SURVEILLANCE OF PERSONAL IMAGES FROM FIEND ON SOCIAL NETWORK

Security for Images on a Social Network

Selve K
Department of Computer Science and Engineering
Prist University
Trichy, India
Shelve22@gmail.com

***Abstract*— In the recent years, we have witnessed a dramatic rise in popularity of online social networking services, with several Social Network Sites (SNSs) such as My space, Face book, Blogger, You Tube, Yahoo! Groups etc are now among the most visited websites globally. However, since such forums are relatively easy to access and the users are often not aware of the size and the nature of the audience accessing their pro-files, they often reveal more information which is not appropriate to a public forum. As a result, such commercial and social site may often generate a number of privacy and security related threats for the members. This paper highlights the commercial and social benefits of safe and well-informed use of SNSs and emphasizes the most important threats to users of SNSs as well as illustrates the fundamental factors behind these threats. It also presents policy and technical recommendations to improve privacy and security without compromising the benefits of information sharing through SNSs. This paper mainly focuses on suspicious image detection in social networks.**

Keywords*— *Online Social Network, Privacy, Profile squatting, Identity threat, Image Tagging and Cross-profiling.

I. INTRODUCTION

The advent of the Internet has given rise to many forms of online sociality, including e-mail, Usenet, instant messaging, blogging, and online dating services. Among these, the technological phenomenon that has acquired the greatest popularity in this 21st century is the Online Social Networks or Social Networking Sites (SNSs). For the past few years, the number of participants of such social networking services has been increasing at an incredible rate. These Online Social Networks are the network spaces where the individuals are allowed to share their thoughts, ideas and creativity, and also to form social communities. These online networks provide significant advantages both to the individuals and in business sectors. Some of the noteworthy benefits of online social networks are:

Enable the people to stay connected with each other very conveniently and effectively, even on an international level. The connectedness and intimacy developed through this social networking might contribute to in-creased self-esteem and satisfaction might life for some students [6].

Allow the like-minded individuals to discover and interact with each other. Provide a forum for new modes of online collaboration, education, experience-sharing and trust-formation, such as the collection and exchange of reputation for businesses and individuals.

In the business sector, a well-tuned SNS can enhance the company's collective knowledge and engage a broad range of people in the company in the strategic planning process.

Since the success of an SNS depends on the number of users it attracts, there is pressure on SNS providers to encourage design and behavior which increase the number of

users and their connections. However, the security and the access control mechanisms of SNSs are relatively weak by design as the security and privacy are not considered as the first priority in the development of SNSs [1]. As a result, along with the benefits, significant privacy and security risks have also emerged in online social networking [17] as well as the study of SNSs' security issues has now become an extensive area of research.

The aim of this paper is to provide a useful introduction to security issues in the area of Social Networking. In this paper, we have examined some of the most important threats associated with Social Networking Sites and figured out the primary reasons behind these threats and finally based on that, we have provided some recommendations for action and best practices to reduce the security risks to users.

The remainder of this paper is organized as follows. Section 2 summarizes the related works in the privacy and security of online social networks. Then some of the major threats in social network have been elaborated in terms of vulnerabilities and risks in Section 3. Section 4 represents discussion and several recommendations for enhancing the privacy and security of SNSs. And finally, the paper is ended with the conclusion at section 5.

II. RELATED WORKS

The popularity of the concept of online social network has been increasing since 1997. As a result, in the recent years, social networking has gained intense media attention.

In addition to that, there have been significant research works on the security issues of online social networking. Analyzing the privacy relevant behavior and privacy risks on popular online sites are of prime concern now. In article [7], the author has studied online social network users to determine the users' attitude towards the Social Networks (SN). The study has revealed the fact that the users normally tend to reveal a variety of information including their name, age, gender, address, photos etc using their profile and some of them tend to hide, fabricate such information as well. Figure 1 describes the types of information revealed by the users and the status of the revealed information The information that is available in the users' profile can be searched based upon different criteria and thus can also be accessed by the strangers. Most of the people tend to expose real identity information; thus it raises privacy and security issues. Unfortunately many users are not aware of this. The kinds of information users tend to reveal and corresponding percentage are also studied in the article [7] and the result is represented in Table 2:

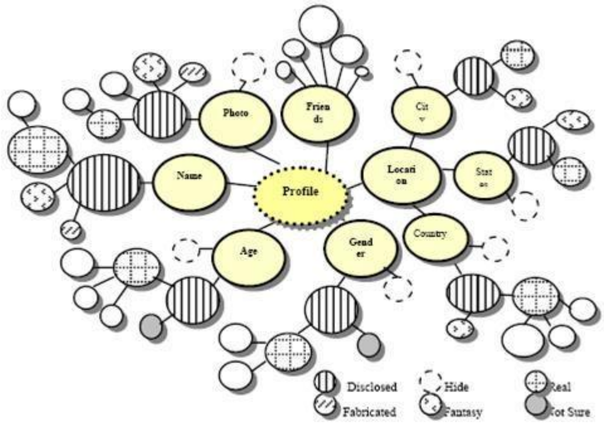


Figure 1: An overview of personal information disclosure [7]

Almost half of the participants disclose all elements of their personal information.

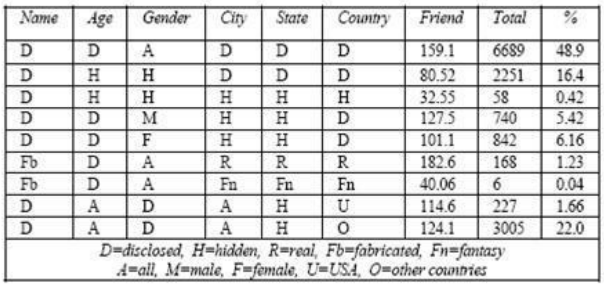
More than a quarter of users hide both their age and gender.

People who hide some of their identity elements have fewer friends.

Women are more likely to hide their location in comparison to men.

People who fabricate their identity are less likely to use a fantasy location and they have the most friends.

In a separate study of Facebook users done by Gross and Acquisty reveals that 71% of the Facebook users have the tendency to provide large amounts of sensitive personal information such as image, birthdates, in their profile that expose themselves to various kinds of security risks [11]. In a research on Human Computer Interaction (HCI), Wenday Mackay has shown that only a minimal percentage of users tend to change the default privacy preferences which are highly permeable [18].



Name	Age	Gender	City	State	Country	Friend	Total	%
D	D	A	D	D	D	159.1	6689	48.9
D	H	H	D	D	D	80.52	2251	16.4
D	H	H	H	H	H	32.55	58	0.42
D	D	M	H	H	D	127.5	740	5.42
D	D	F	H	H	D	101.1	842	6.16
Fb	D	A	R	R	R	182.6	168	1.23
Fb	D	A	Fn	Fn	Fn	40.06	6	0.04
D	A	D	A	H	U	114.6	227	1.66
D	A	D	A	H	O	124.1	3005	22.0
D=disclosed, H=hidden, R=real, Fb=fabricated, Fn=fantasy A=all, M=male, F=female, U=USA, O=other countries								

Figure 2: Combination of classified identity elements [7]

Also a number of new methods and strategies have been proposed in different scientific studies to mitigate the risks associated with this information revelation. In [10], the authors have developed a novel face de-identification algorithm that can limit the ability of automatic face recognition soft-ware by removing identifying information

while presenting other aspects of the face such as gender, ethnicity and expression. However, such methods have not been deployed to the social networks yet.

III. THREATS OF ONLINE SOCIAL NETWORKING

The casual posting of personal information on a digital medium might create a permanent record of the users' indiscretions and failures of judgments that can be exploited by the third-party commentary to produce a number of threats to the users. The potential threats that the users might face can be broadly categorized in four groups: Privacy related threats, SNS variants of traditional network and information security threats, Identity related threats and Social threats. In the following subsections we have descried about these threats:

A. Privacy Related Threats

Digital Dossier of personal information

Vulnerabilities: With the advancement of data mining technology and the reduction of cost of disk storage, the third party can create a digital dossier of personal data with the information revealed on the profiles of SNSs. A common vulnerability is that more private attributes which are directly accessible by profile browsing can be accessed via search (e.g. a person's name and profile image is accessible via search on MySpace, Facebook and others, unless default privacy settings are changed).

Risk: The information revealed on SNS can be exploited by an adversary to embarrass, to blackmail or even to dam-age the image of profile holder. For instance people are miss-ing out their employment opportunities since the employer reviews the SNS profiles of the prospective candidates [8, 9]. In some cases people are threaten as well such as recently the Miss New Jersey, 2007 was threatened with publication of images taken from her SNS profile if she would not give up her crown [15].

Face Recognition

Vulnerabilities: Users of the social network often tend to add images to their individual profiles that can be used for identifying the corresponding profile holders. Thus an stranger can use this data source for the correlating profiles across services using face recognition which is a part of the broader threat posed by so called mashups.

Risk: Face recognition can be used for the linking of image instances (and the accompanying information) across services and websites which in turn enables connecting, for example, a pseudo-anonymous dating profile with an identified corporate website profile. As a result, an adversary can gather substantially more information about

a user than in-tended.

Content-based Image Retrieval

Vulnerabilities: Most of the SNSs haven't employed any privacy controls over the images of the profiles to prevent the disclosure of information through the Content Based Image Retrieval (CBIR) yet. CBIR is an emerging technology which is able to match features, such as identifying aspects of a room (e.g. a painting) in very large databases of images and thus increases the possibilities of location the users [4][14][16].

Risk: CBIR opens up the possibility of deducing location data from apparently anonymous profiles containing images of users' homes. This can lead to stalking, unwanted marketing, blackmailing and all other threats associated with un-wanted disclosure of location data.

Image Tagging and Cross-profiling

Vulnerabilities: The SNS user has the option to tag im-ages with metadata such as the name of the person in the photo, a link to their SNS profile (even if they are not the owner/controller of that profile), or even their e-mail address.

Risk: An adversary can use this feature to slander some well-known personalities or brands and gain profit from their reputation.

Difficulty of Complete Account Deletion

Vulnerabilities: Users of SNS normally face more difficulty in deleting the secondary information than to delete their user accounts from any online social network. In some cases, such secondary information is almost impossible to remove. For instance the public comments a user has made on other accounts using their identity will remain online even after deleting his account.

Risk: The user may lose the control over his/her personal information. The information that can't be removed can be used as digital dossier.

A. SNS Variants of Traditional Network and Information Security Threats:

Spamming

Vulnerabilities: The enormous growth of social networking sites has encouraged the spammers to create the unsolicited messages known as Social Network (SN) Spams to produce traffic overload in the social networks.

Risk: SN Spam may cause the traffic overload, loss of trust or difficulty in using the underlying application as well as Phishing and diversion to pornographic sites.

Cross Site Scripting, Viruses and Worms

Vulnerabilities: SNSs are vulnerable to cross-site scripting (XSS) attacks and threats due to widgets produced by weakly verified third parties[12].

Risk: An adversary can use this vulnerability to compromise the account, to perform phishing attack and to spread the unsolicited content to the email and Instant Messaging (IM) traffic. Moreover, it can also be used for Denial of ser-vice and associated loss of reputation.

SNS Aggregators

Vulnerabilities: Some of the new applications such as Snag, Profile Linker provide read/write access to several SNS accounts to integrate the data into a single web application. But such applications use weak authentication method and thus the vulnerability is increased.

Risk: The effects of this vulnerability are Identity theft, Zombification of SNS accounts, e.g. for XSS attacks or advertising, loss of privacy for other members of the SNS by allowing search across a broader base of data.

B. Identity Related Threats:

Phishing

Vulnerabilities: A phisher can easily and effectively exploit the information available on social network to increase the success rate of a phishing attack. For instance, the email phishing attacks can be achieved 72% hit rate by using the information available in the social network [13]. SNSs are also vulnerable to social engineering techniques which exploit low entry thresholds to trust networks and to scripting attacks which allow the automated injection of phishing links.

Risk: Phishing can reveal the sensitive information, such as passwords and credit-card or bank account numbers and cause financial and reputation damage.

Information Leakage

Vulnerabilities: The privacy of online social networks is jeopardized since an adversary can easily become a friend of a member of any restricted group by dissembling his identity and then access to the private information that belongs to the members of only that group. Moreover, on many SNSs such as MySpace it is even possible to use scripts to invite friends.

Risks: Some of the potential risks associated with this threat are: Leakage of Private information, Phishing for information and conducting spamming and marketing campaigns.

Profile squatting through Identity theft

Vulnerabilities: A malicious attacker can create a fake profile to impersonate a renowned person or a brand. Such profiles are usually created by the people who know the personal details of a user and create a profile to impersonate him or her and thereby causing all sorts of problems for the victim.

Risks: Profile squatting can done a significant damage to the reputation of a person or any brand which may in turn Lead to the financial and social embarrassment. Recently an underage student at University of Missouri-Columbia was in trouble when college administrators found a picture of her duct-taped to a chair while another student poured beer in her mouth. This was a matter of considerable embarrassment as she had just been elected student body vice president.

C. Corporate Espionage

Vulnerabilities: Social engineering attacks using SNSs are a growing but often underrated risk to corporate IT infrastructure.

Risk: The main risk here is the loss of corporate intellectual property, but gaining access to insiders may also be a component in a broad range of other crimes, such as hacking corporate networks to cause damage, blackmailing of employees to reveal sensitive customer information and even to access physical assets.

IV. DISCUSSION AND RECOMMENDATION

By analyzing the different kinds of threats associated with the Social Network Sites, I have found the following major factors that might be considered as the root of all threats:

Most of the users (especially the teenagers) are not concerned with the importance of personal information disclosure and thus they are in the risk of over-disclosure and privacy invasions due to this underestimation of ex-tent and activity of their social network. Especially, the major portion of threats is related with the friends list, posted pictures. Wall posts etc. in which users are relatively less conscious compare to the personal profile information.

Users who are aware of the threats, often fails to properly manage the privacy preference due to the complexity and ambiguity of the interface and lack of user-friendly guidelines that would help the users to choose the appropriate privacy settings.

The existing legislation and policy are not equipped to deal with many of the challenges that the social net-work currently presents including the legal position on image-tagging by third parties, the legal position on profile-squatting etc.

Lack of appropriate authentication and access control mechanisms as well as other security related tools to handle different privacy and security issues of online social networks.

Recommendations:

Some of the recommended strategies for circumventing the threats associated with the online social networks are described below:

Building self awareness about the information disclosure:

Users need to be more conscious about the information they reveal through their personal profiles in online social networks. They also have to accurately maintain their profiles through periodical review and necessary modification of the profile contents to ensure appropriate disclosure of information.

Encouraging awareness-raising and Educational Campaigns:

Government should initiate different educational and awareness-raising campaigns to inform the users to make the rational usage of the Social Networking Sites as well as to encourage the providers to develop and practice security conscious corporate policies.

Reviewing and reinterpreting the regulatory framework:

The existing legislation may need to be modified or extended due to the introduction of some issues like the legal position of image tagging by the third person which are not addressed by the current version. As a result, the regulatory frame-work governing SNSs should be reviewed and revised as it requires.

Promoting stronger authentication and access-control where appropriate: The strength of authentication method varies from SNS to SNS. However, in order to avoid fake and troublesome memberships, the authentication mechanism need to be further strengthen using additional authentication factors such as e-mail verification through Captchas.

Setting appropriate defaults: Since most of the users are not aware of the necessity for changing the default privacy preference [19], it is essential to set the default setting as safe as possible. The SNS service provider also needs to offer user-friendly guidelines that help the users to change the privacy settings successfully.

Providing suitable security tools: Providers also need to offer the following strategies for better user control on different privacy and security related issues.

Tools that will allow the users to remove their accounts as well as edit their own posts on the other people’s public notes or comment areas conveniently.

Automated filtering tools for determining the legitimate contents. Tools for controlling the tagging of images depicting them.

New privacy software such as visualization tools for increasing the utilization of privacy options by providing clear representations of social networks, friend proximity, and availability of profile features.

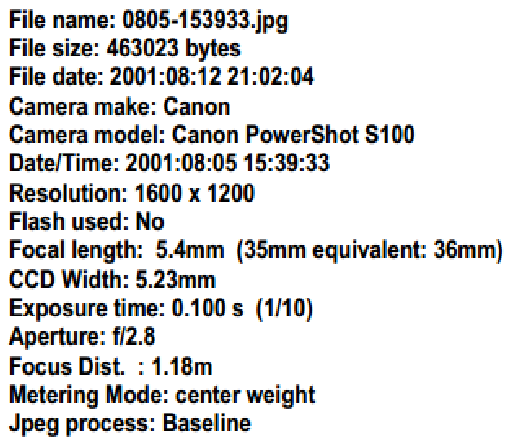
V. USING EXTENDED FILE INFORMATION (EXIF) FILE HEADERS IN DIGITAL EVIDENCE ANALYSIS

A. Metadata in Digital Photography

Metadata is a data about data. For example, a Microsoft Word document’s metadata may contain the author’s name and the dates the document was created/modified. Metadata may contain useful information for an investigator.

Specifically, digital camera pictures may contain an Extended File Information (EXIF) header, which saves information about the camera that took the picture.

The EXIF format was created by the Japan Electronic Industry Development Association and is referenced as the preferred image format for digital cameras in ISO 12234-1. Many digital camera manufacturers, such as Canon, Sony and Kodak implement the use of EXIF headers. This header is stored in an "application segment" of a JPEG file, or as privately defined tags in a TIFF file. This means that the resulting JPEG or TIFF is still in a standard format readable by applications that are ignorant of EXIF information. Below is a typical EXIF header (in human readable format):



File name: 0805-153933.jpg
File size: 463023 bytes
File date: 2001:08:12 21:02:04
Camera make: Canon
Camera model: Canon PowerShot S100
Date/Time: 2001:08:05 15:39:33
Resolution: 1600 x 1200
Flash used: No
Focal length: 5.4mm (35mm equivalent: 36mm)
CCD Width: 5.23mm
Exposure time: 0.100 s (1/10)
Aperture: f/2.8
Focus Dist. : 1.18m
Metering Mode: center weight
Jpeg process: Baseline

Figure 3 EXIF Format

B. Value in Retrieving EXIF Headers

By reviewing EXIF headers, some valuable information can be recovered. For example, the one above shows two dates. The first is the file creation date/time. The other is the date/time the picture was taken. The date/time the picture was taken will not change, even if the file is copied to another medium. The EXIF header also shows the camera make and model. The EXIF header is placed in the file by the camera that took the picture. If the file is modified with picture editing software, the EXIF header will be lost. Therefore, if a file contains EXIF information, then it is possible that the picture is unaltered. However, not all digital cameras use EXIF headers; pictures taken with such cameras do not have EXIF data.

C. Retrieval of EXIF Header

Although it is possible to retrieve EXIF headers by looking at each picture in a disk editor, a considerable amount of time is required to translate the hex codes into human readable format. Fortunately, there are other ways. An open-source program called jhead allows the retrieval of EXIF headers from jpg files.

D. Performance Analysis of Human Skin Region Detection Techniques with Face Detection Application

This paper [2] deals with 3D Histogram, dynamic cluster formation, local and global optimum solution. The local optimum solutions are determined by Hillclimbing segmentation with K-Means clustering algorithm of CIEL*a*b color image. Then these local solutions are further refined by the PSO technique, in order to find the global solution by YCbCr color space explicit skin color conditions. Then the results are compared with our Hybrid approach and HSFCM . Finally face detection results shows the importance and efficiencies of the Optimization technique

E. Pornographic Images Detection Based on CBIR and Skin Analysis

In this paper[3], proposes to detect pornographic images in a two-stage scheme. For the first step, the content-based image retrieval technique (CBIR)to determine whether the image has human in it. For the second step, a skin color model is established to analyze the skin-like pixels and identify the presence of pornographic content. The proposed two-stage detecting way accords with the human vision system (HVS). A fast k nearest neighbor search (KNNS) method is employed in the retrieval step, which speed up the whole system. The combination of the CBIR and detailed skin color analysis reduces the false positives in detecting pornographic images while retaining a high true positives.

A. A LEGO-like Metadata Architecture for Image Search&Retrieval

This paper aims contributing to solve some of the current problems of images’ metadata management architectures by introducing the notion of a ‘‘composable metadata model’’ as a means to allow the usage of multiple metadata formats together, along with mechanisms to specify semantic mappings among the different formats, within an image search&retrieval system. The paper defends the idea that the choice of a unique metadata model is not sustainable in the midterm, and that users should be able to snap together selected ‘‘building blocks’’ provided by different metadata standards, the ‘‘LEGO Metaphor’’.

B. Composable metadata models, the LEGO Metaphor

A helpful metaphor is to think of metadata annotations as a assembly of LEGO® pieces, being each one of the pieces an individual metadata statement (e.g. “format = image/jpeg”) and being each metadata format a kit of several LEGO pieces. In real LEGO, individual pieces from different kits can be easily combined to build complex artefacts because each individual piece has a clearly defined interface (self-explanatory or well documented) and can be used independently. Coming back to the metadata world, some metadata formats are based in data model theories that do not facilitate the usage of individual metadata statements separatedly (e.g. XML). The Semantic Web data model theory, the RDF model, already allows the individual usage of metadata statements.That the syntax and semantics of each “metadata piece” will be always clearly specified (e.g. specifying that the “format” property, when used for an image, expects an image-based MIME type). Current Semantic Web technologies allow to freely specify the syntax and semantics of properties, but the absence of compulsory canonical ways of doing it impedes the achievement of the LEGO Metaphor in practice.

C. A New Fast Skin Color Detection Technique

In this paper[5] ,the goal is to generate a large texture image from a small one. Efros et al. find seams that minimize the error surface defined by two overlapping texture patches. This way, the original small texture image is quilted to form a much larger texture image. This was later extended to handle both image and video texture synthesis by Kwatra et al. That showed how to increase the space and time dimensions of the original texture video. Many fast skin color detection techniques are based on the image resizing. To overcome the time consuming problem in skin color detection, a new fast technique is introduced for skin detection which can be applied in a real time system. In this technique, instead of testing each image pixel to label it as skin or non-skin (as in classic techniques), and skip a predetermined number of pixels. The reason of the skipping process is the high probability that neighbors of the skin color pixels are also skin pixels, especially in adult images and vice versa. The skipping process can be applied with the resizing technique to obtain better results. This hybrid technique takes the advantages of both methods

D. System for Screening Objectionable Images Using Daubechies' Wavelets and Color Histograms

In this paper[6], the approach is the content-based feature vector indexing and matching developed in our multimedia database research. Image feature vector indexing has been developed and implemented in several multimedia database systems .A new algorithm is developed to efficiently and accurately compare the semantic content of images mainly consisting of objects such as the human body. Using Daubechies' wavelets, moment analysis, and histogram indexing, the algorithm produces feature vectors that provide excellent accuracy in matching images of relatively isolated objects such as the human body. A novel multi-step metric is used to compute the distance between two given images. A training database of about 500 objectionable images and about 8,000 benign images has been indexed using such an algorithm.

When a query comes in, and compute the feature vector and use it to match with the training database. If it matches with objectionable images in the training database, then classify it as an objectionable image. If it does not match with objectionable images in the training database, then classify it as a benign image. Promising results have been obtained in experiments using a test set of 437 objectionable images and 10,809 benign images.

E. Performance Analysis for Detection and Location of Human Faces in Digital Image With Different Color Spaces for Different Image Formats

In this paper[7], the algorithm is very simple. First, it trains the network by Levenberg –Marquardt training algorithm so that it can detect face or non faced image. Now the threshold value of the network above which is a face and below which is a non-face is determined with the network output graph and is different for different color spaces for each of the image formats bmp, jpeg, gif, tiff and png. This depends on the training of the network. The algorithm takes an input image and chooses initial windows of size 300x300 which scan the whole image and take the mug shot each time and feed it to the neural network trained earlier with Levenberg –Marquardt training algorithm. If the output is greater than the threshold value, then it is a face described by a square drawn on it.

The same operation is performed with reduced window size, diminished by 50 and continued till the size becomes 100x100. So all faces between size 300x300 and 100x100 will be detected. If there is redundancy i.e., two or more squares of different sizes represent the same face, then the squares of smaller sizes are omitted. This simple approach has not been made

earlier and also a comparison with six different color spaces has been done to choose the appropriate color space. This is the reason for making this paper.The proposed algorithm is run for each of the six color spaces RGB, YES, YUV, YCbCr, YIQ and CMY for each of the image formats bmp, jpeg, gif, tiff and png. The different image formats may affect the performance and accuracy of detection and location of human faces in a digital image of a particular image format.

Sample Social Network Creation

In this module the sample social network is created. In this social network each must register with user name and profile photo. The User can share some information via Text and Image to other friends in the social network.

Meta Information Extraction

In this module the image detector read the user uploaded image and extract the Meta information. It extracts EXIF header of the image along with other Meta-Info such as image height, width and bit depth and aimed to store into the image structure. The MD5 digest of the image will be stored into flat file in future work.

Skin Tone Analysis

In module the image detector analysis the skin tones of the uploaded image. The goal is to identify a suspect image by detecting the amount of skin exposed in an image. Using Bicubic interpolation technique the image is resampled. The skipping technique is applied on the resampled image to detect skin pixels in a fast manner by processing lesser number of pixels for faster execution. Hybrid color filter of RGB and YCbCr is used because of the racial artifacts of skin tone as well as the illumination issues. Amount of pixels marked as skin out of total pixels are calculated. If the count exceeds a pre-defined threshold, the image will be marked as suspicious.

Suspicious Image Detection

In this module the image detector detect whether the uploaded image is suspicious or not. After Meta-Information and Skin-tone analysis is performed, it will generate patterns by analyzing metadata of the images which have been identified as malicious. It will perform statistical analysis over images metadata structure to filter out suspicious ones. This module classify whether the image contains any suspicious information.

which will help in identifying suspicious images in a probabilistic approach so as to improve real-time performance of the system. The use of intelligence factor to first train the system using malicious image attributes helps in better prediction of suspiciousness in images.

The proposed scheme results into calculation of the skin content in image. The system will reside on the client machine. The system will identify possible candidates for threats by analyzing the meta-info of the images for any manipulation as well as locating images with a large portion of skin exposed. If a hidden script is detected which is embedded within the image file, the image is immediately classified as malicious without further analysis.

VI. CONCLUSION

Online social networks offer exciting new opportunities for interaction and communication, but also raise new privacy concerns. In this paper, we have briefly described of some major features and benefits of social networking that have made this technology as one of the most popular internet technologies at this moment. We have also highlighted the crucial privacy and security threats that may arise due to ’almost-anything-goes’.

“Suspicious Image Identification using EXIF metadata” is the proposed system in the form of a reusable library which will help in identifying suspicious images in a probabilistic approach so as to improve real-time performance of the system. The use of intelligence factor to first train the system using malicious image attributes helps in better prediction of suspiciousness in images.

The proposed scheme results into calculation of the skin content in image. The system will reside on the client machine. The system will identify possible candidates for threats by analyzing the meta-info of the images for any manipulation as well as locating images with a large portion of skin exposed. If a hidden script is detected which is embedded within the image file, the image is immediately classified as malicious without further analysis.

REFERENCES

[1] A. Acquisti and R. Gross. Imagined Communities Awareness, Information Sharing, and Privacy on the Facebook, . In 6th Workshop on Privacy Enhancing Technologies, June 2006. www.careerjournal.com/jobhunting/usingnet/20060112-flesher.html.

[2] D. Boyd. Reflections on friendster, trust and intimacy. In Intimate (Ubiquitous) Computing Workshop -Ubicomp, Seattle, Washington, USA, October 2003.

[3] D. Boyd. Friendster and publicly articulated social networking. In Conference on Human Factors and Computing Systems (CHI 2004), Vienna, Austria, April 2004.

[4] Chen, Y., Roussev, V., Richard, G. III, Gao, Y. Content-based image retrieval for digital forensics. In Proceedings of the First International Conference on Digital Forensics (IFIP).

[5] D. B. Donath, J. Public displays of connection. In BT Technology Journal 22, pages 71 – 82, 2004. Ellison, N. B., Steinfield, C., and Lampe, C. . The benefits of Facebook "friends:" Social capital and college students’ use of online

social network sites. In Journal of Computer-Mediated Communication, volume 12, 2007.

[6] R. Feizy. Evaluation of Identity on Online Social Networking: Myspace. In 18th Conference on Hypertext and Hypermedia (HT ’07), December 2007.

[7] J. Flesher. How to Clean Up Your Digital Dirt Before It Trashes Your Job Search. In The Internet Engineering Task Force, 2006. http://www.careerjournal.com/jobhunting/usingnet/20060112-flesher.html.

[8] R. Gross and L. Sweeney. Towards real-world face de-identification. In IEEE Conference on Biometrics: Theory, Applications and Systems, 2007.

[9] A. Gross R., Acquisti. Privacy and information revelation in online social networks. In ACM Workshop on Privacy in the Electronic Society (WPES), 2005.

[10] G. Hogben. Security Issues and Recommendations for Online Social Networks. Position paper, ENISA, European Network and Information Security Agency, October 2007.

[11] R. Vijayanandh and Dr. G. Balakrishnan, Performance Analysis of Human Skin Region Detection Techniques with Face Detection Application, International Journal of Modeling and Optimization, Vol. 1, No. 3, August 2011.

[12] Ruben Tous and Jaime Delgado, A LEGO-like Metadata Architecture for Image Search & Retrieval, 20th International Workshop on Database and Expert Systems Application, 2009.

[13] Bei-bei Liu and Jing-yang Su and Zhe-ming Lu and Zhen Li, Pornographic Images Detection Based on CBIR and Skin analysis, Fourth International Conference on Semantics, Knowledge and Grid, 2008.

[14] Tarek M. Mahmoud, A New Fast Skin Color Detection Technique, World Academy of Science, Engineering and Technology, 43, 2008.

[15] Paul Alvarez, Using Extended File Information (EXIF) File Headers in Digital Evidence Analysis, International Journal of Digital Evidence Winter, Volume 2, Issue 3, 2004.