ISSN No:-2456-2165

Social Media Security: Identity Theft Prevention

M.M.Shahria[1]
Department of Computer Science & Engineering
East Delta University
Chittagong, Bangladesh.

Mohammed Nazim Uddin[2]
School of Science Engineering &Technology,
East Delta University
Chittagong, Bangladesh.

Miraj Ahmed[1]
Department of Computer Science & Engineering
East Delta University
Chittagong, Bangladesh.

Abstract:- Social networking sites are becoming parts and parcels of our daily life. With the increasing of its popularity, the cybercrimes, targeting these platforms are also increasing. Cybercriminals use this platform to harass the victims personally, socially and financially. Such type of crimes is performed using some of the vulnerabilities of the social networking platforms. Identity theft is one of those crimes which is increasing alarmingly. By creating a fake account, using the same information and profile picture, one can easily take disguise of another person. Hence, the criminal can chat with other persons impersonating the victim. Thus, the criminal takes the disguise of a person and starts harassing other people. The consequence of this problem is very dangerous. By doing so, the criminal ruins the image of the victim. There are so many cases where victims attempted to commit suicide after facing this type of terrible problem. All these things are occurring as the criminal can download or collect the profile picture of the victim easily and open a clone account easily. The availability of information is giving the chance to the cybercriminal to make an account exactly looks like the victim's one. In this paper, we attempt to prevent this type of identity theft by an image based solution on the social networking platforms. The name of this model is 'Image Based Identity Theft Prevention'.

Keywords:- *Identity Theft, Social Networks, Fake account, Social Harassment, Cyber Crime, Image comparison.*

I. INTRODUCTION

Nowadays social networking sites have become an important part of our life. From a Teenager to an adult person, People of every age, every race is being involved with social networking platforms. People are sharing their thoughts, Images and personal information over these social networking sites. These platforms are not only being important for general people but also getting useful for marketers and businessmen. Its tons of active members are blissful scope for growing sells of a company. People are transacting their money over the social media as well. Therefore, people are using social media to increase their friends, communities, and business. They are taking it as an opportunity to build a new relationship as well. Social networking platforms are modern era's phenomena as users have taken these seriously. Among all the social networking sites, Facebook is considered to be the most popular and influential platform in the world.

According to the Facebook newsroom, it has 1.32 billion daily active users on average along with 2.01 billion monthly active users as of June30, 2017 [1].

A user spends on an average fifty minutes on the Facebook, Instagram and Messenger platform [2] in their daily life according to the statistics. The number of cybercrime is also increasing aiming at the number of social media users. Cyber threat has been the number one problem regarding these social media growth. As a result, security issues are grabbing the attention of us to protect these large volumes of private data. People use their personal information in an open platform. Hence, they make themselves easy victims of cybercrimes. As people are building their relationship using these platforms, the probability of network phishing, fraud, and other criminal activities tend to increase [3]. It is important to protect the privacy of people as invading the privacy with a view to an unhealthy intention will cause a major harm as well as harassment of the victim. It is highly necessary to stop the invasion of the private data as this will not only harm a person's social image but also lead that person to an uncomfortable zone. While using the social media we must always remember that "what happens on the internet always stays on the internet". That is why we should always keep an eye on the steps taken on the social media while sharing our private data.

A few numbers of security models for social media were developed previously. Among those models, one of the most significant methods is the new face to photo security of Facebook [4]. But this does not give any permanent solution to this type of identity theft problem on the social networking platforms. In this paper, we have proposed a model named Image Based Identity Theft Prevention which can be applied only on the social networking platforms.

Our demonstration of this paper is as follows. In the section 2 of this paper, we have described a scenario so that the crime that can be committed by stealing someone's profile picture can be understood clearly. In the section 3, we have demonstrated an image based identity theft

ISSN No:-2456-2165

prevention model to secure the social networking platforms. In the section 4 and 5 we have demonstrated our experiment to check the adoptability of the model.

II. SECURITY ISSUE IN THE SOCIAL MEDIA

Facebook admits that there are at least 270m fake accounts on this platform [5] whereas every day the number is increasing. These accounts are a huge threat to the real users. By a fake account, there are so many types of cybercrimes that can be committed. Data search and sharing are two important functionalities in social networks [6]. By sharing the data on the social media platforms, we give all the other people easy access to our information. Thus, other users can collect our information as well as the profile picture from our account. Usability of the same profile picture in another account increases the rate of crimes.

By creating a fake account with the victim's profile picture and profile name, the criminal can harass the victim socially and personally. There are so many scenarios and crimes that have been occurring by implementing this method.

The following scenario is a perfect example of the statement of the problem. In this scenario, there are two people namely Adeel Abideen and Jishan. They both are bosom friends.

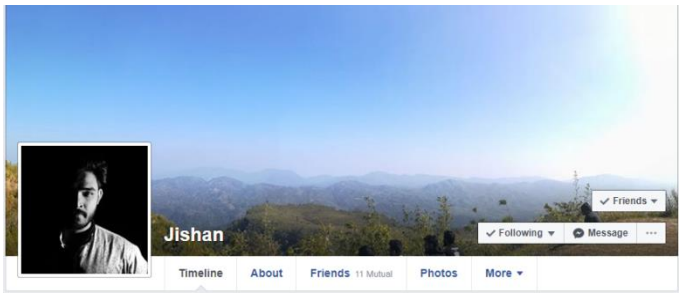

Fig 1:- Jishan's Facebook Account [7]

Fig 2:- Adeel Abideen's Facebook account [8]

The main medium of their communication is Facebook. There one more person in this case whose name is Amin. He is a mutual friend of Jishan and AdeelAbideen. On the other hand, Amin feels envious about AdeelAbideenhaving a healthy relationship with Jishan.

Fig 3:- Amin's Facebook Account [9]

He decides to create a conflict between them. In the meantime, His mind flings from one idea to another through which he can create a distance between them. Finally, he decides to create a fake account of Adeel Abideenon the Facebook. Amin decides to create this account so that he can write mean things about Jishanby using Adeelabideen's fake account and spread it without Adeel Abideenhaving any knowledge about it.

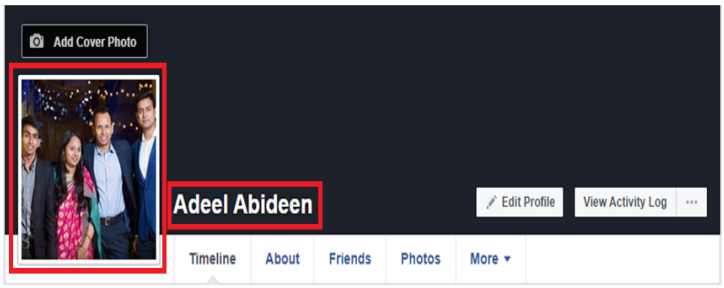

Fig 4:- Adeel Abideen's fakeFacebook account

The next step by Amin after creating the fake account of AdeelAbideenis that he chats to himself by using AdeelAbideen's fake account and tells mean things about Jishan. That meansamin uses his account as well as AdeelAbideen's fake account to create a chat history. The point that must be kept in focus is that the fake account of AdeelAbideen looks exactly similar to the real account. To gain this similarity, amin must use the exact profile picture, profile name as well as other information of AdeelAbideen's real account while creating that fake account. So, when Jishan receives the screenshot that Amin has captured, Jishan will be totally convinced that it was Adeel Abideen who has negative thoughts about him.

There is technically no scope for jishan to justify whether those messages were sent from Adeelabideen's real account or not, as there is no way still available to find the difference between the fake and real chat's screenshot. Both of thesecontain the same profile picture. The same profile picture and profile name make it look like authentic.

Therefore, Jishan will have no doubt that the messages that were sent to Amin were from none other than AdeelAbideen.

ISSN No:-2456-2165

Fig 5:- No difference between fake and real account's chat box

III. AN IMAGE BASED IDENTITY THEFT PREVENTION MODEL

To resolve the problem which has been described in the section no. 3, we have designed a model. The name of the model is image based identity theft prevention. There are two cases may appear when a user tries to impersonate another person. The first case is when the user tries to upload an image as soon as he/she opens an account on the social media platform. And the second case is when the criminal tries to upload the victim's profile picture in an existing account. We have created structures to counter identity theft in both of these cases. In the section 3.1 and 3.2, we have discussed thoroughly on these two cases.

A. Identity theft prevention model for case one

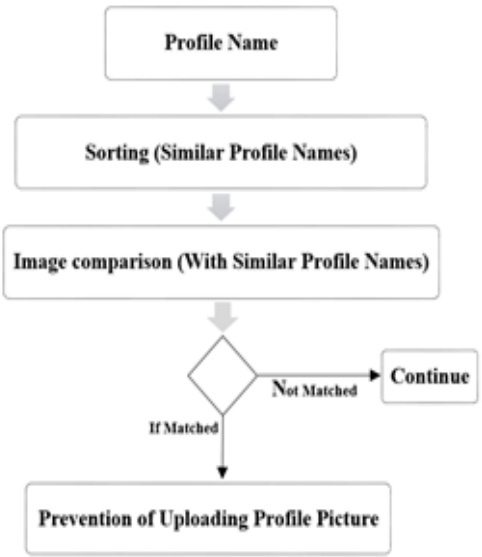

Fig 6:- Model Structure to Prevent Identity Theft (Case 1)

Social media is defined as an internet-based platform for people where people meet in virtual communities and share their Information [10]. Therefore, sharing information may trap users in the problems like identity theft. Here we have created a model to prevent identity theft for the first case scenario. This model is applicable when user creates an account and instantly tries to upload a profile picture. Our model suggests that a user must upload a profile picture while opening a new account. This model will help the social media administrations to detect the accounts which will be trying to steal another one's identity.

The whole model is demonstrated below with the help of a diagram. This can be considered as the proposed model to solve the problem of this paper. Every step of this structure model will be described one by one in an individual section.

The model starts working as soon as an individual tries to open an account on a social networking site. If the Proposed model is followed properly; it is possible to weed out identity theft from the social networking sites completely. While opening an account the user must give a name to set it as a profile name. The step by step demonstration of fig 6 is given below.

➢ *Profile Name*

While opening an account on the social networking site, a user needs to input a profile name. To make a clone account the criminal has to use the same profile name as the victim's profile name. This is the first step where a criminal starts his process. The identity of a person can be determined by his name. And then a profile picture is needed for detail information.

If a person has an account named Adeel Abideen, the criminal must open an account by using the name Adeel Abideen. The criminal does not use any uppercase and lower case letters in between. He enters the exact name of the victim.

When someone tries to open an account on the social media, there is some basic information that is required. The basic information might be the name of that person, his mobile phone no. or email as most of the social networking sites, uses these two ways verification to authenticate a person's existence to nullify the bot problems or spamming.

A password is also required to get entrance to his account. After giving all of this information a unique user ID will be created for that particular person in the database. Later he can add the additional information and in the further process, he can add an image as his profile picture. In our proposed model, this is where the process begins. And this is where the solution to the problem needs to be started.

➢ *Sorting Out.*

Now the profile name is created. As the profile name has been created, it has already been stored in the database. To eliminate the redundancy while comparing the profile pictures, we must decrease the number of the accounts by using some certain parameters. To do so, we need to gather the ids which have got the same profile name. This is how; we can make this process more efficient. The criminal wants to create a profile with the name Adeel Abideen. So, after creating a profile by using the name Adeel Abideen, the criminal automatically enters into the system. But in the back-endprocess, we can sort out all the ids which hold the

ISSN No:-2456-2165

name ‘Adeel Abideen’. By doing so, we will get all the ids that are stored in the database of that social media which contains the name Adeel Abideen.To achieve this it is needed to automate a query as soon as the user submits all the basic information.

The main disadvantage of this process is it'stime-consuming. Every time a user tries to open an account, it has to fetch all the data related to its name. To get rid of this, we can decrease the results using the parameters like gender, country etc. To reduce the time complexity, further research is required in this field.

➢ *Image Comparisons*

What we have shown in the statement of the problem, to resolve this, some image comparison techniques can be implemented. There are various ways to compare among some images. As the problem will occur when a criminal tries to upload a similar photo of the victim as a profile picture, an efficient technique is needed to match the image with the victim’s image.

There are various ways of comparing images. But there are two types of scenario when a criminal uploads an image of the victim. The first one is, the criminal might upload exactly the same image that he downloads from victim’s wall. And the second scenario is the criminal might be wicked and tries to trick the platform by slightly changing the image by shifting the image or resizing the image. As the main intention of this paper is to prevent identity stealing on social media by an image comparison technique, we need to find out the best possible algorithm for this task. Here, some image comparison techniques are being illustrated.

- *Pixel by Pixel operation*

Image difference calculation is most probably the easiest and effective at the same time when it comes to the pixel by pixel comparison. Pixel to pixel operation is performed by sorting out the differences between each pixel pair. So, if the image neither is distorted nor be resized, this algorithm comes handy.

But in most cases, images can be manipulated and resized. In these cases, it would be difficult for the system to match two images even if they are of the same persons.

In those circumstances, it would be wise to segment an image into smaller pieces, So that it would be possible to analyze more perfectly. These segments are called regions of interest (ROI) segments.

- *Key point matching.*

The main idea of key point matching is to pick the most important points rather than picking random points of an image. Rather than picking 200 random points, it is better to pick 200 important points. In every image, there are some points which are more identical than most of the other points. These points contain more information than other points.

This is to be notified that some particular parts of an image have precise and detailed information than the other part of those images. As an example, Centre of an image contains more valuable information than the edges and corners of that image. For an effective image matching process, these points are exactly what makes the comparison efficient and more accurate.

Key point matching is efficient only when the image is affected by an affine transformation. Affine transformation refers to translation, scaling, reflection, rotation, and shearing of an image.

So, even if any image is distorted by affine transformation, Key point matching process can find out the similarity between two images. Generally, Key point matching has been implemented by two Frameworks. The first one is SURF (Speeded up Robust Features) [11] and the second one is the SIFT (Scale Invariant Feature Transform) [12].

Nowadays, SIFT key points are very much popular among the developer for its effectiveness. Under SIFT; images can be matched even if they are differently scaled, rotated or lighted.

One of the most downsides of key point matching is its run time. It takes O (n^2m) while comparing among m images.

Here, n is the number of key points of an image. Key points refer to the most significant points of the image whereas; m is the number of total images in the database.

- *Histogram method*

Histogram-based image matching algorithms calculate the histogram components of two pictures and then try to measure the similarity [13].It is a potential idea to build feature histogram for each and every image. The histogram of the profile picture needs to be calculated first, and then it needs to be compared with other image’s histograms. For this reason, it is not that time efficient.

To get it worked very well, the images need to be very similar. That means, if the criminal re-scale the image or rotate the image from left side to right side, it would be difficult for this process to find out the similarities.

But, some negligible small changes like cropping the image would not fail the algorithm.

- *2D correlation.*

Image matching problem can be solved by apply 2D correlation as well. It can detect resized image very well. If an image is shifted right or shifted left, the algorithm will make it possible to match the image with the actual one pretty decently.

The algorithmfor 2D correlation is stated below.

- ✓ Firstly, The RGB values of the image need to be saved as an array.
- ✓ Then, the RGB values need to be converted into grey-scale value using W3c luminance.
- ✓ All data need to be normalized.
- ✓ On the normalized data, an accurate 2D correlated operation needs to be performed.

By 2D correlation method, it is easier to find out the similarities of degrees between two or more image.

From all of these algorithms that have been stated above any of this Key point, matching would be most effective. But any of these algorithms other than these can be implemented considering time, accuracy and simplicity.

➢ *Prevention of Uploading Profile Picture*

If the uploaded profile picture is matched with another existing profile picture, then the user will be abandoned. A message will be shown a dialogue box which contains the message that he cannot upload this as his profile picture. Otherwise, the user can upload the profile picture successfully.

B. Identity theft prevention model for case two

The previous model is for the case where the user opens a new account and therefore uploads a profile picture out there. But the scenario can be another way as well. A user can not only upload a profile picture while opening an account but also may change the profile picture in an existing account with a view to identity stealing.

The social media give the chances to change the profile picture frequently. That is why it is even possible for someone to pretend as another person even when it is an older account.

As it is permissible to upload a profile picture whenever the user wants, it needs to be checked at the same time. Hence, a model is also needed for this case.

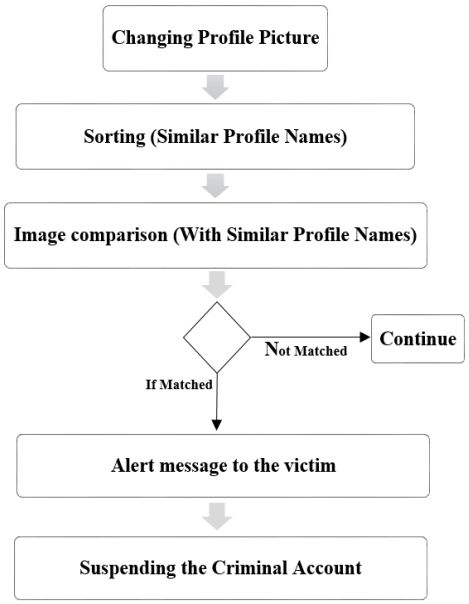

Fig 7:- Model Structure to Prevent Identity Theft (Case 2)

So, when a user uploads a new profile picture, the automated query should summon all the matched profile names to compare all the profile pictures.

After comparing the same algorithm as it has been discussed in case 1 in details, an action needs to be taken depending on the result. If an existing image is detected, then an alert message should be shown to the user. At the same time, an alert message should be forwarded to the possible victim. And then the next action would be taken against the criminal by suspending his account.

IV. EXPERIMENTATION AND EVALUATION

A. Create a new account

In our system, we have created a social media where a user must give his basic information while opening an account. In the figure 8, a new account is being created using the name Adeel Abideen.

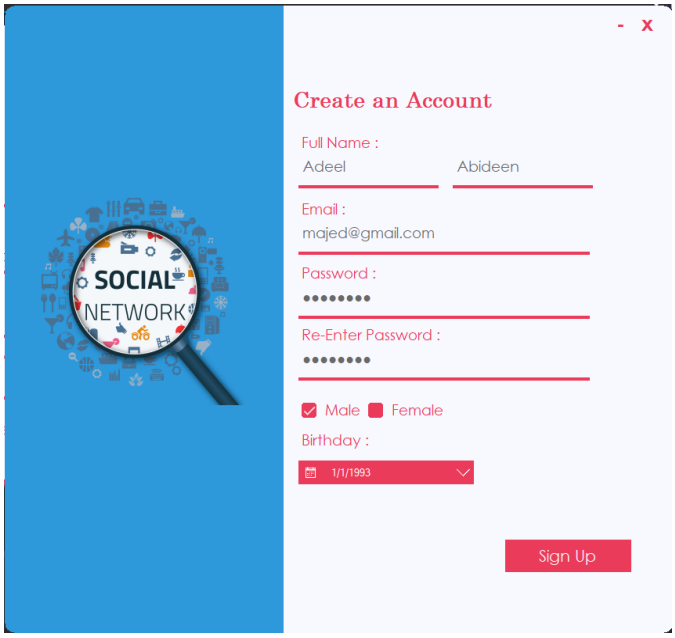

Fig 8:- Creating new account

B. Storing the information in the database

The given information will be stored in the database.

	userID	firstName	lastName	password	email	profile_pic
Edit Copy Delete	1	Adeel	Abideen	amin2646	jishan@gmail.com	http://socialmedia.com/profile_pic/12344
Edit Copy Delete	2	Adeel	Abideen	jishan22	majed@gmail.com	http://socialmedia.com/profile_pic/12345
Edit Copy Delete	3	Pseudo	Amin	kk2222	kkk@gmail.com	http://socialmedia.com/profile_pic/12347
Edit Copy Delete	4	konick	Noakhali	jjjkk222	konick@gmail.com	http://socialmedia.com/profile_pic/12348
Edit Copy Delete	5	M M	Shahria	dkdfkj	afh@gmail.com	http://socialmedia.com/profile_pic/12349
Edit Copy Delete	6	Miraj	Ahmed	ahafjh	miraj@gmail.com	http://socialmedia.com/profile_pic/12350
Edit Copy Delete	7	Jishan	Ahmed	amin2646	jishan@gmail.com	http://socialmedia.com/profile_pic/12351
Edit Copy Delete	8	Adeel	Abideen	jjjkk222	konick@gmail.com	http://socialmedia.com/profile_pic/12352
Edit Copy Delete	9	Miraj	Ahmed	ahafjh	miraj@gmail.com	http://socialmedia.com/profile_pic/12353
Edit Copy Delete	10	Pseudo	Amin	kk2222	kkk@gmail.com	http://socialmedia.com/profile_pic/12354

Fig 9:- Storing in the database

C. Uploading the profile picture

After opening an account on the social networking site, a user must upload an image as a profile picture as per our model.

ISSN No:-2456-2165

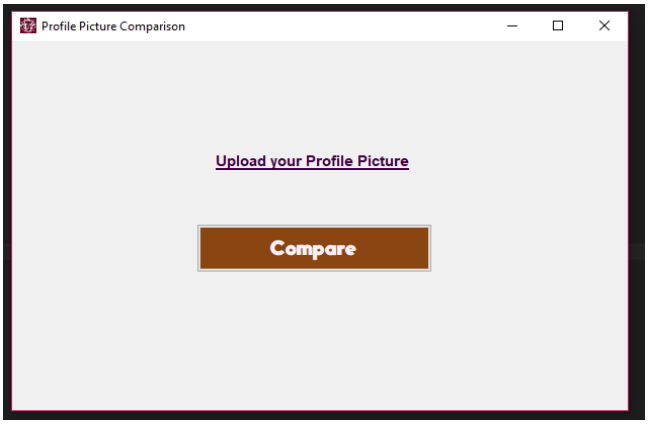

Fig 10:- interface of image comparison simulation

D. Sorting out the similar name

Whenever the profile picture tries to occupy a space in the database an automated query will summon all the ID which contain the same profile name.

Generally, by using the SELECT keyword, we can fetch all the data that we want on a MySQL database system. Here, our goal is to summon all the ids which have got the same name. That is why it is necessary to implement this SQL query in the database-

SELECT * FROM user WHERE name LIKE '%AdeelAbideen%';

This query should fetch all the records where Adeel Abideen appears anywhere in the name field. By doing so, we can get all the similar names together for operating the image comparison operation.

userID	firstName	lastName	password	email	profile_pic
1	Adeel	Abideen	amin2646	jishan@gmail.com	http://socialmedia.com/profile_pic/12344
2	Adeel	Abideen	jishan22	majed@gmail.com	http://socialmedia.com/profile_pic/12345
8	Adeel	Abideen	jjjkk222	konick@gmail.com	http://socialmedia.com/profile_pic/12352

Fig 11:- Summoning the same profile names

E. Comparing the image with the all other profile images which hold the same profile name

Using an iterative and efficient image comparison technique, all the profile images of the summoned ids need to be compared with the uploaded profile picture.

V. EXPERIMENTAL RESULTS

If the profile picture matches with any other profile pictures that are available in those ids, then a dialogue box will be shown to the user which will hold the message that he/she cannot upload that picture. On the other hand, if does not get matched with any other profile picture, the image will be set as the profile picture of that account.

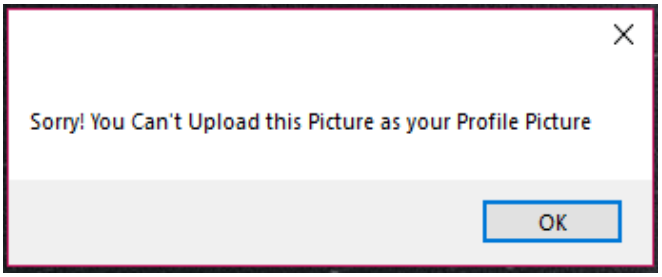

Fig 12:- Message when the image is not unique

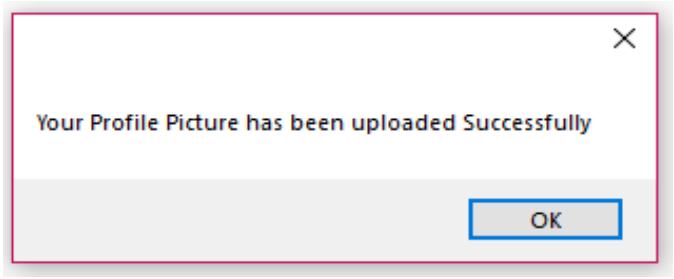

Fig 13:- Message when the image is unique

VI. CONCLUSION AND FUTURE WORK

The main purpose of this paper was to solve the identity theft problem on SocialMedia. For eliminating this type of problem, structure models, as well as an implantation process, have been discussed thoroughly in this paper. Though we tried to reach the most effective solution, still there is some vulnerability that should be fixed to make it more efficient.

As foran instance, if someone uploads an image of any object or place rather than uploading his own face then some problems may arise. If another person with the same name uploads the same picture, our structure model will detect it as an identity theft whereas it is not intended by the second user.

On the other hand, the image comparison techniques are time-consuming. That is why we have to use the most efficient image comparison algorithm in this model.

It is needed to use an optimal and time efficient image comparison technique while implementing this model on the social networking sites. At the same time, to reduce the processing time we need to decrease the number of images that need to be compared with the uploaded image to check its uniqueness.

Hence, we should look for some more parameters by which we can shrink the number of images while comparing for detecting identity theft. Further researches may ease these things to make this model more effective. In the last decade, as the development of various electronic devices grow, the number of internet users have increased exponentially as well [14]. That is why, we need to focus on the security issues of the social networking platforms to keep safe these volume of large data.

REFERENCES

[1]. https://newsroom.fb.com/company-info/, last accessed 2018/1/18
[2]. https://www.nytimes.com/2016/05/06/business/facebook-bends-the-rules-of-audience-engagement-to-its-advantage.html, last accessed 2018/2/3
[3]. T. Jagatic, N. Johnson, M. Jakobsson and F. Menczer, "social phishing", Communications of the ACM, 2005.
[4]. R. Sharma, A. Jain and R. Rastogi, "A new face to photo security of Facebook," 2013 Sixth International Conference on Contemporary Computing (IC3), Noida, 2013, pp. 415-420.
[5]. https://www.telegraph.co.uk/technology/2017/11/02/facebook-admits-270m-users-fake-duplicate-accounts/,last accessed 2018/03/29
[6]. XF. Wang, Y. Mu and RM. Chen, "Privacy-preserving data search and sharing protocol for social networks through wireless applications", concurrency and computation-practice & Experience, volume: 29, Issue 7, DOI: 10.1002/epe.3870, 2017.
[7]. https://www.facebook.com/Majed.JC, last accessed 2018/3/20
[8]. https://www.facebook.com/adeel.abideen, last accessed 2018/3/22
[9]. https://www.facebook.com/imAmin, last accessed 2018/3/20
[10]. Gaff, B.M. (2014). Corporate Risks from Social Media. Computer, 47, 13–15.
[11]. H. Bay, T. Tuytelaars, and L. V. Gool, "Surf: Speeded up robust features," in ECCV, 2006, pp. 404–417.
[12]. D. Lowe, "Distinctive image features from scale-invariant keypoints,"International Journal of Computer Vision, vol. 60, no. 2, pp. 91–110, 2004.
[13]. Jia, Wenjing& Zhang, Huaifeng& He, Xiangjian& Wu, Qiang. (2006). A Comparison on Histogram Based Image Matching Methods. 97. 10.1109/AVSS.2006.5.
[14]. Henson, B., Reyns, B.W. & Fisher, B.S. (2013). Fear of crime online? Examining the effect of risk, previous victimization, and exposure on fear of online interpersonal victimization. Journal of Contemporary Criminal Justice.