.

$GPST_i$ найчастіше представляється в наземній системі координат, наприклад *WGS 84* (*World Geodetic System* – являє собою астрономо-геодезичну-гравіметричну систему відліку, вписану у фігуру землі) або *UTM* (*Universal Transverse Mercator* – система картографічних проекцій, в якій поверхня Землі розділена на 60 витягнутих у меридіональному напрямку зон шириною 6 градусів). $CAMT_i$ оцінюється в системі координат моделі тривимірних зображень усередині ковзаючого вікна.

Ці системи координат мають різний початок, масштаб та орієнтацію осей.

За основу, як зразок, у роботі пропонується брати систему планіметричного позиціонування за допомогою *GPS*. У ковзаючому вікні система координат $GPST_i$ перетворюється на систему $CAMT_i$ з використанням двовимірної конформної моделі:

$$TGPST_i = X_0 + \rho R(\varphi) GPS_j, \qquad (5)$$

де φ – кут повороту, ρ – масштабний коефіцієнт, X_0 – вектор трансляції системи координат $GPST_i$ відносно системи координат $CAMT_i$.

У виразі (5) $TGPST_i$ – це перетворений вектор положення GPS_i у виразі (2). Для отримання φ, ρ та X_0 використовувалися відповідні координати першого і останнього зображення в межах ковзаючого вікна від GPS і засобів візуальної одометрії. Після перетворення $GPST_i$ трансформується $TGPST_i$:

$$TGPST_i = \left\{\left(t_j, TGPS_j\right),\ldots,\left(t_{j+k-1}, TGPS_{j+k-1}\right)\right\}; \quad j = i-(k-1)/2. \qquad (6)$$

Для підвищення точності даних векторів положення БпЛА в умовах просторового переміщення (Его-переміщення) доцільно використовувати додаткові методи та інструменти, зокрема методи штучного інтелекту. З цією метою в роботі пропонується вдосконалений метод інтелектуальної оцінки оптичного потоку та формування дескрипторів з використанням рекурентних згорткових нейронних мереж.

1.3. Оцінка оптичного потоку та формування дескрипторів з використанням рекурентних згорткових нейронних мереж. Для оцінки оптичного потоку та формування дескрипторів «Переміщення» БПЛА, а також прийняття рішення про атаку спуфінгу, у роботі пропонується використовувати мережеву структуру на основі рекурентних нейронних мереж. Структура методу проілюстровано на рис. 3.

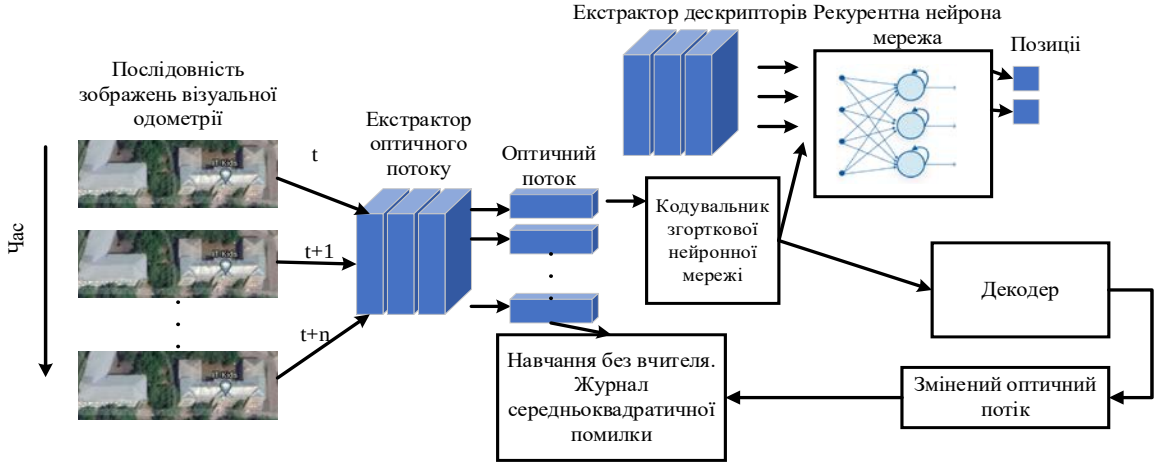


Рис. 3. Структура методу оцінки «Переміщення» з використанням рекурентних згорткових нейронних мереж (**Fig. 3.** The structure of the method of estimating "Movement" using recurrent convolutional neural networks)

Розглянемо докладніше представлений метод. У першій частині схеми пропонується використовувати мережу *PWC-Net*, запропоновану *NVIDIA Corporation* [16], щоб згенерувати поле оптичного потоку для послідовних пар ковзаючих зображень. *PWC-Net* – це компактна та ефективна модель згорткової нейронної мережі для оцінки поля оптичного потоку. Наступною сполучною ланкою представленої схеми є кодувальник та декодер оптичного потоку. Кодер повинен вивчити приховане представлення оптичного потоку та виконати генерацію його. Декодер з архітектурою, що є зворотньою кодувальнику, повинен відновлювати поле оптичного потоку так щоб кодер можна було навчати окремо неконтрольованим чином. Процес кодування та декодування показаний на рис. 4.

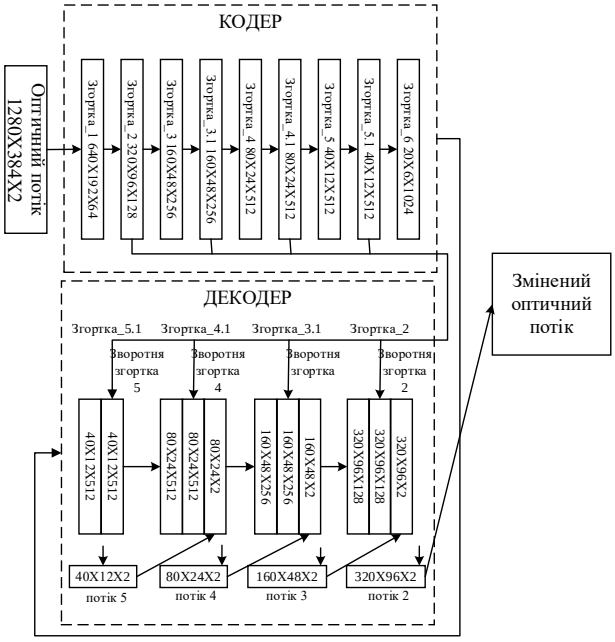


Рис. 4. Структурна схема процесу кодування та декодування (**Fig. 4.** Block diagram of the encoding and decoding process)

Кодер складається з 9 згорткових шарів, за кожним з яких слідує функція активації *Rectified Linear Unit (ReLU).* Для ініціалізації використовується метод *Xavier*. Кодер генерує підпростір оптичного потоку з 1024 каналами, кожен з роздільною здатністю 20×6. Потім підпростір оптичного потоку відновлюється в декодері з чотирма рівнями декодування, за кожним з яких слідує операція підсумовування та підвищення дискретизації. Візьмемо приклад першого рівня декодування, шар «Зворотнч згортка 5» деконволюціонує тензор (20×6×1024), створений «Згортка_6», і генерує новий тензор розміром 40×12×512. Потім він складається з тензором, згенерованим шаром «Згортка_5.1» розміром 40×12×512, для генерації нового тензора розміром 40×12×1024. При цьому використовується згортковий шар "потік 5", щоб згенерувати відновлений оптичний потік (40×12×2). Відновлений оптичний потік піддається підвищуючої дискретизації за допомогою білінійної інтерполяції для використання на наступному рівні декодування. З використанням чотирьох рівнів декодування підпростір оптичного потоку відновлюється до вихідного поля оптичного потоку. Під час навчання кодувальника використовується відновлене поле оптичного потоку як контрольний сигнал і порівнюється з вихідним полем оптичного потоку, згенерованого моделлю *PWC-Net.*

Слід зазначити, що у цьому використовуються піксельні квадрати втрат *RMSLE* для представлення перепусток. Функція втрат визначається як:

$$f_{nom} = \sum_i \left\| \log\left(\hat{\phi}^{(i)} + 1\right) - \log\left(\phi^{(i)} + 1\right) \right\|_2^2, \qquad (7)$$

де $\hat{\phi}^{(i)}$ та $\phi^{(i)}$ – відновлений вектор оптичного потоку *i*-го пікселя та вектор вхідного оптичного потоку.

Після кодувальника згорткової нейронної мережі, наступний елемент схеми – глибока рекурентна нейронна мережа. Вона призначена для проведення послідовного навчання, тобто для моделювання динаміки та відносин між послідовністю підпростору оптичного потоку. Рекурентна нейронна мережа в даний час є кращою мережею для обробки даних часових рядів і широко використовується в багатьох галузях [17]. У роботі використовується мережа з довгою короткостроковою пам'яттю (*LSTM*), яка здатна досліджувати довгострокові залежності. Таким чином, розроблений метод оцінки «Его-переміщення» з використанням рекурентних згорткових нейронних мереж, відмінною особливістю якого є комплексне використання рекурентних згорткових нейронних мереж при дослідженні малорозмірного простору оптичного потоку та дескрипторів гістограми напрямку переміщення БПЛА, що дозволило врахувати особливості «Его-переміщення»

1.4. Порівняння субтраєкторій камери та *GPS*. Для оцінки значень даних двох субтраєкторій необхідно визначитися з додатковим показником порівняння. У роботі пропонується використовувати показник суми евклідових відстаней між відповідними точками $CAMT_i$ та $TGPST_i$. Аналітичний вираз для розрахунку суми евклідових відстаней між точками траєкторії є таким:

$$COPMPR\left(CAMT_i, TGPST_i\right) = \\ = \sum_{j=i-(k-1)/2}^{i+(k-1)/2} d\left(TGPS_j, CAM_j\right), \qquad (8)$$

де $d\left(TGPS_j, CAM_j\right)$ – евклідова відстань між CAM_j та $TGPS_j$. На рис. 5 представлена ілюстрація евклідова відстані між відповідними точками CAM_j та $TGPS_j$ в межах ковзаючого вікна з п'яти точок. На цьому рисунку точка С' є початковою точкою спуфінгу БПЛА і точкою його перенаправлення в результаті *GPS* спуфінгу, що записується в $CAMT_i$. Евклідову відстань можна використовувати як інструмент прямого порівняння CAM_j і $TGPS_j$. У той же час для непрямого порівняння можна використовувати кутову відстань та таксономічну відстань між дескрипторами траєкторій (гістограма напрямку переміщення $CAMT_i$ та $TGPST_i$). Дескриптор траєкторії гістограми напрямку переміщення являє собою структуру формалізації даних в комірки якої записується величина зміщення об'єкта, що рухається, в різних напрямках від 0° до 360°. Величина числа інтервалів гістограми визначає кутовий дозвіл гістограми, відповідно до виразу:

$$PM = 360°/NI, \qquad (9)$$

де PM – кутовий дозвіл гістограми, NI – величина кількості інтервалів гістограми.

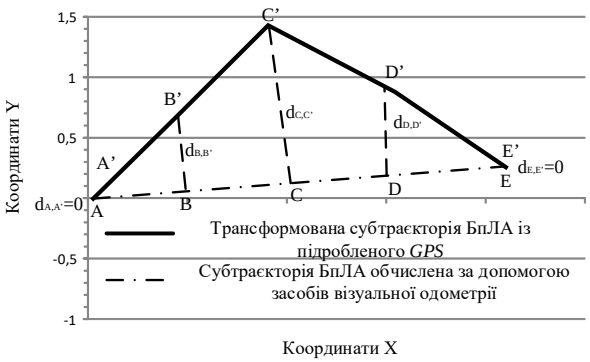


Рис. 5. Ілюстрація евклідова відстані між відповідними точками CAM_i та $TGPS_i$ в межах ковзаючого вікна з п'яти точок (**Fig. 5.** Illustration of the Euclidean distance between the respective CAM_i and $TGPS_i$ points within a five-point sliding window)

Приклад такої оцінки кутового дозволу у вигляді ілюстрації гістограми напрямку переміщення при $NI = 8$ представимо на рис. 6.

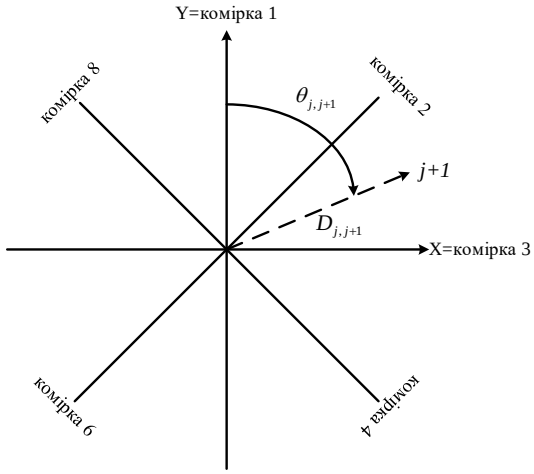


Рис. 6. Приклад дескрипторів траєкторії гістограми напряму переміщення з вісьма комірками, відстань $D_{j,j+1}$ ділиться між двома найближчими комірками щодо кута $\theta_{j,j+1}$ (**Fig. 6.** Example of descriptors of the trajectory of the histogram of the direction of movement with eight cells, the distance $D_{j,j+1}$ is divided between the two nearest cells relative to the angle $\theta_{j,j+1}$)

Скористаємося відомою методикою, описаною в роботі [18]. Відповідно до даної методики розрахунку відстані $D_{j,j+1}$ спільно з азимутальним кутом $\theta_{j,j+1}$ є основними складовими при оцінці гістограми напрямку переміщення,

$$\theta_{j,j+1} = a\tan 2^{-1}\left(\left(x_{j+1} - x_j\right)\left(y_{j+1} - y_j\right)\right), \quad (10)$$

при цьому частка комірки обчислюється як:

$$\alpha = D_{j,j+1}\left(1 - \left(\left|\theta_{j,j+1}\right| / PM - \left|\left(NI - 1\right)\right|\right)\right). \quad (11)$$

Дві найближчі комірки гістограми обчислюються відповідно до виразів:

$$NI1 = \left\lfloor \theta_{j,j+1} / PM \right\rfloor + 1, \quad (12)$$

$$NI2 = NI1 + 1. \quad (13)$$

Для порівняння $CAMT_j$ і $GPST_j$ з дескрипторами гістограми напряму переміщення виникає потреба у перетворенні та адаптації $GPST_j$ до системи координат $CAMT_j$. Для цього автори [18] пропонують дві міри відмінності та адаптації:

1. Кутова відстань між дескрипторами гістограми напряму переміщення:

$$\beta(a,b) = \frac{1}{\pi}\cos^{-1}\left(\frac{\langle a|b\rangle}{\|a\|\|b\|}\right), \quad (14)$$

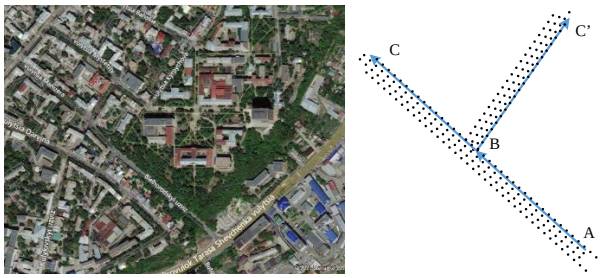
2. Таксономічна відстань між дескрипторами гістограми напряму переміщення:

$$\chi(a,b) = \sum_{i=1}^{p=NI} \left|a_i - b_i\right|, \quad (15)$$

де a та b – відповідно дескриптори гістограми напрямку переміщення траєкторій $CAMT_i$ та $TGPST_i$; a_i та b_i – i-ті компоненти a та b.

2. Дослідження розробленого методу виявлення спуфінгу БПЛА

Для дослідження та оцінки ефективності запропонованого методу виявлення спуфінгу БПЛА було використано 50 фотографій території Національного технічного університету «Харківський політехнічний інститут». На рис. 7 показаний один з фотознімків та лінії польоту БПЛА, що використовуються при реалізації різних сценаріїв кібератаки. На рис. 8 представлені два послідовні зображення набору даних.



а б

Рис. 7. Супутникове фотозображення Національного технічного університету «Харківський політехнічний інститут» (а) та лінії польоту БПЛА за представленим на фотозображенні маршрутом (б) (**Fig. 7.** Satellite photo image of the National Technical University "Kharkiv Polytechnic Institute" (a) and UAV flight lines along the route (b) shown in the photo image)

а б

Рис. 8. Стереозображення Національного технічного університету «Харківський політехнічний інститут» з висоти польоту БПЛА (**Fig. 8.** Stereo image of the National Technical University "Kharkiv Polytechnic Institute" from the height of the UAV)

У ході дослідження виконано імітаційне моделювання справжніх та хибних траєкторій БПЛА (рис. 7, б). На рис. 9 схематично представлений перший сценарій спуфінгу БПЛА. Зображення та координати *GPS* на заздалегідь визначених та хибних траєкторіях вибираються відповідно до лінії польоту. З рис. 10 видно, що спочатку певна траєкторія польоту БПЛА (траєкторія *AC*) була перервана активним спуфінгом у точці *B*. При цьому БПЛА був перенаправлений в точку *C′*. Передбачалося, що у сегменті польоту *AB* не відбувалося аномальних подій спуфінгу. Виходячи з цього, попередньо задана траєкторія польоту БПЛА і справжня траєкторія імітації БПЛА співпадають на цій ділянці. У кожному ковзаючому вікні W_i, *GPS*-положення зображень БПЛА з геотегами використовувалися для побудови $GPST_i$, а відповідні зображення використовувалися для побудови $CAMT_i$. Після атаки спуфінгу в точці *B*, вимірювання *GPS* під час польоту БПЛА над лінією *BC′* повинні демонструвати лінію *BC*. Отже, положення *GPS* лінії *BC* повинні представлятися підробленим розташуванням *GPS* в лінії *BC′*.

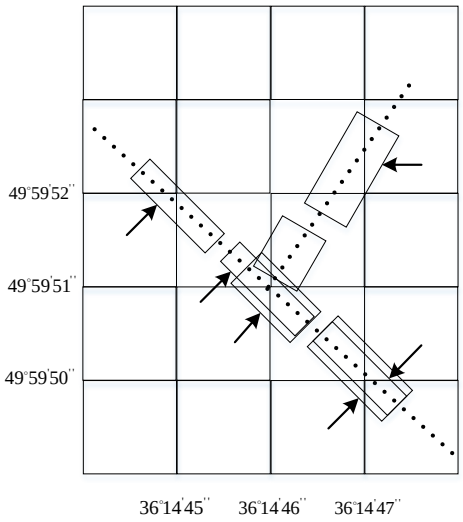
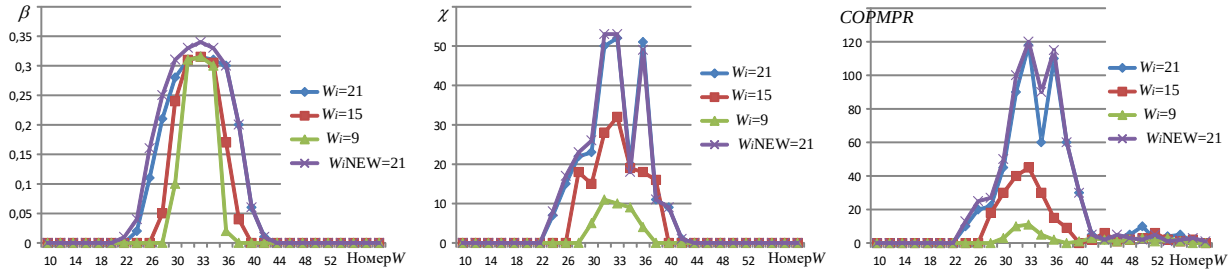


Рис. 9. Схема першого сценарію спуфінгу БПЛА (**Fig. 9.** Scheme of the first UAV spoofing scenario)

На рис. 10 наведені графіки залежності показників виявлення спуфінгу (*β*, *χ*, *COPMPR*) від значень позиції зображення.



а б в

Рис. 10. Графіки залежності показників виявлення спуфінгу (*β*, *χ*, *COPMPR*) від значень позиції зображення (**Fig. 10.** Graphs of dependence of spoofing detection indicators (*β*, *χ*, *COPMPR*) on image position values)

Як видно із рис. 10, а при збігу позиції зображення, отриманого від засобів візуальної одометрії, з позиціями *GPS* у ковзаючому вікні показник *β* кутової відстані між дескрипторами гістограми напрямку переміщення близький до нуля. Однак при досягненні вікна з номером 27 і введенням першого підробленого *GPS*-положення у вікно значення показника спуфінгу *β* починає зростати. Максимальна різниця між $CAMT_i$ та $GPST_i$ спостерігається в межах ковзаючого вікна 33. Після проходження певного вікна (на прикладі це ковзаюче вікно 41) *β* знову стає близьким до нуля, так як у цих позиціях $CAMT_i$ збігається з $TGPST_i$. Результати досліджень показників *χ* і *COPMPR* показують їх значну залежність від величини ковзаючого вікна. При цьому дані показники також вказують на позицію 33 як точку виявлення спуфінгу. Використання розробленого методу оцінки оптичного потоку та формування дескрипторів з використанням рекурентних згорткових нейронних мереж дозволило до 3% підвищити точність оцінки помилкових *GPS*-положень БПЛА. Це особливо помітно на рис. 10, а при використанні показника *β* кутової відстані між дескрипторами гістограми спрямування переміщення. Кількість помилкових *GPS*-положень, що фіксуються розробленим методом виявлення спуфінгу БПЛА з використанням засобів візуальної одометрії, наведено в табл. 1.

Таблиця 1 – **Кількість помилкових *GPS*-положень, що фіксуються методом виявлення спуфінгу БПЛА з використанням засобів візуальної одометрії**

	COPMPR	*β*	*χ*
W = 9	30	13	16
W = 15	31	19	21
W = 21	32	25	27
WNEW = 21	33	28	28

Представлені результати демонструють практично 100% показник виявлення помилкових *GPS*-положень за допомогою *COPMPR*. Це обґрунтовується більшою чутливістю *COPMPR* до невеликих змін швидкості БПЛА внаслідок спуфінгу.

Ще один сценарій спуфінгу БПЛА графічно зображено на рис. 11. Відмінною особливістю цього сценарію порівняно з попереднім є заздалегідь задана траєкторія БПЛА, яка представляє собою криву лінію. При цьому напрям у початковій траєкторії змінюється поступово з інтенсивністю 1° від одного положення зображення до іншого.

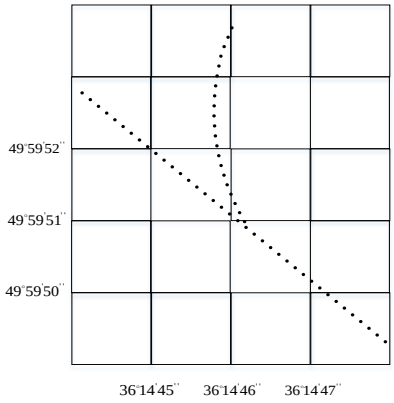
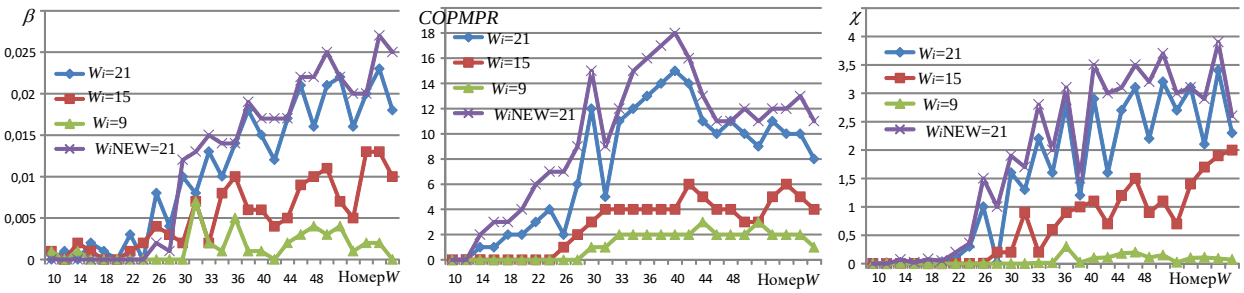


Рис. 11. Схема другого сценарію спуфінгу БПЛА (**Fig. 11.** Scheme of the second UAV spoofing scenario)

Результати реакції показників спуфінгу на зміни траєкторій представлені на рис. 12.

Як видно з рисунку, всі досліджувані показники спуфінгу при величинах ковзаючого вікна від 15 і вище дають можливість оцінки активних кібератак на БпЛА. При цьому кількість виявлених помилкових *GPS*-положень вище за використання показників $COPMPR$ та χ. У той же час використання розробленого методу оцінки оптичного потоку та формування дескрипторів з використанням рекурентних згорткових нейронних мереж дозволило до 5% підвищити точність оцінки помилкових *GPS*-положень БПЛА. Це особливо помітно на рис. 12 (в) при використанні показника $COPMPR$ суми евклідових відстаней між точками траєкторії.



а б в

Рис. 12. Графіки залежності показників виявлення спуфінгу (β, χ, $COPMPR$) від значень позиції зображення під час використання другого сценарію (**Fig. 12.** Graphs of dependence of spoofing indicators (β, χ, $COPMPR$) on the values of the image position when using the second scenario)

Висновки

Таким чином, розроблено метод виявлення спуфінгу БПЛА на основі інтелектуальної оцінки оптичного потоку та обробки даних візуальної одометрії. Відмінною особливістю методу є використання технології розрахунку субтраєкторії $CAMT_i$ на основі субтраєкторій візуальної одометрії та $GPST_i$ з *GPS*-положень у ковзаючому вікні з урахуванням інтелектуальної оцінки оптичного потоку та формування дескрипторів «Его-переміщення» БПЛА. В якості порівняння показників спуфінгу було запропоновано використання заходів β, χ та $COPMPR$. Результати експерименту для двох сценаріїв спуфінгу показали ефективність оцінки положень принаймні двох з трьох показників (χ та $COPMPR$), в умовах використання ковзаючих вікон розміром від 15 і вище, з часовою затримкою, що становить половину розміру вікна. Крім того, показано, що використання інтелектуального методу оптичного потоку та формування дескрипторів з використанням рекурентних згорткових нейронних мереж.

СПИСОК ЛІТЕРАТУРИ (REFERENCES)

1. Jafarnia-Jahromi, Ali, Broumandan, Ali, Nielsen, J. & Lachapelle, G. (2012), “GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques”, *Int, Journal of Navigation and Observation*, doi: https://doi.org/10.1155/2012/127072.
2. Lawal, A.B. (2020), How to Design GPS/GNSS Receivers Books 2, 3, 4 & 5, URL: https://books.google.com.ua/books?id=RXANEAAAQBAJ&printsec=frontcover&hl=ru&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false.
3. Shepard, D.P.; Bhatti, J.A.; Humphreys, T.E. & Fansler, A.A. (2012), “Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks”, *Radionavigation Laboratory Conf. Proc.*, The University of Texas at Austin: Austin, TX, USA,.
4. Kerns, A.J.; Shepard, D.P.; Bhatti, J.A.; Humphreys, T.E. Unmanned Aircraft Capture and Control Via GPS Spoofing. J. Field Robot. 2014, 31, 617–636.
5. He, D., Qiao, Y., Chen, S., Du, X., Chen, W., Zhu, S. and Guizani, M. (2019), “A Friendly and Low-Cost Technique for Capturing Non-Cooperative Civilian Unmanned Aerial Vehicles”, *IEEE Netw.*, 33, pp. 146–151.
6. Guo, Y., Wu, M., Tang, K., Tie, J. and Li, X. (2019), “Covert Spoofing Algorithm of UAV based on GPS/INS Integrated Navigation”, *IEEE Trans. Veh. Technol.*
7. Broumandan, A.; Jafarnia-Jahromi, A.; Daneshmand, S.; Lachapelle, G. (2016), “Overview of Spatial Processing Approaches for GNSS Structural Interference Detection and Mitigation”, *Proc. IEEE*, 104, pp. 1246–1257.
8. Milaat, F.A. and Liu, H. (2018), “Decentralized Detection of GPS Spoofing”, *IEEE Commun. Lett.*, 22, pp. 1256–1259.
9. Sun, C.; Cheong, J.W.; Dempster, A.G.; Zhao, H.; Demicheli, L.; Feng,W. A (2018), “New Signal Quality Monitoring Method for Anti-spoofing”, *China Satellite Navigation Conference* (CSNC) 2018 Proceedings, Springer, Singapore, pp. 221–231.
10. Humphreys, T., Bhatti, J. and Ledvina, B. (2010), “The GPS Assimilator: A method for upgrading existing GPS user equipment to improve accuracy, robustness, and resistance to spoofing”, *Radionavigation Laboratory Conference Proceedings*, Proceedings of the ION GNSS Conference, Portland, OR, USA, The University of Texas at Austin: Austin, TX, USA,.

11. Oligeri, G., Sciancalepore, S., Ibrahim, O.A. and Pietro, R.D. (2019), “Drive me not: GPS spoofing detection via cellular network: (architectures, models, and experiments”, *Proc. of the 12th Conf. on Security and Privacy in Wireless and Mobile Networks, Miami*, FL, USA, 14–17 May; pp. 12–22.
12. Qiao, Y., Zhang, Y. and Du, X. A. (2017), “Vision-Based GPS-Spoofing Detection Method for Small UAVs”, *Proceedings of the 2017 13th International Conference on Computational Intelligence and Security* (CIS), Hong Kong, China, pp. 312–316.
13. Chowdhary, G., Johnson, E.N., Magree, D., Wu, A. and Shein, A. (2013), “GPS-denied indoor and outdoor monocular vision aided navigation and control of unmanned aircraft”, *J. Field Robot*, 30, pp. 415–438.
14. Gonzalez, R.; Rodriguez, F.; Guzman, J.L.; Pradalier, C. and Siegwart, R. (2012), “Combined visual odometry and visual compass for mobile robots localization”, *Robotica*, 30, pp. 865–878.
15. Scaramuzza, D. and Siegwart, R. (2008), “Appearance-Guided Monocular Omnidirectional Visual Odometry for Outdoor Ground Vehicles”, *IEEE Trans. Robot*, 24, pp. 1015–1026.
16. Sun, Deqing, Yang, Xiaodong, Liu, Ming-Yu & Kautz, Jan (2018), PWC-Net: CNNs for Optical Flow Using Pyramid, Warping, and Cost Volume”, *2018 IEEE/CVF Conf. on Comp. Vision and Pattern Recognition*, pp. 8934-8943.
17. Gerardus, Blokdyk (2018), *Recurrent neural network: Real Life Actions Paperback*, 132 p.
18. Varshosaz, Masood, Afary, Ali Reza, Mojaradi, Barat, Saadatseresht, Mohammad & Ghanbari Parmehr, Ebadat (2019), “Spoofing Detection of Civilian UAVs Using Visual Odometry”, *ISPRS International Journal of Geo-Information*, 9, doi: https://doi.org/10.3390/ijgi9010006.

Received (Надійшла) 01.11.2021
Accepted for publication (Прийнята до друку) 05.01.2022

ВІДОМОСТІ ПРО АВТОРІВ/ ABOUT THE AUTHORS

Волошин Денис Геннадійович – аспірант кафедри "Обчислювальна техніка та програмування", Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Denys Voloshyn – graduate student of Computer Engineering and Programming Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: ultrageron@gmail.com; ORCID ID: https://orcid.org/0000-0002-1077-9658.

Бульба Сергій Сергійович – кандидат технічних наук, доцент кафедри "Обчислювальна техніка та програмування", Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Serhii Bulba – Candidate of Technical Sciences, Associate Professor of Computer Engineering and Programming Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: bssserega@gmail.com; ORCID ID: https://orcid.org/0000-0003-0358-7516.

Интеллектуальный метод определения спуфинга БПЛА

Д. Г. Волошин, С. С. Бульба

Аннотация. В работе представлен интеллектуальный метод обнаружения спуфинга БПЛА. Отличительной особенностью метода является использование технологии расчета субтраектории на основе субтраекторий визуальной одометрии и GPS-положений в скользящем окне с учетом интеллектуальной оценки оптического потока и формирования дескрипторов «Эго-перемещения» БПЛА. В ходе исследования проведен анализ и сравнительные исследования широкого спектра методов спуфинга БПЛА, выявлены наиболее часто рекомендованные и практически используемые методы. Сделан вывод об актуальности проблематики GPS-спуфинга. Проведен анализ методов защиты от GPS спуфинга БПЛА. Выявлены перспективные направления интеллектуального обнаружения спуфинга БПЛА с использованием методов и средств визуальной одометрии. В ходе исследования методов фиксации входных данных предложен подход оценки оптического потока с использованием скользящего окна. При этом аргументировано доказана необходимость интеллектуальной обработки входных данных. Оценка оптического потока и формирование дескрипторов проводилась с использованием рекуррентных сверточных нейронных сетей. В результате разработана структурная схема метода обнаружения спуфинга БПЛА. Это позволило провести исследование разработанного метода. Результаты эксперимента для двух сценариев спуфинга показали эффективность оценки положений не менее двух из трех показателей в условиях использования скользящих окон размером от 15 и выше, с временной задержкой, составляющей половину размера окна.

Ключевые слова: спуфинг; БПЛА; скользящее окно; оптический поток; дескриптор.

Intelligent UAV Spoofing Detection Method

Denys Voloshin, Serhii Bulba

Abstract. The paper presents an intelligent method for detecting UAV spoofing. A distinctive feature of the method is the use of subtrajectory calculation technology based on visual odometry subtrajectories and GPS positions in a sliding window, taking into account the intelligent estimation of the optical flow and the formation of UAV “Ego-movement” descriptors. In the course of the study, an analysis and comparative studies of a wide range of UAV spoofing methods were carried out, the most frequently recommended and practically used methods were identified. The conclusion is made about the relevance of the problems of GPS spoofing. The analysis of methods of protection against UAV GPS spoofing has been carried out. Promising directions for intelligent detection of UAV spoofing using methods and means of visual odometry are identified. In the course of studying methods for fixing input data, an approach was proposed for estimating the optical flow using a sliding window. At the same time, the need for intelligent processing of input data is argued. The estimation of the optical flow and the formation of descriptors was carried out using recurrent convolutional neural networks. As a result, a block diagram of the UAV spoofing detection method was developed. This allowed us to study the developed method. The results of the experiment for two spoofing scenarios showed the efficiency of estimating the positions of at least two of the three indicators under the conditions of using sliding windows of size 15 or more, with a time delay of half the window size.

Keywords: spoofing; UAV; sliding window; optical flow; handle.