

ВИЯВЛЕННЯ FORM-БОТІВ ІЗ ВИКОРИСТАННЯМ МЕТОДІВ МАШИННОГО НАВЧАННЯ

О. М. Чорний¹, А. М. Родіонов¹

¹Національний технічний університет України «Київський політехнічний інститут»

Анотація

У даній роботі розглядається метод виявлення ботів, що призначені для автоматичного заповнення і відправки веб-форм, що базується на використанні методів машинного навчання.

Ключові слова: виявлення ботів, машинне навчання, навчання з учителем, класифікація

Вступ

В наш час глобальна мережа Інтернет набула широкого поширення. Люди використовують її для спілкування, отримання останніх новин, пошуку необхідної інформації, інтернет-банкінгу, здійснення покупок в інтернет-магазинах тощо. Одним із основних способів вводу інформації та реєстрації на сайтах є форми – набори полів вводу чи вибору інформації, відповідних їм текстових міток та кнопки, при натисненні на яку введена інформація передається для подальшої обробки сервером. Специфіка роботи веб-застосунків передбачає можливість створення ботів – застосунків, що здатні заповнювати форми та виконувати їх відправку автоматично. Створені таким чином боти можуть виконувати розповсюдження спаму та посилань на шкідливе ПЗ, наповнювати веб-ресурси сміттям, виконувати сотні замовлень в інтернет-магазинах, тим самим блокуючи їх роботу. Очевидно, що такі явища є вкрай небажаними та потребують певних засобів для їх попередження. Таким чином, метою даної роботи є побудова системи розпізнавання form-ботів.

1. Методи захисту

Найбільш розповсюдженим методом боротьби із form-ботами є CAPTCHA[1] та її різновиди, наприклад reCAPTCHA. Зазвичай вона являє собою зображення зі спотвореним текстом, котрий людина повинна ввести в спеціальне поле й відправити на перевірку серверу. Даний метод має кілька суттєвих недоліків. По-перше, деякі реалізації такої CAPTCHA настільки спотворюють текст, що інколи його дуже важко зрозуміти навіть людині. Проходження такого тесту створює незручностей користувачам та забирає багато часу, що може негативно відобразитись на рейтингу веб-ресурсу. По-друге, вже існує досить багато інструментів для автоматичного розпізнавання тексту на зображеннях, що суттєво знижує ефективність такого виду захисту. Це говорить про необхідність розробки альтернативних методів захисту від form-ботів.

Однією із можливих альтернатив є система розпізнавання побудована на основі вимірювання певних біометричних характеристик людської поведінки. Імітація людської поведінки комп'ютером наразі є одною із найскладніших проблем, для якої не існує досить ефективних методів вирішення, отже така система повинна забезпечувати достатній рівень захисту.

В даній роботі для створення подібної системи було використано характеристики руху рук людини при користуванні мишкою або тачскріном мобільного пристрою.

2. Архітектура системи

Система розпізнавання може бути вбудованою в системи реєстрації, відправки повідомлень, оформлення замовлень та інші системи більшості веб-ресурсів. Складається вона із двох компонент: клієнтська підсистема логування, яка займається збиранням даних про рух руки користувача та серверна, яка приймає на вхід зібрані дані та приймає рішення про віднесення користувача до одного із класів – «людина» або «бот». Підсистема логування буде активуватись в той момент, коли користувач натискає на кнопку відправлення даних на сервер. В цей момент перед ним на екрані з'явиться спеціальне завдання, під час виконання якого буде здійснюватись запис всіх його рухів для подальшої класифікації.

3. Метод вирішення задачі

Зважаючи на велику кількість можливих рухів користувачів скласти явний алгоритм для класифікації дуже складно, тому для вирішення даної задачі доцільно використати методи машинного навчання. Дана задача є типовим прикладом навчання із учителем (supervised learning). Нехай у нас є множина об'єктів X , множина відповідей Y та невідома залежність:

$$y: X \rightarrow Y$$

Потрібно за наявною вибіркою $\{x_1, x_2, \dots, x_l\} \subset X$ та відомими відповідями $y_i = y(x_i)$, $i = 1, \dots, l$

знайти:

$$a: X \rightarrow Y$$

– алгоритм, що наближує залежність y на всій множині X .

Об'єкти задаються у вигляді векторів ознак, які бувають: бінарні, номінальні (категоріальні), порядкові, кількісні. Відповіді у задачах класифікації на 2 класи задаються як елементи множини $\{0, 1\}$.

Для того щоб звести задачу виявлення ботів до задачі машинного навчання із учителем необхідно виконати наступне:

- 1) Зібрати навчальну вибірку, яка буде складатись як із людських даних так і з даних ботів.
- 2) Скласти ознаковий опис елементів навчальної вибірки.
- 3) Обрати алгоритм класифікації, який би давав якомога кращі результати.

4. Збір даних

Для збору людських даних було створено спеціальну веб-сторінку, на котрій знаходилося зображення темного прямокутника на світлому фоні. Всім бажаним пропонувалося виконати наступне завдання: за допомогою комп'ютерної мишки необхідно було «стерти» зображення прямокутника та натиснути кнопку «Відправити», для передачі всіх зібраних системою логуювання даних для подальшого зберігання і обробки серверу. Всього вдалося зібрати 382 набори даних від близько 90 користувачів. Для отримання даних, характерних для ботів необхідно було змодельовувати бота, який би намагався імітувати людський рух. Такі моделі можна розділити на 2 типу: моделі на основі статистичних даних про рух справжніх людей та моделі, які не використовують таких даних. На даному етапі виконання роботи створено модель другого типу, планується також створити модель першого типу.

5. Ознаковий опис об'єктів

Об'єктом нашої задачі є ланцюжок із точок, кожна із яких представлена трійкою $\langle x, y, t \rangle$, де x – координата зареєстрованого руху по осі абсцис, y – координата зареєстрованого руху по осі ординат, t – час реєстрації. Спочатку для ланцюжка рахуються наступні характеристики:

Формула	Опис
$v_i = \frac{\sqrt{(x_{i+1}-x_i)^2 + (y_{i+1}-y_i)^2}}{t_{i+1}-t_i}$	Швидкість
$a_i = \frac{v_{i+1}-v_i}{\frac{t_{i+1}+2t_i+t_{i-1}}{4}}$	Прискорення
$F_i = \frac{\varphi_{i+1}-\varphi_i}{t_{i+1}-t_i}$	Кутова швидкість
$dF_i = \frac{F_{i+1}-F_i}{\frac{t_{i+1}+2t_i+t_{i-1}}{4}}$	Кутове прискорення

Тут φ_i – кут між додатнім напрямом осі абсцис та вектором, кінцями якого є точки (x_{i-1}, y_{i-1}) та

(x_i, y_i) . Окрема характеристика ланцюжка є послідовністю чисел, для якої рахувались наступні статистичні показники: середнє значення, середньоквадратичне відхилення, 0.25 – квантиль, 0.75 – квантиль. Отримані показники і брались у якості ознак ланцюжка точок.

6. Використані алгоритми

Для класифікації об'єктів було використано наступні алгоритми:

- Логістична регресія[2], яка є прикладом лінійного класифікатора
- Градієнтний бустинг[2], що є композицією більш простих алгоритмів – дерев рішень.
- Просте голосування, що також є композиційним методом, яке повертає у якості відповіді зважену суму відповідей кількох інших алгоритмів.

Для перевірки якості навчання використовувався метод, що називається кросс-валідація. При його використанні навчальна вибірка випадковим чином розбивається на K частин після чого проводиться K ітерацій навчання, в кожній із яких одна із частин використовується в якості тестової вибірки для обчислення точності класифікації, а решта частин беруться в якості навчальної вибірки. Отримані на кожній ітерації результати усереднюються, в результаті чого і отримується фінальна оцінка якості навчання. В даній роботі K було обрано рівним 5.

7. Отримані результати

Логістична регресія та градієнтний бустинг показали на кросс-валідації результат 99%, а просте голосування двох останніх алгоритмів дали 100% результат.

Висновки

В ході виконання даної роботи було створено систему виявлення form-ботів, що базується на біометричних характеристиках руху руки людини та методах машинного навчання для класифікації вхідних даних. Отримані показники точності класифікації показують на перспективність використання біометрії для розв'язування задач даного типу. Побудована система здатна виявляти ботів, які під час генерації траєкторії свого руху, не використовують статистичні дані руху рук людини. Планується також створення бота, що використовує такі дані, більш глибоке тестування та, можливе, вдосконалення побудованої системи.

Перелік використаних джерел

1. The Official CAPTCHA Site. — 2010. — URL: <http://www.captcha.net>.
2. T. Hastie, R. Tibshirani, J. Friedman. The Elements of Statistical Learning. — 2 edition. — Springer, 2009. — P. 764. — URL: http://statweb.stanford.edu/~tibs/ElemStatLearn/printings/ESLII_print10.pdf.