Detecting Bot Behaviour in Social Media using Digital DNA Compression

Nivranshu Pasricha **Conor Hayes**
nivranshu.pasricha@insight-centre.org

Insight
Centre for Data Analytics

Introduction

It is estimated that bots make up 9-15% of all Twitter accounts. A paradigm-shift [1] has been observed in the last few years in the behaviour of Twitter bots where more sophisticated social bots have been identified that can fool traditional bot detection techniques as well as human annotators.

Digital DNA

We assume that the long-term behaviour of a bot account is less random than the behaviour of a genuine user and we model the temporal activity [3] of a Twitter account using the technique of digital DNA [2] with the following alphabet:

$$\mathbf{B}^{3}_{type} = \left\{ \begin{array}{l} \mathsf{A} \leftarrow \text{tweet}, \\ \mathsf{C} \leftarrow \text{reply}, \\ \mathsf{T} \leftarrow \text{retweet} \end{array} \right\}$$

String Compression

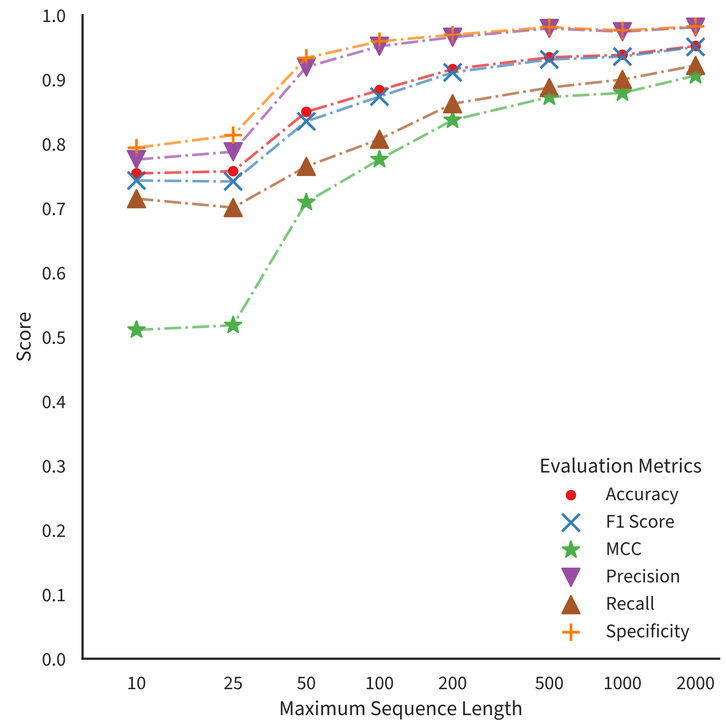
A string s = "ACTCATTTTA" can represent a sequence of 10 posts made by an account. We employ a string compression algorithm on such digital DNA sequences and use the compression statistics as features to train a logistic regression model that classifies Twitter accounts as bots or genuine users.

Figure 1: Compression statistics for Digital DNA sequences.

Length of Digital DNA Sequence

We set different limits $L = \{10, 25, 50, 100, 200, 500, 1000, 2000\}$ for the maximum length of the DNA sequence and for each account, we pick a DNA sub-sequence of random length between 1 and L. We observe great improvements in the performance as the DNA sequence length increases.

Figure 2: Results with different values for maximum sequence length L.



Conclusion & Future Work

Our approach is a fast and scalable extension on the idea of digital DNA, which is language and content independent as well as easy to represent visually. Future work can incorporate other user-profile and content-based features into the digital DNA sequence and apply this technique to identify automated accounts on other social media platforms such as Facebook and Reddit.

References

[1] S. Cresci, R. Di Pietro, M. Petrocchi, A. Spognardi, and M. Tesconi. The paradigm-shift of social spambots: Evidence, theories, and tools for the arms race. In *WWW '17 Companion*, pages 963–972, 2017.

[2] S. Cresci, R. D. Pietro, M. Petrocchi, A. Spognardi, and M. Tesconi. Social fingerprinting: Detection of spambot groups through dna-inspired behavioral modeling. *IEEE Transactions on Dependable and Secure Computing*, 15(4):561–576, July 2018.

[3] A. Kan, J. Chan, C. Hayes, B. Hogan, J. Bailey, and C. Leckie. A time decoupling approach for studying forum dynamics. *World Wide Web*, 16(5): 595–620, Nov 2013.

Results

Table 1: Comparison of our bot detection technique based on String Compression with the k-Common Substring technique from [2]. The dataset contains a random sample of genuine user accounts and a sample of bot accounts which were found to be created to target Mayoral elections in Rome, Italy.

Technique	Metrics					
	Accuracy	Precision	Recall	F-Measure	MCC	Specificity
k-Common Substring - Unsupervised [2]	0.976	0.982	0.972	0.977	0.952	0.981
k-Common Substring - Supervised [2]	0.977	0.982	0.977	0.977	0.955	0.981
String Compression - Compressed DNA Size	**0.980**	0.978	**0.981**	**0.980**	**0.960**	0.978
String Compression - Compression Ratio	**0.984**	**0.992**	0.976	**0.984**	**0.968**	**0.992**

A World Leading SFI Research Centre

This work has emanated from research supported in part by a research grant from Science Foundation Ireland (SFI) under Grant Number SFI/12/RC/2289P2.

DCU · NUI Galway OÉ Gaillimh · UCC University College Cork, Ireland Coláiste na hOllscoile Corcaigh · UCD Dublin · Science Foundation Ireland sfi For what's next