Title:	Fake Accounts Detection in Twitter based on Minimum Weighted Feature set
Author(s):	Ahmed ElAzab **Amira M. Idrees** Mahmoud A. Mahmoud Hesham Hefny
Journal/Conference:	ICDAR 2016 : 18th International Conference on Document Analysis and Recognition
Publication details:	Proceedings of the ICDAR 2016 https://www.waset.org/conference/2016/01/johannesburg/ICDAR/home
Publication Date:	January, 12-13, 2016
Publisher	World Academy of Science Engineering and Technology
Place	Johannesburg, South Africa

Paper Title:	**Fake Accounts Detection in Twitter based on Minimum Weighted Feature set**
Problem:	Social networking phenomenon has grown tremendously through the last twenty years. During this rise, the different types of social networking have created many online activities which instantly attracted the interests of large number of users where users increasingly depend on the credibility of the information exposed on Online Social Networks (OSNs). On the other hand, OSNs suffer from expanding the number of fake accounts that has been created, fake accounts means that the accounts do not match to real humans. Fakes can present fake news, web rating, and spam. OSN operators currently expend different and determined resources to detect, physically confirm, and close fake accounts. One of the main problems in social media is the scammers as they can use their accounts for different targets. One of these targets is spreading rumors which may affect a determined business or even the society as a larger segment. One of the examples in 2013, in the event of the Boston Marathon Bombing, a fake account on twitter has taken the advantage of the kindness of the people by twitting an announcement for a donation of $1 for each retweet.
Context:	According to the importance of the effect of social media to the society, in this research, the research aims to detect the fake profile accounts from twitter online social network as a step towards the detection of fake news. Different researches have been presented to detect fake accounts by introducing a set of attributes such as Fabr´ıcio2010 who identified 23 attributes, upraja 2015 identified 10 attributes. However, the research presents the minimum set of attributes that can effectively be applied in a classification technique to detect the fake account. Selecting the best classification algorithm is also provided by applying a set of algorithms using the selected set of features.
Solution approach:	We proposed an approach for detecting fake accounts on Twitter social network, the proposed approach was based on determining the minimum set of effective features for the detection process. The attributes have been collected from different research, they have been filtered by extensive analysis as a first stage, and then the features have been weighted. Different experiments have been conducted to reach the minimum set of attributes with perceiving the best accuracy results. From more than 22 attributes, the proposed approach has reached only seven effective attributes for fake accounts detection. The attributes were

	applied on five of the best classification algorithms, Random Forest, Naïve Bayes, Decision Tree, Neural Network, and SVM. The classification output have been presented with highlighting the best results We claim that these attributes can succeed in discovering the fake accounts in other social networks such as Facebook with minor changes according to the unique nature of each social network. Moreover, providing an analysis to the tweets content of the user can provide more accurate results in the detection process
Contribution:	the research contribution can be summarized as follows: 1. The minimum set of attributes for detecting the fake accounts on Twitter has been determined and tested. 2. Five of the best classification algorithms have been applied and the results have been compared 3. Evaluating both steps is applied and compared with other researchers' results which proved the advancement in the accuracy level of the proposed approach.

إسم البحث	**اكتشاف الحسابات المزيفه على تويتر طبقا لوزن خصائص الحسابات الملفات الشخصيه**
ملخص المشكلة	وفقا للدور الحيوى لمواقع التواصل الاجتماعي مثل الفيس بوك وتوتيتر ووغيرها من المواقع ومع زياده اهميتها اصبح لها تاثير في الحياه العامه للشعوب والدول وعمليات صنع القرار علي سبيل المثال ظهر تاثير تويتروالفيس بوك في نشر اعمال الفوضي والشغب في مدينه مكسيكو عام 2012 نتيجه نشر اخبار كاذبه من حسابات وهميه عن اطلاق نار في المدينه . وقد لعبت الحسابات ال مزيفه دور ا هاما فى مواقف عديدة مثل الانتخابات الامريكيه عاما 2012 في فلوريدا لحساب المرشح Romney عن مرشحه Obama حيث تبين ان عدد كبير من الحسابات الشخصيه المؤيده له علو تويتر هى حسابات مزيفه وكذلك استغلال انفجار سباق بوسطن عام 2013 للتبرع لضحايا على حساب مزيف . ولذلك كان لعمليه البحث العلمى دور ا هاما في الكشف عن الحسابات المزيفه على تويتر ومن هنا ظهرت محاولات البحث للكشف على تصنيف الحسابات الوهميه وكان ذلك طبقا للخصائص الملف الشخصى لكل حساب لذا قام الباحثون بتقديم أبحاث فى هذا الصدد والتى تعتمد على تقديم عدد من العناصر التى تستخدم لإكتشاف الحسابات المزيفه منها بحث مقدم من Fabr´ıcio Benevenuto عام 2010 والذى توصل فيه لاستخدام 23 عنصر و upraja 2015 الذى قدم 10 عناصر فقط. ومن هذا المنطلق قامت فكره هذا البحث في تصنيف أهميه تلك الخصائص وتقليص عددها لتقليل العملية المطلوبه لإستخراج وتجهيز البيانات المطلوبة ولزيادة نسبة الدقة فى إكتشاف الحسابات المزيفة
سياق البحث	فكره البحث أعتمدت على تصنيف أهميه الخصائص المستخدمه فى الكشف عن الحسابات المزيفه فى أحد أشهر شبكات التواصل الإجتماعى تويتر و إستخدام المقاييس المختلفه بهدف زياده الدقه للنتائج مع القدرة على تقليل العملية المطلوبه لإستخراج البيانات المطلوبه و تحهيزها تم استخدام البياتات التى تم استخدامها بمعهد الاتصالات والمعلومات بايطاليا ، وتم تحديد الخصائص وتطبيق ال GAIN Measure لتقييم الخصائص و تحديد أهمية كل خاصية كما تم إختيار و تطبيق خمسه من أفضل الخوزميات الخاصة بتصنيف البيانات على مجموعة الخصائص التى تم تحديدها.
إسلوب البحث	إعتمادا على دراسة وتطبيق نتائج GAIN Measure على 19 عنصر بالبيانات الخاصه بمعهد اللا تصالات بايطاليا وحساب النتائج . تم تحديد سبعه فقط من هذه العناصر عند اخد القيم الى تتعدى حاجز GAIN Measure 0.5 ثم تم تجهيز البيانات الخاصه (data set) بمعهد الاتصالات والمعلومات بايطاليا تمهيدا لتطبيق الخصائص على هذه البيانات باكثر من تجربه حيث انقسمت الي ثلاث تجارب • التجربه الاولى وهى التعامل مع كل العناصر المتاحه للملف الشخصي للحساب على تويتر وتطبيق اكثر من خوارزم وتحليل النتائج • التجربه الثانيه التعامل مع كل العناصر التى ظهرت له قيم باستخدام gain ratio حيث ظهرت بعض العناصر ذات قيم صفر مثل ان يكون للملف الشخصي اسم او صوره وبالتطبيق ظهر عدم تاثر النتائج بتلك القيم التى تساوى صفر. • التجربه الثالثه التعامل مع كل العناصر التى ظهرت له قيم باستخدام gain ratio التى تتعدى قيمه 0.5 ومع تطبيق اوسع للخوزميات عن التى استخدمها معهد الاتصالات بايطاليا مثل

	مثل Random forest و Decision Treeو Naïve Bayesو Neural Network و SVM
النتائج المستخلصة	تم تقليل عدد العناصر الخاصه بالملف الشخصي للحساب الى 7 بدلا من 22 وبدرجه دقه اعلي وقاعده اكبر للتطبيق من قبل الخوزميات مثل Random forest و Decision Treeو Naïve Bayes و Neural Networkو SVM وذلك بمعايير دقه اعلي من نتائج معهد الاتصالات والمعلومات بايطاليا حيث وصلت النتائج الى Random forest بنسبه 99.47% ودقه % 99.4مع Naïve Bayes ودقه مماثله مع خورزاميات التى تم تطبيقها في بحث معهد الاتصالات والمعلومات بايطاليا ومع تطبيق البحث على خوزميات اخرى لم يتم تطبيقها في المعهد مثل Neural Network وSVM وصلت النتائج الى 99.55%