

РЕЦЕНЗІЯ

рецензента – кандидата технічних наук, доцента, доцента кафедри штучного інтелекту Державного університету інформаційно-комунікаційних технологій Шантиря Антона Сергійовича на дисертаційну роботу

Мішкура Юрія Валентиновича на тему: «Інформаційна технологія стегоаналізу зображень на основі глибокого навчання та мультимодальних моделей», подану на здобуття ступеня доктора філософії в галузі знань

12 – Інформаційні технології за спеціальністю

123 – Комп'ютерна інженерія

Актуальність обраної теми.

Стрімкий розвиток цифрових технологій, широке використання мультимедійних даних та зростання обсягів інформаційного обміну сприяють активному поширенню методів прихованої передачі інформації. Одним із найбільш розповсюджених підходів є стеганографія, яка дозволяє вбудовувати конфіденційні повідомлення у цифрові зображення без помітного погіршення їх якості.

Поряд із законним використанням стеганографічних технологій виникають суттєві загрози інформаційній безпеці, пов'язані з можливістю прихованого передавання конфіденційних даних, шкідливого програмного коду або координування протиправної діяльності. У зв'язку з цим особливого значення набувають методи стегоаналізу, спрямовані на виявлення прихованої інформації у цифрових контейнерах.

Сучасні методи стегоаналізу дедалі частіше використовують технології глибокого навчання та штучного інтелекту. Водночас традиційні підходи не завжди забезпечують достатню точність виявлення прихованих повідомлень при використанні сучасних адаптивних стеганографічних алгоритмів. Особливо перспективним напрямом є застосування мультимодальних моделей та гібридних архітектур штучного інтелекту, здатних враховувати як локальні, так і глобальні особливості зображень.

Таким чином, тема дисертаційної роботи Мішкура Ю.В., присвячена розробленню інформаційної технології стегоаналізу зображень на основі глибокого навчання та мультимодальних моделей, є актуальною та має важливе значення для розвитку методів забезпечення інформаційної безпеки та комп'ютерної інженерії.

Обґрунтованість наукових положень, висновків і рекомендацій дисертації.

Наукові положення, висновки та рекомендації, сформульовані у дисертаційній роботі, є достатньо обґрунтованими та достовірними.

Автором проведено комплексний аналіз сучасних методів стеганографії, стегоаналізу, комп'ютерного зору та глибокого навчання. Для розв'язання поставлених завдань використано сучасні методи математичного моделювання, машинного навчання, глибоких нейронних мереж, мультимодального аналізу даних та статистичної обробки результатів експериментів.

Достовірність отриманих результатів підтверджується значним обсягом експериментальних досліджень, використанням відкритих наборів даних, порівнянням із відомими аналогами та статистичною оцінкою отриманих результатів.

Оцінка новизни наукових результатів дисертаційного дослідження.

Серед ключових елементів наукової новизни слід відзначити:

1. Вперше розроблено гібридну архітектуру стегоаналізу, яка за рахунок поєднання блоку паралельної багатомасштабної високочастотної фільтрації із семантичним аналізом мультимодальних великих мовних моделей, використання механізму формування природномовних інтерпретацій результатів детекції, інтеграції CNN-компонента з MLLM-компонентом через спеціалізований шар-адаптер та реалізації механізму локального мультимодального аналізу на платформі Ollama, дозволила забезпечити підвищення точності та інтерпретованості процесів виявлення прихованої інформації у цифрових зображеннях, а також формування обґрунтованих природномовних висновків щодо характеру виявлених аномалій.

2. Вперше запропоновано механізм семантичного арбітражу в задачах виявлення прихованої інформації, який за рахунок використання мультимодальних великих мовних моделей для верифікації результатів нейромережевого класифікатора, формування контекстно-залежної оцінки аномалій, аналізу особливостей текстурних областей зображення та інтеграції семантичних і статистичних ознак у межах єдиного процесу прийняття рішень, дозволив ефективно розрізняти природний шум складних текстур від цілеспрямованого стеганографічного втручання та підвищити достовірність результатів стегоаналізу.

3. Удосконалено структуру вхідного шару стегоаналітичних нейронних мереж, яка за рахунок інтеграції механізму адаптивного перерахунку ваг каналів ознак (SE-блоків) для паралельних груп фільтрів різних просторових розмірів, використання механізму селективного підсилення інформативних ознак стегошуму та адаптивного балансування внеску багатомасштабних високочастотних компонентів, дозволила підвищити чутливість системи до дрібнорозмірних артефактів стеганографічного втручання та покращити якість виявлення прихованої інформації в умовах складних текстур і JPEG-стиснення.

4. Дістала подальший розвиток модель багатомасштабної попередньої обробки зображень, яка за рахунок одночасного використання спрямованих високочастотних ядер 3×3 , 5×5 та 7×7 пікселів, поєднання просторового та частотного аналізу ознак вбудовування, формування багатоканального представлення залишкових шумів та інтеграції результатів багатомасштабної фільтрації у єдиний вхідний простір CNN-класифікатора, дозволила одночасно ідентифікувати ознаки прихованого вбудовування як у просторовому, так і в частотному доменах та підвищити ефективність стегоаналізу цифрових зображень.

Отримані результати характеризуються науковою новизною та є вагомим внеском у розвиток інформаційних технологій стегоаналізу.

Практична цінність отриманих результатів.

Практична цінність дисертаційної роботи полягає у створенні програмно-алгоритмічного комплексу стегааналізу цифрових зображень, який може бути використаний для підвищення ефективності систем забезпечення інформаційної безпеки.

Розроблена інформаційна технологія дозволяє підвищити точність виявлення прихованих повідомлень у цифрових зображеннях та забезпечити ефективний аналіз сучасних стеганографічних контейнерів.

Результати роботи можуть бути використані в системах кібербезпеки, цифрової криміналістики, моніторингу інформаційних ресурсів, правоохоронній діяльності та під час підготовки фахівців з інформаційних технологій і кібербезпеки.

Зв'язок роботи з науковими програмами, планами, темами

Дисертаційна робота виконана відповідно до наукової тематики Державного університету інформаційно-комунікаційних технологій та пов'язана з виконанням науково-дослідних робіт, спрямованих на розвиток методів штучного інтелекту, комп'ютерного зору, інформаційної безпеки та аналізу мультимедійних даних.

Результати дослідження відповідають сучасним пріоритетним напрямкам розвитку інформаційних технологій та кібербезпеки.

Повнота викладу основних результатів дисертації в публікаціях.

Основні результати дисертаційної роботи достатньо повно висвітлені у наукових працях автора.

Публікації автора відображають основні положення дисертаційного дослідження, його наукову новизну та практичне значення. Результати роботи пройшли апробацію на міжнародних та всеукраїнських наукових конференціях, а також опубліковані у фахових наукових виданнях.

Кількість і рівень публікацій відповідають вимогам до дисертацій на здобуття ступеня доктора філософії.

Оцінка змісту дисертації, відповідність встановленим вимогам щодо оформлення.

Дисертаційна робота має логічну структуру та складається зі вступу, розділів основної частини, висновків, списку використаних джерел та додатків.

Матеріал викладено послідовно, аргументовано та на належному науковому рівні. Робота містить достатній обсяг теоретичних досліджень, математичних обґрунтувань та результатів експериментальної перевірки запропонованих рішень.

Оформлення дисертації відповідає вимогам чинного законодавства України щодо підготовки дисертацій на здобуття ступеня доктора філософії.

Зауваження до проведеного дисертаційного дослідження.

Разом із тим, у роботі є кілька дискусійних аспектів:

1. У роботі недостатньо детально досліджено вплив різних архітектур мультимодальних моделей на якість виявлення прихованих повідомлень.

2. Для більш повної оцінки ефективності запропонованої технології доцільно було б провести порівняння з найсучаснішими мультимодальними моделями великого масштабу.

3. Недостатньо уваги приділено оцінюванню стійкості розробленого методу до навмисних атак, спрямованих на приховування ознак стеганографічного вкладення.

4. Перспективним напрямом подальших досліджень є розширення запропонованої технології на інші типи мультимедійних даних, зокрема відео та аудіофайли.

5. У роботі доцільно було б більш детально розглянути питання обчислювальної складності та можливості використання розробленої технології в системах реального часу.

Наведені зауваження мають рекомендаційний характер і не впливають на загальну позитивну оцінку дисертаційної роботи.

Висновок.

Дисертаційна робота Мішкура Юрія Валентиновича на тему «Інформаційна технологія стегоаналізу зображень на основі глибокого навчання та мультимодальних моделей» є завершеним самостійним науковим дослідженням, у якому вирішено актуальне науково-прикладне завдання підвищення ефективності виявлення прихованої інформації у цифрових зображеннях шляхом розроблення нової інформаційної технології стегоаналізу на основі методів глибокого навчання та мультимодального аналізу.

За актуальністю, науковою новизною, теоретичним і практичним значенням отриманих результатів дисертаційна робота відповідає вимогам Постанови Кабінету Міністрів України від 12 січня 2022 року № 44 «Про затвердження Порядку присудження ступеня доктора філософії», а її автор — Мішкур Юрій Валентинович — заслуговує на присудження ступеня доктора філософії з галузі знань 12 «Інформаційні технології» за спеціальністю 123 «Комп'ютерна інженерія».

Рецензент

кандидат технічних наук, доцент,
доцент кафедри штучного інтелекту
Державного університету
інформаційно-комунікаційних технологій



Антон ШАНТИР

Підпис

ЗАСВІДЧУЮ

Учений секретар

Державного університету

інформаційно-комунікаційних технологій

