МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеська національна академія харчових технологій
Університет Інформатики і прикладних знань, м.Лодзь, Польща
Національний технічний університет України «Київський політехнічний інститут»
Навчально-науковий інститут комп'ютерних систем і технологій «Індустрія 4.0» ім. П.М. Платонова

XXI Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Матеріали конференції

Одеса

22-23 квітня 2021 р.

Стан, досягнення та перспективи інформаційних систем і технологій / Матеріали XXI Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 22-23 квітня 2021 р**.** - Одеса, Видавництво ОНАХТ, 2021 р. – 229 с.

Збірник включає матеріали доповідей учасників конференції, які об'єднані за тематичними напрямками конференції.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Матеріали подано українською, російською та англійською мовами.
Редактор збірника Котлик С.В.

Often for financial systems based on blockchain technology, high transaction transparency may be undesirable. It is possible to achieve greater anonymity by using protocols based on zero-knowledge proofs. Range proof, as an example of zero-knowledge proofs, is used in some modern blockchain protocols based on elliptic-curve cryptography that provide high transaction anonymity.

In this work, we consider the possibility of applying protocols based on zero-knowledge proofs to increase the anonymity of financial transactions in financial systems based on blockchain technology. The relevance of this topic is driven by the growing interest in financial systems based on blockchain protocols. Today financial instruments based on blockchain technology have become widespread. The high interest in it is caused by its properties such as decentralization, high transparency of transactions, data safety, and resistance to data spoofing. However, in many areas of human activity, especially in finance, high transaction transparency may be undesirable. So, for example, in the Bitcoin payment system, if the address of one of the users is known, it is possible to obtain information about the history of his transactions, and details of the transactions. This work explores the possibility of using zero-knowledge proofs to achieve greater anonymity of financial transactions and discusses some of the common protocols such as ZK-SNARK and Mimblewimble.

Zero-knowledge proof is an interactive cryptographic protocol that allows one of the communicating parties to verify the validity of a statement without receiving any unnecessary information from the other party [1]. The idea is to prove that one of the parties has a piece of information without revealing its content. The protocol requires interactive input from the verifier, usually in the form of a task or a problem. The goal of the prover in this protocol is to convince the verifier that he has a solution, without revealing even part of the "secret" proof. The purpose of the verifier is to make sure that the prover indeed has the required information. Also, there are zero-knowledge proof protocols that do not require interactive input. Most of such protocols rely on the assumption of a perfect cryptographic hash function. The idea of using such protocols for validating transactions in financial systems without excessive disclosure of transaction details is very promising. Zero-knowledge proofs are widely used in many blockchain protocols that require high transaction anonymity. For example, the idea behind the Mimblewimble protocol is to hide the details of financial transactions using elliptic-curve cryptography. Due to the properties of elliptic curves, this protocol needs to use the range proofs [2] to avoid creating transactions with negative values. Range proof is proof that a number is within a specified interval, without revealing the number itself. There are also some other similar protocols, for example, ZK-SNARK, which uses elliptic-curve cryptography, and the alternate protocol ZK-STARK, which uses hash functions. Thus, using blockchain protocols based on zero-knowledge proofs allows achieving greater anonymity of financial transactions.

[1] N. R. Gowravaram, "Zero Knowledge Proofs and Applications to Financial Regulation", PhD thesis, Harvard College, 2018. [Online]. Available: https://dash.harvard.edu/handle/1/38811528. [Accessed Apr. 11, 2021].
[2] B. Bunz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille and G. Maxwell, "Bulletproofs: Short Proofs for Confidential Transactions and More," 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2018, pp. 315-334.

УДК 004.91

РОЗРОБКА ПРОГРАМИ ДЛЯ ПЕРЕВІРКИ ТЕКСТІВ НА ОРИГІНАЛЬНІСТЬ

БЕВЗ С.В. (*svbevz@i.ua*), БУРБЕЛО С.М. (*burbelo@vntu.edu.ua*),
ВОЙТКО В.В. (*dekanfki@i.ua*), ЗАВАЛЬНЮК Є.К. (*qq9272627@gmail.com*)
Вінницький національний технічний університет

Розглянуто особливості розробки програм для перевірки оригінальності текстових робіт. Проведено аналіз наявних програм. Описано розробку програми для оцінювання оригінальності тексту.

Вступ

Принципи доброчесності, збереження і повага до авторського права є нормою в сучасному світі. Недопустимим є використання чужого тексту у своїй роботі без належного оформлення посилання на роботу автора. Важливим питанням сьогодні постає перевірка на оригінальність текстових робіт з метою унеможливлення появи плагіату. Тому важливою є розробка програми для перевірки текстів на оригінальність.

Метою роботи є підвищення достовірності перевірки текстових робіт на оригінальність шляхом розробки і використання програми, що реалізує порівняння речень з використанням коефіцієнта Очиаї.

Об'єктом дослідження є процес обробки текстових даних.

Предметом дослідження є методи і засоби розробки програм для перевірки текстових робіт на оригінальність.

Задачею роботи є проведення порівняльного аналізу відомих ресурсів для перевірки текстів на наявність плагіату та розробка програми для перевірки текстів на оригінальність.

Розробка програми перевірки текстів на оригінальність

Серед відомих систем виявлення плагіату можна виділити Content-watch, PLAGIATSEARCH, Unicheck.

Веб-ресурс Content-watch забезпечує онлайн-перевірку тексту в Інтернеті. Серед його недоліків відмітимо неможливість завантаження тексту файлом та обмеження кількості перевірок тексту до трьох разів [1].

Додаток PLAGIATSEARCH, розроблений Гавенком О. В. у Вінницькому національному технічному університеті, дозволяє здійснити локальну перевірку наборів текстових файлів. Однак, у програмі відсутня можливість пошуку у мережі, а процес перевірки не автоматизований [2].

Ресурс Unicheck, розроблений Phase One Carma, є потужним ресурсом для локальної та глобальної перевірки. Однак, ресурс є платним, а також у ньому відсутня перевірка зображень [3].

Створена програма TextOriginal призначена для перевірки текстів на оригінальність. Процес перевірки файлів у програмі TextOriginal повністю автоматизований. Результати перевірок зберігаються у спеціальних папках в окремих файлах.

Розроблений програмний додаток TextOriginal (інтерфейс зображено на рис. 1) є безкоштовним додатком.

Серед функціоналу програми виділимо можливість перевірки текстів на оригінальність. Текстові файли порівнюються в локальних базах шляхом встановлення, наскільки схожі їх речення (тут використовується коефіцієнт Очиаї).

Результати порівняльного аналізу аналогів зведено в табл. 1.

Таблиця 1 – Порівняльний аналіз аналогів

Характеристика / Засіб	Content-watch	PLAGIATSEARCH	Unicheck	TextOriginal
Перевірка глобального плагіату	+	-	+	+-
Перевірка локального плагіату	-	+	+	+
Безкоштовне використання	+-	+	-	+

Перевірка заміни символів	-	-	+	+
Перевірка усього набору файлів	-	-	+	+
Сумарний показник	1.5	2	4	4.5

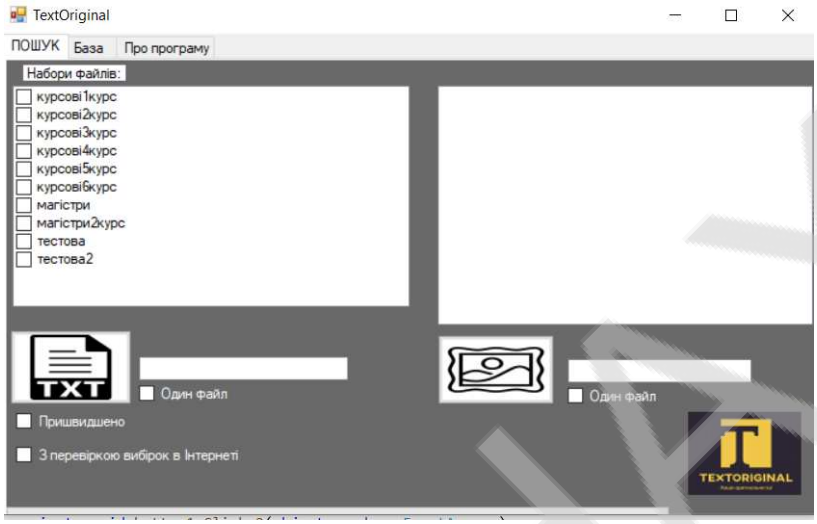

Рисунок 1 – Інтерфейс додатку TextOriginal

У програмі TextOriginal забезпечена можливість пришвидшити перевірку тексту на оригінальність, використовуючи виявлення повністю ідентичних речень. Перед перевіркою текст модифікується, видаляються закінчення слів, анулюється заміна символів.

Під час перевірки окремого файлу формується вибірка з десяти повністю схожих речень, пошук яких можна здійснити глобально у пошуковій системі Google.

Висновок

Розроблено програму TextOriginal для обробки текстової інформації на предмет встановлення оригінальності текстів. Додаток призначений для підвищення ефективності обробки текстів у локальних наборах файлів. Програма розроблена з використанням мови C# та середовища Visual Studio. Для пошуку вибірки речень в Інтернеті використано бібліотеки Google API.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Проверить текст на уникальность [Електронний ресурс] – Режим доступу до ресурсу: https://content-watch.ru/text/.
2. Войтко В. В. Розробка комп'ютерної програми для перевірки текстів на плагіат / В. В. Войтко, С. В. Бевз, С. М. Бурбело, О. В. Гавенко [Електронний ресурс]– Режим доступу до ресурсу: https://cutt.ly/RllbVOv.
3. Unicheck [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Unicheck.

УДК 004.42

XXI Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Одеса

22-23 квітня 2021 р.

Збірник включає доповіді учасників конференції. Тези доповідей публікуються у вигляді, в якому вони були подані авторами.

Відповідальність за зміст і форму подачі матеріалу несуть автори статей.

Редакційна колегія: Котлик С.В., Корнієнко Ю.К.

Комп'ютерний набір і верстка: Соколова О.П.

Відповідальний за випуск: Котлик С.В.