@I seek 'fb.me': Identifying Users across Multiple Online Social Networks

Paridhi Jain†, Ponnurangam Kumaraguru†, Anupam Joshi*
†Indraprastha Institute of Information Technology (IIIT-Delhi), India
*University of Maryland, Baltimore County (UMBC), USA
{paridhij, pk}@iiitd.ac.in, joshi@cs.umbc.edu

ABSTRACT

An online user joins multiple social networks in order to enjoy different services. On each joined social network, she creates an identity and constitutes its three major dimensions namely profile, content and connection network. She largely governs her identity formulation on any social network and therefore can manipulate multiple aspects of it. With no global identifier to mark her presence uniquely in the online domain, her online identities remain unlinked, isolated and difficult to search. Literature has proposed identity search methods on the basis of profile attributes, but has left the other identity dimensions e.g. content and network, unexplored. In this work, we introduce two novel identity search algorithms based on content and network attributes and improve on traditional identity search algorithm based on profile attributes of a user. We apply proposed identity search algorithms to find a user's identity on Facebook, given her identity on Twitter. We report that a combination of proposed identity search algorithms found Facebook identity for 39% of Twitter users searched while traditional method based on profile attributes found Facebook identity for only 27.4%. Each proposed identity search algorithm access publicly accessible attributes of a user on any social network. We deploy an identity resolution system, *Finding Nemo*, which uses proposed identity search methods to find a Twitter user's identity on Facebook. We conclude that inclusion of more than one identity search algorithm, each exploiting distinct dimensional attributes of an identity, helps in improving the accuracy of an identity resolution process.

Categories and Subject Descriptors

H.3.3 [**Information Search and Retrieval**]: Search process; H.3.5 [**Online Information Services**]: Web-based services

Keywords

Online Social Networks, Identity search, Identity resolution, Privacy, Digital footprint

1. INTRODUCTION

Over the last decade, multiple online social networks have been introduced in webosphere e.g. Facebook, Twitter, Pinterest, etc. Each online social network follows a unique set of protocols to facilitate information sharing and to maintain social connections. Different ways in which social networks operate, attract users to exploit each social network for a different purpose. For instance, users may exploit LinkedIn for professional connections while Facebook for personal connections [1], and may use Twitter for public information sharing while Facebook for restricted information sharing. To practice services offered by each social network, users then become members of multiple social networks.

On each social network, a user defines her online identity which includes a set of attributes that describes her uniquely and differentiate her from others. User's online identity includes her username, her profile, her friends network, and the content she creates or that is shared with her. Her online identity creation process on each social network gives her a large control on how she can choose to give / hide / skip her identity attributes and therefore her identity attributes may vary largely across multiple social networks. With no handle / identifier / attribute for a user to mark her presence uniquely across online social networks, her multiple social network identities remain un-linked with each other. Because of varied and non-linked identities of a user, it is difficult to find them and match them together. The problem of finding and establishing identities of a user on other social networks, given her identity on one social network, is termed as *"Identity Resolution in Online Social Networks"*.

Solutions to the problem have multiple application domains. In security domain, our solution can help searching for malicious user's multiple online identities. Malicious users exploit online social media for activities such as Phishing, Spam, Identity theft, etc. Such malicious users create multiple accounts on different networking sites to enhance reachability to targets (victims). To identify malicious users, security researchers have devised features on Twitter [2, 3, 4, 5], YouTube [5], Myspace [6] and other social networks. Solutions suggested to detect malicious user accounts are network dependent, hence security analysts need to identify malicious accounts on each networking site. In order to reduce identification cost and efforts, linking malicious user identities present on multiple online social networks is suggested. However in real world, malicious users demonstrate active obfuscation of their attributes to avoid detection and linkage of their multiple identities. To address this challenge, behavior based identity resolution (based on content and network attributes) can help in finding and linking malicious user's identities across social networks. In privacy domain, the problem finds its application in understanding the quantity and quality of the user's information leakages

WWW 2013 Companion, May 13–17, 2013, Rio de Janeiro, Brazil.
ACM 978-1-4503-2038-2/13/05.

via either aggregation of user's information from multiple social networks or differences in privacy policies of multiple social networks [7, 8, 9, 10]. System analysts then can improve privacy policies and anonymization methods to preserve user's privacy. In recommendation domain, our solution can help in building friend recommendation feature. The recommendation feature can find a user's friends' identities on multiple social networks with their information on one social network and can suggest her to connect to the suggested friends' identities.

Identity Resolution problem can be divided into two subproblems namely, *Identity Search* and *Identity Matching*. Literature has proposed multiple identity matching methods to connect various identities but has not explored identity search methods to find similar identities, to their potential. In this paper, we propose novel identity search methods to improve accuracy of an identity resolution process in online social networks. We experiment with the proposed identity search methods and existing identity matching methods on two popular and significantly different online social networks – Twitter and Facebook. We show that exploiting multiple identity search methods, surfaces the identities similar to the given identity in different aspects other than the traditional ways (e.g., similar name) and therefore, increases the accuracy of finding correct identities users across social networks.

2. NOTATIONS AND DEFINITIONS

2.1 Identity

Definition: An identity of a user on an online social network is composed of three dimensions of attributes – Profile, Content and Network. Profile is composed of set of attributes which describes her persona such as username, name, age, location, etc. Content is composed of attributes which describes the content she creates or is shared with her such as text, time of post, etc., and Network is composed of connection attributes which describes the network, she creates to connect to other users such as number of friends. A real-world user is denoted by I and her identity on a social network SN_A is denoted by I_A.

2.2 Identity Resolution

Problem Definition: *Given an identity I_A of user I on social network SN_A, find her correct identity I_B on social network SN_B.*

$$I_A \rightarrow \{I_B\}$$

Generic Methodology: The process of identity resolution in online social networks follows two subprocesses – identity search and identity matching. Identity search process lists a set of candidate identities on SN_B, which are similar to given identity I_A and possibly belong to user I. Identity matching process then calculates the similarity score between I_A and every candidate identity returned by identity search process, on certain metrics. Candidate identities are then ranked on the basis of similarity score, and the candidate identity with highest match-score is returned as I_B.

2.3 Identity Search

Problem Definition: *For a user I, given her identity I_A on social network SN_A and a search parameter S, find a set of identities I_{Bj} on social network SN_B such that $S(I_A) \simeq S(I_{Bj})$.*

$$\{I_A, S\} \rightarrow \{I_{B1}, \ldots, I_{Bj}, \ldots, I_{BN}\}$$

Each identity I_{Bj} in the set is termed as *candidate identity* and the set as *candidate set*. The size of the candidate set is termed as *candidate set size* and is denoted by N.

Generic Method: Any search method takes a source and a set of search parameters as input and retrieves a set of candidate items which hold similar values for the search parameters. For an identity search algorithm, source can be given identity I_A and search parameters can be I_A's attributes defined on her three identity dimensions namely profile, content, and network. *Identity Search by profile*, implies searching for candidate identities on SN_B by profile attributes as search parameters extracted from I_A. The candidate identities I_{Bj} returned are similar to I_A in terms of profile attributes as username, name, gender, school, education, etc. *Identity Search by content*, implies searching for candidate identities on SN_B with content attributes of I_A as search parameters. The candidate identities I_{Bj} returned are similar to I_A in terms of content creation, URLs posted, platform used for content creation, timestamp, etc. *Identity Search by network*, implies searching for candidate identities on SN_B by network attributes of I_A as search parameters. The candidate identities I_{Bj} are similar to I_A in terms of friends, network in-degree, network out-degree, etc.

2.4 Identity Matching

Problem Definition: *Given an identity I_A of user I on social network SN_A, a set of candidate identities $Q = \{I_{B1}, \ldots, I_{Bj}, \ldots, I_{BN}\}$ on social network SN_B and a match function M, locate an identity pair (I_A, I_{Bj}) such that $M(I_A, I_{Bj}) = \max\{M(I_A, I_{B1}), \ldots, M(I_A, I_{BN})\}$. I_{Bj} with highest match score is inferred as I_B.*

$$\{I_A, Q, M\} \rightarrow \{I_A, I_{Bj}\} \rightarrow I_B$$

Generic Method: An identity matching algorithm identifies the correspondence between identity I_A and each candidate identity I_{Bj} by calculating a match score $M(I_A, I_{Bj})$ between their respective identity parameters and then rank the candidate set on the basis of match score. Candidate identity I_{Bj} with highest match score is concluded as I_B.

Match score between two identities can be calculated by methods as syntactic matching methods, semantic matching methods, image matching methods, graph matching methods, and crowd-sourced based matching algorithms, applied on identity parameters such as profile, content and network. Syntactic and Semantic matching methods calculate metrics as edit distance, jaccard distance, jaro distance, soundex, ontology matching, etc. on string based profile or content attributes of two given identities I_A and I_{Bj} (e.g., name, username, location, school, content). Image matching algorithms calculate similarity between profile (background) images used by two identities. Graph matching methods calculate the friend network structure similarity of two identities. Crowd-sourced matching methods generate human intelligence tasks to associate a match score to each candidate identity, on the basis of their background knowledge and apprehension.

3. RELATED WORK

To the best of our knowledge, researchers have exploited *only* profile attributes (private and public) to search for a set of candidate identities of a user on social network SN_B, given her identity on social network SN_A [1, 11, 12, 13]. Researchers then select any of the identity matching methods – Syntactic matching [1, 13, 14, 15, 16], Semantic matching [17, 18, 19, 20], Crowd-sourced matching [11], and Graph matching [21, 22], to match and rank candidate set and infer the most similar candidate identity as I_B.

Identity Search algorithms on the basis of profile attributes are effective but have limitations and have not been exploited to its potential. Firstly, search by profile attributes is highly restrictive, and dependent on the availability of same profile attributes across networks. For example, 'gender' profile attribute is available on Facebook while no such attribute exists on Twitter. Location profile attribute is public in Twitter while is private on Facebook. Therefore, a search algorithm may have access to limited profile attributes to use as search parameters. Secondly, search by limited profile attributes results in large number of candidate identities which have similar profile attributes e.g. same name, similar username or similar location. Matching large number of candidate identities becomes computationally expensive and time consuming. Thirdly, search by profile attributes may miss identities for those users, who use significantly different profile attributes across social networks, either purposely or unintentionally. For such users, candidate set may never contain the correct identity of the user. This results in lower accuracy of complete identity resolution process. Fourthly, URL attribute of a profile has been discussed in literature but has not been exploited in any of the profile based identity search methods. We think that URLs mentioned as a profile attribute on one social network may help in locating a user's identity on other social networks.

Therefore, we hypothesize that search by limited profile attributes may not give satisfying results. We observe that search methods on the basis of content and network attributes remain unexplored. Content and Network attributes are important aspects of a user's identity on a social network. Due to advanced services to push content simultaneously on multiple online social networks, users post same / similar content across networks. Search by content can help in finding such users' identities across networks. Further, a segment of users tend to connect with similar people across social networks [1] and therefore search by network, may also help in finding the identities of a user across networks. In this work, we attempt to understand if inclusion of search methods based on an identity's content and network attributes, along with search methods based on an identity's profile attributes can help in improving the accuracy of the identity resolution process in online social networks. We do not experiment with identity matching methods' improvisation but exploit the identity matching techniques already used in literature, to clearly comprehend the effect of content and network identity search methods. We devise our methods for two popular online social networks, Twitter and Facebook, which exploits *publicly accessible data* only to avoid any user authorization. Given a user's identity (I_A) on Twitter (SN_A), we return user's correct identity (I_B) on Facebook (SN_B).

3.1 Contribution

We show that combination of content and network based identity search methods with improved profile search method, helps in identifying correct Facebook identity for 39% of Twitter users queried, as compared to traditional profile based search method, which returns correct Facebook identity for 27.4% only. We, therefore, observe an increase in the accuracy of an identity resolution process by 11.6%. Further, we achieve a mean average precision of 0.83 for the identity resolution process with profile, content and network identity search methods and image-based identity matching method. In other words, our identity resolution process returns the correct Facebook identity of 39% Twitter users within top-2 ranks.

We infer that using different identity search algorithms based on different identity dimensions help in two ways – **Narrowing** the correct identity by filtering out the candidate identity, returned by more than one identity search method and **Expanding** the candidate set, by including all identities which are similar to the given identity in any dimension. Other contributions and observations are –

- We demonstrate that a user's public Facebook friendlist can be created automatically and chronologically by exploiting public activity feed of a user. The bug can be exploited to not only know "who is friends with whom" but also "when who became friends with whom" on Facebook.
- We observe that males and females are equally unaware of their identity leaks which may further lead to consequent privacy leaks, as compared to the literature which proves that females are more privacy concerned than males. However, the validation of the observation demands a bigger user base.
- We observe that users often leak their identity on multimedia social networks via URLs posted in their tweets. Such identity leaks can be exploited to build a user's unique footprint and infer diverse information about her. We leave the task of a comprehensive analysis on our future work.

The paper is organized as follows: Section 4 describes the identity search and Section 5 describes identity matching methods we use, Section 6 describes the methodology by which we implement an identity resolution system, Section 7 evaluates identity resolution system and therefore the proposed identity search methods on a set of metrics, Section 8 presents some preliminary observations, and Section 9 discusses the implications of better search methods for identity resolution process, limitations and future directions.

4. IDENTITY SEARCH METHODS

In this section, we discuss the identity search methods proposed to search for a user's candidate identities on Facebook. We explain a set of methods which exploits available information of I_A on Twitter, to search for her identity on Facebook. The methods are – **Profile Search**, **Content Search**, **Self-mention Search** and **Network Search**. The methods access only publicly available data about any user, as compared to other algorithms proposed in literature which were allowed to access detailed information about a user as discussed in Section 3. We now discuss each of the methods in detail.

4.1 Profile Search

An identity of a user on a social network includes a set of profile attributes, which gives basic information about the user such as username, name, location, gender, description, etc. If the user does not demonstrate any active obfuscation and does not create altogether a different identity, it is likely that she re-uses certain profile attributes' value, on the social networks she joins. If the user demonstrates such behavior, profile attributes can be used as a search parameter S to find her identity on other social networks. Further, to make comparisons between any two identities using profile attributes, it is essential to have same set of attributes publicly available for both identities. Twitter has a limited set of attributes however publicly available [1] while Facebook has larger set of attributes, however private. We consider only those profile attributes which are publicly available on both networks – username, name, profile image and URL. Using the value of the mentioned profile attributes of I_A on Twitter, we search Facebook for candidate identities with similar profile attributes. We add location as another attribute available on Twitter to refine the search on Facebook. The search produce a list of candidate identities with same attribute values as of I_A on Twitter. The flow of the Profile Search algorithm is illustrated in Figure 1.

Firstly, we use I_A's username on Twitter, and query Twitter API to extract her name, username, location, profile image and URL. We use URL attribute first to observe if I_A herself has given her Facebook identity (I_B). We term this behavior of mentioning one's Facebook network identity (or any other network identity) on Twitter explicitly, as "*Self-Identification*". We observed two varieties of self-identification behavior – one in which a user directly gives her Facebook identity on her URL attribute and other in which a user indirectly gives her Facebook identity via referring to a webpage on her URL attribute, that contains her Facebook identity. A user referring to her blog on Twitter URL with her blog having her Facebook identity is an example of indirect self-identification. If I_A has not identified herself via URL, we use her username, name and location attribute to query Facebook Graph API to find identities with same or similar username / name having the same or similar location. Facebook Graph API returns a set of searchable [2] identities (users, pages and communities) who either have same name as the "queried" name or a part of "queried name" in their name and share "queried" location. [3] We also search for a candidate identity on Facebook who has the same username as I_A's Twitter username. The reason for the "same username" search is motivated by the previous research which shows that many users have same username across social networks [23]. Therefore, there is a possibility that I_A have the same username on Facebook as on Twitter. We aggregate I_A's candidate identities on Facebook as returned by Facebook Graph API and term the set as "Non-ranked" set, as we are unsure of ranking algorithm used by Facebook Graph API to rank the candidate set returned.

[1] Accessible to any user on the Internet.
[2] Users who allow to be searched within Facebook and do not have this feature turned off in privacy settings.
[3] "Queried" name is I_A's name on Twitter.

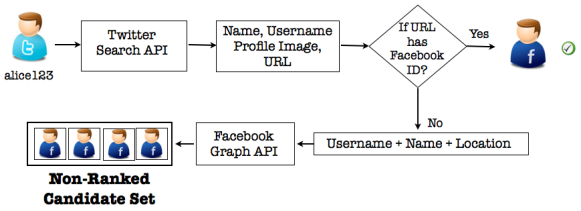

Figure 1: Profile Search Algorithm. In this method, we use profile attributes of a Twitter user as search parameters to search her Facebook identity.

4.2 Content Search

An identity of a user on a social network includes the content that she creates or is shared with her. Owing to the popularity of social aggregation sites and ways to link multiple networks together, a user is facilitated with a choice to push the same content on multiple networks simultaneously. For example, Twitter provides a functionality to connect Twitter and Facebook identity to post user's tweets on her Facebook timeline, Twitterfeed [4] allows a user to connect Twitter, Facebook, and LinkedIn to push feeds in three social networks simultaneously. Because of such services, it is likely that a user generates same content on multiple social networks. Such a user behavior can be exposed by Twitter API which provides the "source" of a tweet i.e. from where the tweet is posted e.g. Facebook, Twitterfeed, etc. Source can be exploited to reduce the search space for a user's online identities, if an analyst intend to save her efforts by searching for a user in only social networks where she has hints of her existence. Content Search method uses content as a search parameter S for users who use the mentioned services. In this paper, we do not use source of the tweets since we limit our focus to search for I_A's identity only on Facebook and with the help of ground truth we know the I_A has a Facebook identity. However, we plan to use this information to search for any user in online social media in our future work.

Figure 2 explains the flow of content search algorithm. We extract most recent 100 (or less) [5] posts by I_A on Twitter, and process each of the posts to limit the length to 75 characters and to remove non-ascii characters. We query Facebook Graph API with the processed post to search for the users who posted same or similar content on Facebook. Facebook Graph API returns a candidate set of Facebook identities of users who posted similar content as queried content. We are unsure of the algorithms Facebook Graph API use to retrieve candidate identities who posted same / similar content, however with no other choice, we filter out candidate identities with zero cosine similarity between the post created by them and the queried post. Cosine similarity between two posts is calculated as,

$$Cosine\_sim(I_A, I_{Bj}) = \frac{\overrightarrow{P_{I_A}}.\overrightarrow{P_{I_{Bj}}}}{|\overrightarrow{P_{I_A}}||\overrightarrow{P_{I_{Bj}}}|}$$

[4] http://www.twitterfeed.com
[5] We limit to process most recent 100 tweets to avoid long execution time.

where $\overrightarrow{P_{I_A}}$ and $\overrightarrow{P_{I_{Bj}}}$ are word-frequency vector of post by I_A and post by candidate identity I_{Bj}, respectively.

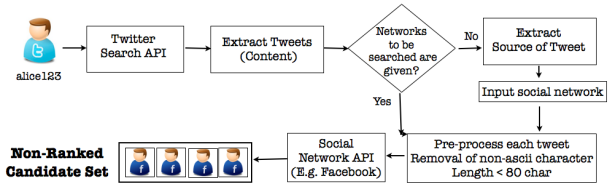

Figure 2: Content Search Algorithm. In this method, we use content created by a Twitter user as search parameter to search her Facebook identity.

4.3 Self-mention Search

This method exploits a user's tendency to cross-pollinate information on Online Social Media [24] and was introduced by Correa *et al.* [23]. The method explores content attributes of I_A and assumes that if I_A has accounts on two or more networks, she might cross refer to her other account, in few of her tweets. For example, I_A might post a tweet with a URL referring to an album on Flickr, indirectly revealing her Flickr identity. We term this behavior of posting URLs indirectly but consciously, pointing to user's other network identity as "*Self-mention*". Self-mention behavior allows identity leaks via content created in the form of URLs by the user. This method exploits self-mention behavior to search for a user identities across networks.

Figure 3 illustrates the algorithm. We query Twitter Search API to extract 100 (or less) recent tweets by I_A and filter out the tweets with URLs and then further process each URL to verify if it refers to Facebook. We create a set of all the Facebook URLs posted by I_A, query Facebook Graph API to process each URL and extract identity of the candidate user (if the URL refers to a user's identity and not apps), thereby creating a set of candidate identities.

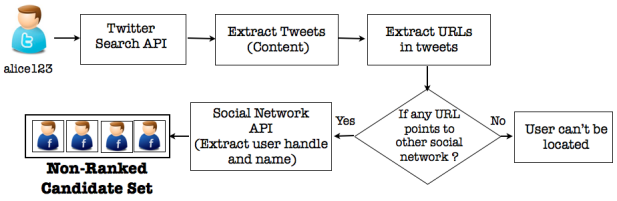

Figure 3: Self-mention Search Algorithm. In this method, we use content attribute of a user to observe if a user herself has posted a link to her Facebook post / identity.

4.4 Network Search

Network is an important dimension of a user's identity on a social network. It is a dimension of a user, which is defined with the involvement of other users apart from user herself [25], as compared to other dimensions where other users are not associated for the dimension existence. In other words, a user needs other users to define her network attributes but not her profile attributes. If a user leaks her identity on any other social network, it is likely that identities of users associated with her may also get leaked. Network Search algorithm explores the possibility of a user's identity leak via her network attribute.

We search for I_A's identity on Facebook using her follower and followee network, collectively termed as *connection network*. By exploiting self-identification behavior of users in connection network of I_A on Twitter, her *candidate friend-neighborhood* on Facebook is identified. A candidate friend-neighborhood of I_A is composed of Facebook users whose Twitter identities follow I_A or whom I_A follows on Twitter. Facebook users in the candidate friend-neighborhood of I_A are then queried via Facebook Graph API, to retrieve their Facebook friend-neighborhood. We assume that I_A connects to a same subset of users on both social networks. Therefore, a Facebook identity present in friend-neighborhood of more than one user in candidate friend-neighborhood, may be a candidate identity of I_A on Facebook, since the candidate identity connects to same users on Facebook as I_A connects to on Twitter. In this way, we try to map I_A's identity from one social network to another via mapping her connection network on two social networks (see Figure 4). Note that the method is applicable, even when the incomplete friend-neighborhood of any user are available, as compared to other graph based search methods, which require complete friend-neighborhood of multiple users to find I_B [21].

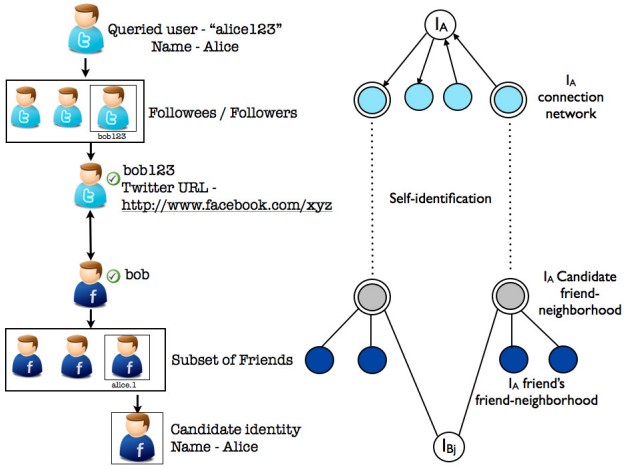

Figure 4: Network Search Algorithm. In this method, we use I_A's Twitter network to locate her identity on Facebook.

In a nutshell, we experiment with all the three major dimensions of a user's identity on a social network. We observe that some users consciously give their Facebook identity by self-identification, and self-mention while other users are uninformed with no intensions of giving their Facebook identity e.g. identity leak via name, location, content and network. We now discuss identity matching methods we used for identity resolution process.

5. IDENTITY MATCHING METHODS

Given a set of candidate identities on Facebook, we use the following methods to first match a pair of Twitter identity and each candidate identity – **Syntactic Matching**, **Image Matching**. We then rank the candidate set on the basis of the match-score associate with each candidate set.

The aim of ranking the candidate set is to retrieve the correct Facebook identity of the queried user, within top results, in order to avoid a scan through the complete candidate list. The ranked candidate set is then presented to a human manual verifier to locate the correct identity among the candidate identities. We chose manual verification on the ranked candidate set, in order to capture gender, age, and other attributes which are difficult to capture via automated methods. We assume that the human verifier is 100% accurate, in making the inferences. In this work, authors are the human verifiers. We now discuss each identity matching method in detail.

5.1 Syntactic Matching

We exploit standard syntactic matching methods to compare the string, numeric and character type attributes of the two identities. Given Twitter identity and a candidate identity returned from Profile Search, Content Search, Network Search and Self-Mention Search, we used Jaro distance [26] metric to compare their username and name attributes. Closer the match, smaller is the value of Jaro distance metric.

5.2 Image Matching

There have been instances where users put same profile image on their multiple online identities. It is therefore easier to infer that identities with closest profile image match, belong to the same user. We used standard RGB-histogram image matching algorithm, to generate a score between profile image of the given Twitter identity and the candidate identity, given by –

$$IM_s(I_A, I_{Bj}) = \sqrt{\frac{(h_{I_A} - h_{I_{Bj}})^2}{N_s}}$$

where h_{I_A} and $h_{I_{Bj}}$ are RGB histograms of Twitter identity profile image (social network A) and candidate identity profile image (social network B), respectively and N_s is the size of h_{I_A}. If two images are exactly the same, IM_s is zero, else any positive number. Closer the match, smaller is the value of the metric.

6. METHODOLOGY

We combine the discussed identity search methods and identity matching methods to create a semi-automated system, named as *Finding Nemo*. [6] Finding Nemo takes a Twitter identity as input and run profile, content, self-mention and network based identity search methods. Candidate identities returned by each method are collected. If there exists an identity returned by more than one search method or if an identity is exposed via URL attribute of the Twitter identity (self-identification), the identity is returned as the correct Facebook identity. The reason for such a decision is that if an identity herself declares her on other social network via URL attribute, any matching methods are not necessary to confirm the claim. Further, if a candidate identity is returned by more than one method, the returned candidate identity is similar to the queried Twitter identity, in more than one aspect, thereby strengthening the fact that the candidate identity is correct Facebook identity of the queried Twitter identity. In all other cases, candidate identities of multiple search methods are collated together and are ranked using identity matching methods – syntactic (username, name), image (profile image). The ranked candidate identities are then presented to a human verifier to locate the correct Facebook identity out of the ranked candidate identity set, if exists. Since we observed that the manual verifiers have to bear less cognitive load in order to identify a match, when the ranked candidate identities are presented with auxiliary information such as, profile image, name, username and gender, we assume that human verifier is 100% accurate and therefore, decision by manual annotation is valid. Facebook identity annotated by a human verifier as the correct Facebook identity for the given Twitter user, is then returned. Figure 5 shows the architecture diagram of Finding Nemo.

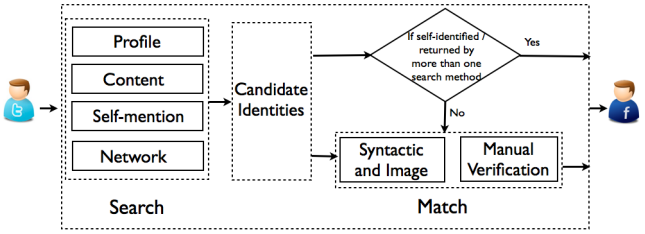

Figure 5: Architecture and Methodology of Finding Nemo.

7. EVALUATION OF IDENTITY RESOLUTION SYSTEM

To evaluate the identity resolution system (Finding Nemo), we borrowed a ground truth dataset from [12] collected from Social Graph API. The dataset consisted of 543 users who themselves mentioned their identity on multiple social networks including Twitter and Facebook. With the dataset of 543 users denoted by U_{total}, we measured the efficiency of the system, and therefore identity search algorithms on two evaluation metrics – Accuracy, and Mean Average Precision (MAP). We define each of the evaluation parameters as follows.

- **Accuracy** - Accuracy of the system is defined as ratio of users for whom correct Facebook identity is identified ($U_{correct}$) and users for whom Facebook identity is searched. It measures the effectiveness of the system in retrieving the correct Facebook identity of the queried user. Higher the accuracy, better is the system. Formally, accuracy is given by

$$Accuracy = \frac{U_{correct}}{U_{total}}$$

- **Precision:** Mean Average Precision (MAP) of the system is defined as,

$$MAP = \frac{1}{U_{correct}} \sum_{j=1}^{U_{correct}} \frac{1}{R_j} \sum_{k=1}^{R_j} P(cand_k) * rel(cand_k)$$

where $U_{correct}$ denotes the set of users for whom precision is non-zero, R_j denotes the number of relevant (correct) identities for the queried user j, $P(cand_k)$ is

[6] http://precog.iiitd.edu.in/research/findingnemo/

calculated as precision of candidate identity $cand_k$ and $rel(cand_k)$ is 0 or 1, if $cand_k$ is relevant or not. In our case, there is only one relevant identity for any user, [7] therefore MAP reduces to –

$$MAP = \frac{1}{U}\sum_{j=1}^{U} P(cand_k) * rel(cand_k)$$

MAP measures how early the system returns the correct Facebook identity of the queried user. Higher the MAP, higher is the rank at which correct Facebook identity is returned, on an average and therefore, better is the system.

We evaluated the system on a Ubuntu server with six quad core processors each of 1.87GHz speed, 16Gb RAM, 8Gb cache size.

7.1 Accuracy

We measured the effectiveness of Finding Nemo by querying the system with a dataset of 543 users. We observed that for 212 Twitter users (39.0%), correct Facebook identity was identified by the system. Table 1 lists the split each search algorithm contributed to surface the correct Facebook identity in the returned candidate set resulting in the overall accuracy of 39.0% for the system.

We further compared our systems' identity search methods with the traditional profile search methods used in literature, assuming only public profile attributes are available. Traditional profile search method finds candidate identities on the basis of search parameters – username, name and location. To the best of our knowledge, no profile search method exploited an important profile attribute, URL attribute of an identity, to understand if a user herself has directly or indirectly self-identity themselves. We included the URL attribute and improvised profile search method, as discussed in Section 4.1. Table 2 shows a comparison of using traditional profile search methods with improvised and proposed identity search methods, to search for a user's Facebook identity. We observe that 11.6% of the users were not identified by the traditional search method, however were identified by the combination of improvised profile and proposed identity search methods.

Search Algorithm	# of users identified	Accuracy
Profile Search (P)	205	37.7%
Content Search (C)	3	0.5%
Self-mention Search (SM)	31	5.7%
Network Search (N)	1	0.2%
Finding Nemo	212	**39.0%**

Table 1: Accuracy of each search algorithm, and the system Finding Nemo. Note that, a correct Facebook identity can be retrieved by more than one search methods.

Search Algorithm	# of users identified	Accuracy
P (without URL)	149	27.4%
P (with URL) + C + N + SM	149+56+6+1 = 149+71	27.4% + **11.6%**

Table 2: Contribution of an accuracy of 11.6% with improvised and proposed identity search algorithms to the traditional profile search method discussed in literature.

7.2 Mean Average Precision (MAP)

MAP score calculates the average precision of the system by incorporating the rank at which the correct identity is retrieved in the candidate set. To retrieve the correct candidate identity in the top results, candidate set returned was ranked with identity matching methods. We compare MAP score of the identity resolution system with each of the identity matching method used for ranking the candidate set (see Table 3). We observed that MAP score was highest when candidate set was ranked on profile image similarity of the candidate and given Twitter identity, using image matching method (0.83). This implies that on for a Twitter user, correct Facebook identity was returned at either rank 1 or rank 2, within the candidate set, ranked with profile image similarity.

Identity Matching Method	MAP Score
Image (profile image)	0.83
Syntactic (username)	0.76
Syntactic (name)	0.80

Table 3: MAP score comparison for two identity matching methods. We observe that ranking candidate set on the basis of profile image retrieves the correct Facebook identity earlier.

Therefore, evaluation scores suggest that inclusion of proposed and improvised identity search algorithms improved the accuracy of the system and image-based identity matching method confirmed a high average precision.

8. OBSERVATIONS

In this work, we made few interesting observations discussed below.

8.1 Gender classification

We investigated the categories of the users who were identified by the system. Table 4 lists the gender and category of Twitter users correctly identified on Facebook. Earlier studies in the privacy domain reports that females are more privacy concerned and identity restrictive than males [27, 28], however we observed that irrespective of the gender of the user, identity is often leaked by user herself via multiple ways. Therefore, males and females both are equally unaware and un-protective of their identity leaks across social networks. We leave the generalization of this observation to the future work.

8.2 Identity Exposure

Apart from Facebook, we observe that users often self-mention their identities on popular photo sharing and video sharing social networks, via URLs posted in tweets pointing to the pictures / videos uploaded on the networks. Table 5 shows the ranked list of the social networks embedded

[7] We assume that no user in the dataset maintains more than one identity across online social networks.

Attribute leak	Males	Females	Business / Professionals
URL attribute leak	48	47	42
Same username leak	37	29	14
Name + Location leak	59	48	30
Content leak	0	0	3
Self-mention leak	6	3	22

Table 4: Gender based comparison of users who leaked their Facebook identity on Twitter. We observer that gender has no role to play in identity leak concerns. Note that, males and females equally leak their identity via URL attribute.

in URLs posted by randomly selected 2,132 Twitter users. With multiple exposed identities of a user, a detailed footprint can be created by aggregating user's details from variety of social networks, which may lead to exposure of certain private attributes e.g. gender, date of birth, family, etc.

Social Network	% of users
Instagram	36.6
Youtube	29.7
Foursquare	6.1
Tumblr	6.0
Yfrog	4.0

Table 5: Popular Social networks embedded in the URLs posted by Twitter users. Users self-mention their identities on other social networks via posts referring to picture, video, location, etc., which if combined together, can lead to privacy leaks.

8.3 Automated Facebook Friendlist

Users on Facebook are given a choice to make their friend-list public or private. For a user with public friends, any other Facebook user can access the user's friend-list, however friend-list is not retrievable via Facebook Graph API. We observed that partial user's public friend-list can be extracted automatically via her public activity feeds. Whenever a user becomes friends with another user on Facebook, an automated activity feed is created saying "user X and Y are now friends" with date and time stamp. Capturing such public activity feeds may not only help an attacker to create a (partial) friend list of a user automatically, but also to rank them chronologically. We think that inaccessibility of a user's Facebook friends via Facebook Graph API, but via public activity feed is a clash. Further, we think that retrieving Facebook friends of a user chronologically may invite attackers to exploit the recency of friendship in variety of ways. We created 158 users' (partial) Facebook friend-list, via automatic methods by capturing public feeds.

9. DISCUSSION AND FUTURE WORK

To summarize, we make an attempt to address the problem of identity resolution in online social networks. We propose novel identity search algorithms which access public information only to find candidate identities. We use traditional identity matching algorithms to match candidate identities with the given identity. We show that combination of various identity search methods exploiting distinct identity attributes, helps in finding the correct identities of a user across online social networks. We understand that better search methods exploiting other identity attributes, not included in this work, may further help in increasing the accuracy of the identity resolution process e.g. timestamp distribution of the content created by a user across networks. We understand that the evaluation results may be biased to the dataset used, and may be altogether different for a bigger or rather different dataset. However, we claim that even if numbers might not be the same, accuracy will improve with inclusion of different search methods. We think that our system, Finding Nemo, can also be used by analysts to find flagged user identities (e.g. spammers) across networks as well as by users themselves to understand their identity leaks and become more cautious. Even though this work has focused on Twitter and Facebook, we believe that extension of identity search methods proposed in this work, can be applied to similar social networks as Twitter and Facebook with minor tweaks. However it'll be interesting to see how different such methods would be if applied to other different social networks.

10. ACKNOWLEDGMENTS

The authors would like to thank TCS Research Fellowship Program for their support, and all members of PreCog research group at IIIT-Delhi for their valuable feedback and suggestions. Special thanks to Anshu Malhotra and Luam Totti for sharing the dataset and Siddhartha Asthana for his feedback during the development of this paper.

11. REFERENCES

[1] M. Motoyama and G. Varghese, "I seek you: searching and matching individuals in social networks," in *Proceedings of the eleventh international workshop on Web information and data management*, ser. WIDM, 2009.

[2] C. Grier, K. Thomas, V. Paxson, and M. Zhang, "@spam: the underground on 140 characters or less," in *Proceedings of the ACM conference on Computer and communications security*, ser. CCS, 2010.

[3] F. Benevenuto, G. Magno, T. Rodrigues, and V. Almeida, "Detecting spammers on Twitter," in *Proceedings of the Annual Collaboration, Electronic messaging, Anti-Abuse and Spam Conference (CEAS)*, 2010.

[4] Z. Chu, S. Gianvecchio, H. Wang, and S. Jajodia, "Who is tweeting on Twitter: human, bot, or cyborg?" in *Proceedings of the 26th Annual Computer Security Applications Conference*, ser. ACSAC, 2010.

[5] F. Benevenuto, T. Rodrigues, V. Almeida, J. Almeida, and M. Gonçalves, "Detecting spammers and content promoters in online video social networks," in *Proceedings of the 32nd international ACM SIGIR conference on Research and development in information retrieval*, ser. SIGIR, 2009.

[6] D. Irani, S. Webb, and C. Pu, "Study of Static Classification of Social Spam Profiles in MySpace," in *ICWSM*, 2010.

[7] B. Krishnamurthy and C. E. Wills, "On the leakage of personally identifiable information via online social networks," ser. SIGCOMM, 2010.

[8] T. Chen, M. A. Kaafar, A. Friedman, and R. Boreli, "Is More always Merrier?: a Deep Dive into Online Social Footprints," in *Proceedings of the ACM Workshop on online social networks*, ser. WOSN, 2012.

[9] E. Zheleva and L. Getoor, "To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles," in *Proceedings of the 18th international conference on World wide web*, ser. WWW, 2009.

[10] O. Goga, H. Lei, S. H. K. Parthasarathi, G. Friedland, RobinSommer, and R. Teixeira, "On exploiting Innocuous User Activity for Correlating Accounts across Social Network Sites," 2012.

[11] M. Shehab, M. N. Ko, and H. Touati, "Social networks Profile Mapping using Games," in *Proceedings of the 3rd USENIX conference on Web Application Development*, ser. WebApps, 2012.

[12] A. Malhotra, L. Totti, W. Meira, P. Kumaraguru, and V. Almeida, "Studying User Footprints in Different Online Social Networks," *International Workshop on Cybersecurity of Online Social Network (CSOSN)*, 2012.

[13] D. Irani, S. Webb, K. Li, and C. Pu, "Large Online Social Footprints–An Emerging Threat," in *Proceedings of the 2009 International Conference on Computational Science and Engineering*, ser. CSE, 2009.

[14] D. Perito, C. Castelluccia, M. A. Kâafar, and P. Manils, "How Unique and Traceable Are Usernames?" in *PETS*, 2011.

[15] M. Szomszor, I. Cantador, E. P. Superior, and H. Alani, "Correlating user profiles from multiple folksonomies," in *In Proceedings of International Conference Hypertext (HT '08)*, 2008.

[16] T. Iofciu, P. Fankhauser, F. Abel, and K. Bischoff, "Identifying Users Across Social Tagging Systems," in *ICWSM*, 2011.

[17] E. Raad, R. Chbeir, and A. Dipanda, "User Profile Matching in Social Networks," in *Network-Based Information Systems (NBiS), 2010 13th International Conference on*, 2010.

[18] K. Cortis, S. Scerri, I. Rivera, and S. Handschuh, "Discovering semantic equivalence of people behind online profiles," in *In Proceedings of the Resource Discovery (RED) Workshop*, ser. ESWC, 2012.

[19] A. Doan and A. Y. Halevy, "Semantic-integration research in the database community," *AI Magazine.*, 2005.

[20] J. Golbeck and M. Rothstein, "Linking social networks on the web with FOAF: a semantic web case study," in *Proceedings of the National conference on Artificial intelligence* -, ser. AAAI, 2008.

[21] A. Narayanan and V. Shmatikov, "De-anonymizing Social Networks," in *Proceedings of IEEE Symposium on Security and Privacy*, ser. SP, 2009.

[22] S. Bartunov, A. Korshunov, S. Park, W. Ryu, and H. Lee, "Joint Link-Attribute User Identity Resolution in Online Social Networks," in *SNAKDD*, 2012.

[23] D. Correa, A. Sureka, and R. Sethi, "WhACKY! - What anyone could know about you from Twitter," in *PST*, 2012.

[24] P. Jain, T. Rodrigues, G. Magno, P. Kumaraguru, and V. Almeida, "Cross-Pollination of Information in Online Social Media: A Case Study on Popular Social Networks," in *SocialCom/PASSAT*, 2011.

[25] M. Rowe, "The credibility of digital identity information on the social web: a user study," in *WICOW*, 2010.

[26] M. A. Jaro, *Unimatch: A record linkage system: Users manual.* Bureau of the Census, 1978.

[27] "We're getting less friendly on Facebook," 2012. [Online]. Available: Accessed on 02/24/2013 - http://www.boston.com/business/technology/articles /2012/02/24/study_were_getting_less_friendly_on_facebook/

[28] P. Kumaraguru and N. Sachdeva, "Privacy in India: Attitudes and Awareness V 2.0," PreCog-TR-12-001, PreCog@IIIT-Delhi, Tech. Rep., 2012, http://precog.iiitd.edu.in/research/privacyindia/.