USING EMOJI PICTURES TO STRENGTHEN THE IMMUNITY OF PASSWORDS AGAINST ATTACKERS

Dr. Mohammed A. Fadhil Al-Husainy
Raghda Ahmed Malih
Department of Computer Science, Faculty of Information Technology,
Middle East University, Amman, Jordan

Abstract

User authentication is an essential step in information security. Textual passwords are the most traditional ways used in most user authentication systems to achieve the security of information, but textual passwords are vulnerable to many types of attacks such as: dictionary attacks, shoulder surfing, and spyware. Graphical password can overcome the shortcomings of the textual passwords, but it still vulnerable to shoulder-surfing attacks, takes much space in the system and sometimes user takes a long time to enter. By using Emoji-pictures, a new technique that overcomes the drawbacks of both textual and graphical passwords was presented in this paper. The proposed technique is resistant to dictionary attacks, shoulder surfing, and spyware in addition to that it doesn't take large space in the system's database and provides a safe and enjoyable session for users during entering the password.

Keywords: Coding, shoulder-surfing, authentication, information security

Introduction

User authentication is a primary and important component in most computer security procedures. It represents the cornerstone for access control and user accountability (Ahmad Almulhem, 2011, Delphin Raj K M. & Nancy Victor, 2014). There are various techniques of user authentication systems, textual username/passwords are the most common technique of user authentication. They are variety and easy to implement and use. Textual passwords should satisfy two contradictory conditions. They have to be easy to remember by a user, and they have to be difficult to guess by attackers. Users usually choose easily guessable and/or short textual passwords, which are an easy target of the dictionary and brute-forced attacks. Enforcing a strong password policy sometimes leads to negative results, where the users resort writing their difficult-to-remember passwords on sticky notes which exposing them to theft (Saraswati B. Sahu & Angad Singh, 2014, Priti Jadhao & Lalit Dole, 2013). Although that textual passwords are the most traditional models that are used for providing security, but textual passwords are vulnerable to shoulder surfing, dictionary attacks, and spyware.

The main drawbacks of textual password can be summarized in follow:

1. Simple passwords are easy to guess by attackers

2. Hard passwords are not easy to remember by user

3. Dictionary attack successively trying all the words list in the dictionary using an exhaustive search

4. Brute-force attack tries to use every possible combination between characters to guess the password

5. Key-space is limited to 64 ASCII characters

Graphical passwords, sometimes called graphical user authentication (GUA) have been suggested as a possible alternative to textual passwords. Motivation particularly comes from the truth that people can remember pictures better than texts. People can remember pictures better than text as the psychological studies shown. Generally, pictures are easier to remember or recognize than text, especially expressive pictures, which are even remembered easily than random pictures (Saraswati B. Sahu & Angad Singh, 2014). To make passwords more memorable and easier for people to use and, therefore, more secure, graphical passwords have been proposed.

While users may find it difficult to remember a password of fifty characters, users are able easily to remember things they have seen like: faces of people, places they visited, etc. These graphical data provide large password spaces because it represents a huge number of bytes of information. Thus, graphical password present a way of making passwords more human-friendly while increasing the level of security. User authentication techniques that use graphical passwords are classified into two main types: recall-based and recognition-based graphical techniques. User is authenticated, in recognition-based techniques, by requesting him/her to identify one or more pictures that were selected by the user during the registration phase. User is authenticated, in recall-based techniques, by asking him/her to reproduce something that the user created or selected earlier during the registration phase.

Graphical passwords overcome the drawbacks of textual passwords, but still they were vulnerable to shoulder surfing attacks (Ms.Kiran P. Lokhande & Ms.Vimmi Gajbhiye, 2014). Where that the conventional password models are vulnerable to shoulder surfing, many researchers in the field of information security tried develop different graphical password models resist against shoulder surfing. Another important problem in a graphical password is the large size of the graphical password which represents all images that are used in login session for each user. These images surely need a large space in the authentication system database. Text-based graphical password models have been proposed because most users are more familiar with textual passwords than pure graphical passwords. Unfortunately, none of existing text-based graphical password models is both secure and efficient enough to resist against shoulder surfing. A person who gets to monitor a login session could guess the password eventually (depending on the model).

Emoji is the Japanese term for picture characters (see fig. 1). It is necessary to mention here that there are a huge number of Emoji pictures of various types like People, Places, Nature, Objects, Symbols, Transport, etc. and many other pictures are continuously created. Emoji pictures are standardized Unicode characters used increasingly in picture messages as a way to communicate through most social networks applications that used in smartphones and handheld devices such as WhatsApp, Viber, Telegram, etc.

Fig. 1: Emoji pictures of various types

The idea behind this research is to present a new technique that involves the use of Emoji pictures in writing password to strengthen the immunity of password against attackers and suggests a safe and enjoyable model to enter a password. This is done through exploiting the strong points and trying to exclude the drawbacks of both textual and graphical passwords.

Related Works

Usually, users' accounts are affected by the improper selection of passwords and lack of awareness about the correct dealing with passwords. This will result to unauthorized entry to the user’s personal account. In order to supply secure and user-friendly authentication, the security experts are highly recommending the new graphical passwords, which include dragging or clicking activities on the pictures instead of typing alphanumeric characters which overcomes most of the problems that arise from the textual password system. There are many researchers that have attempted and successfully used graphical characters through different techniques. The majority of efforts are now employed to protect data from theft, but how can make them effective is an important issue.

The main aim of Mathur A. (2011) is to lay stress on the security issues related to password selection and management. The idea is to give the users of websites an option to choose the password along with their font color. The passwords must not only represent with at least 6 characters scheme, but also with color coded pattern that can be beneficial to improve the security of password.

Jansen W., Gavrila S., Korolev V., Ayers R. & Swanstrom R. (2003) suggested a graphical password scheme built specifically for mobile devices, this scheme based on "image or picture password". To create a password, the user needs to choose the theme first which consists of thumbnail picture pattern. By selecting thumbnail pictures in a specified sequence, the user can register this sequence to form a password. To login the system, the user needs to recognize and identify the previously selected pictures in the correct sequence in order to be authenticated. Because the numbers of thumbnail pictures are limited only to 30, therefore, the size of the password space is relatively small. To make the created password more complex and difficult, a user can select more than one of thumbnail pictures in order to enlarge the size of the password space.

Real User Corporation has built their own commercial technique named Passfaces TM (2007) based on the truth that the human can remember human faces easier than other pictures. In Pass faces technique, users are needed to select the prior seen human face from a set of nine faces: one is known and the others are decoys. The four faces required are determined by repeating the previous step. A comparative study by Brostoff S. & Sasse M. (2000) showed that it is easy to remember the Pass faces pass-word than the textual passwords. But the users which use pass faces technique need long login time than textual passwords.

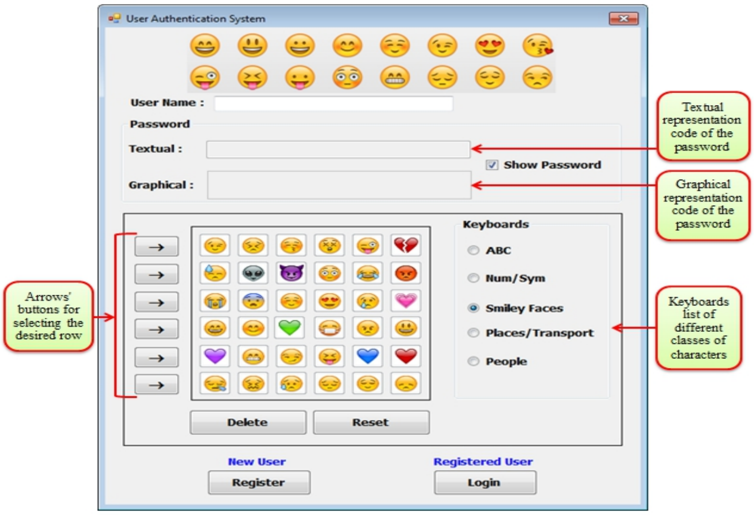
Sobrado L. & Birget J. (2007) introduced a "moveable frame scheme" by selecting three pass objects in this technique. The first object of the pass-objects is put into the movable frame. The user rotates the frame to place all the pass-object in a straight line for authentication. Sobrado and Birget suggested repeat the process many times by clicking or distribute it randomly to decrease the possibility of logging. This is unpleasant step, confusing and lengthy because set non-pass objects are engaged. Sobrado and Birget also suggested a scheme called “special geometric configuration”. Four pass objects are participated to form an intersection point in this scheme. The user requires clicking on the object nearest to the intersection point to be authenticated.

Passlogix (2005) developed a different graphical password system. Users, in this system, must click on various items in the image that displayed by the system in the right sequence in order to be authenticated.

Nithya (2014) was introduced a new graphical password that deals with authentication through pictures. To be authenticated, the user selects four regions which he/she finds simple to remember to produce the password. The user can select his/her own images for creating the password and also for raising the level of security, more than four clicked points could be chosen. The biggest obstacle for current graphical passwords is that the shoulder surfing problem.

The Proposed Password System:

Good password system must achieve many factors: gives an easy to remember and deal with password by user, hard to steal and guess password by attackers, provides safe login session for user that is resisting against different types of password attacks and doesn't take a large space in the authentication system database to store passwords. The proposed system focuses on the use of Emoji pictures, in writing password, to find solutions and overcome the problems of both textual and graphical passwords and to achieve all the factors needed to get a good password. The proposed system was built and implemented using C# programming language. The system's operations involved: **Preparation operations** and **Login session**. Fig. 2 shows the main interface of the system.



☑ Show Password

● Smiley Faces

User Authentication System
User Name :
Password
Textual :
Graphical :
Keyboards
○ ABC
○ Num/Sym
○ Places/Transport
○ People
Delete
Reset
New User
Register
Registered User
Login
Textual representation code of the password
Graphical representation code of the password
Arrows' buttons for selecting the desired row
Keyboards list of different classes of characters

Figure 2: Main interface of the system

Preparation operations

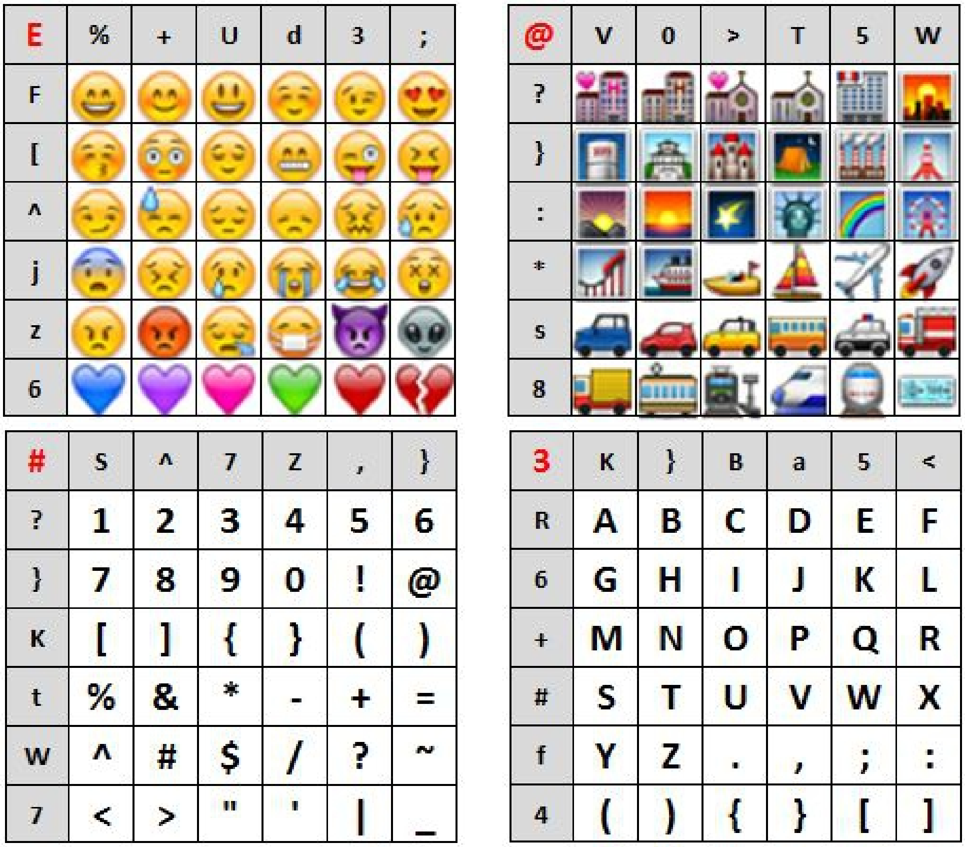
There is number of preparation operations that must be done by the system. These operations are:

1. Classify alphabet letters, numbers, special symbols and Emoji pictures and put each class into different tables (keyboards).

2. Each table (keyboard) consists of n rows and n columns (as 2D matrix). Keyboards of 6×6 have been used here only to give a simplified clarification.

3. Coding the characters in each cell of the table (keyboard) such that each character represents by three ASCII codes (bytes): (Table code, Row code and Column code). See fig. 3 below for example.

Example: Code of: 🚚 is: **@ 8 V**



E	%	+	U	d	3	;
F	😄	😊	😃	☺️	😉	😍
[	😚	😳	😌	😁	😜	😝
^	😏	😓	😔	😞	😖	😥
j	😰	😣	😢	😭	😂	😲
z	😠	😡	😪	😷	👿	👽
6	💙	💜	💗	💚	❤️	💔

@	V	0	>	T	5	W
?	🏩	🏨	💒	⛪	🏢	🌇
}	🏪	🏯	🏰	⛺	🏭	🗼
:	🌄	🌅	🌠	🗽	🌈	🎡
*	🎢	🚢	🚤	⛵	✈️	🚀
S	🚙	🚗	🚕	🚌	🚓	🚒
8	🚚	🚃	🚉	🚄	🚅	🎫

#	S	^	7	Z	,	}
?	1	2	3	4	5	6
}	7	8	9	0	!	@
K	[	]	{	}	(	)
t	%	&	*	-	+	=
W	^	#	$	/	?	~
7	<	>	"	'	|	_

3	K	}	B	a	5	<
R	A	B	C	D	E	F
6	G	H	I	J	K	L
+	M	N	O	P	Q	R
#	S	T	U	V	W	X
f	Y	Z	.	,	;	:
4	(	)	{	}	[	]

Figure 3: Tables (keyboard) of different classes of characters.

Login session

After the system complete the preparation operations, the registration/login session for the users to enter their passwords become ready. Firstly, the system distributes randomly, over the cells of each keyboard, all characters that belong to the keyboard. See fig. 4.

To enter one character in the Emoji password, the user must follow the steps listed below and repeat the same steps for each character in the password:

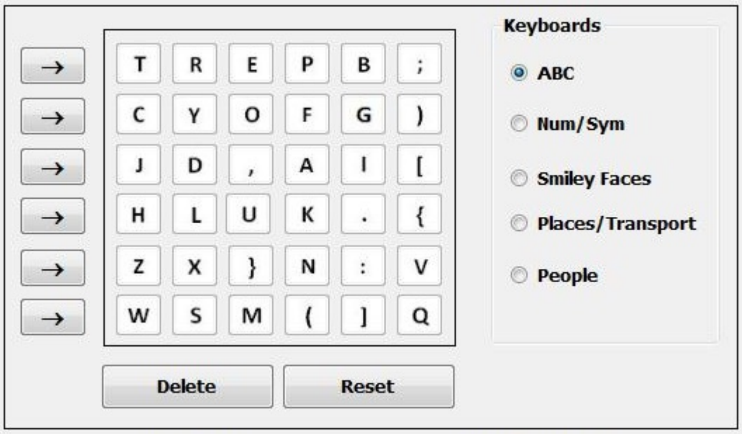
Step 1: the user selects the desired keyboard from the set of keyboards in the right panel by click on the radio button. See fig. 5.

Step 2: the user clicks on the arrow's button that points to the row contains the desired character in the keyboard. The system records the row number that is selected by the user (row number 4 in the fig. 6). No one can know what the character been chosen by the user in that row even the attacker which monitors the login session.

Step 3: the system transposes the rows and columns of the keyboard. This is done by exchanging the elements in each row with the elements in the each column. For example, the character in row 2 and column 5 becomes in row 5 and column 2. See fig. 7.

Step 4: the user clicks on the arrow's button that points to the row contains the same selected character in step 2. The system records the row number that is selected by the user (row number 1 in the fig. 8).

Step 5: The system immediately redistributes randomly all the characters in the keyboard. (See fig. 9). The system uses the row numbers in Step 2 and Step 4 (Numbers 4 and 1 above to determine the selected character by the user through getting the character at row 4 and column 1 from the keyboard in fig. 6 (the keyboard in Step 2). Certainly, only the system can see (access) the mentioned keyboard, because the current keyboard that is now displayed to user (and attacker if he/she exists and monitors the login session) is completely different than the keyboard displayed in Step 2. This will give the system a high immunity against the *shoulder surfing attacks*.



T	R	E	P	B	;
C	Y	O	F	G	)
J	D	,	A	I	[
H	L	U	K	.	{
Z	X	}	N	:	V
W	S	M	(	]	Q

Keyboards

● ABC

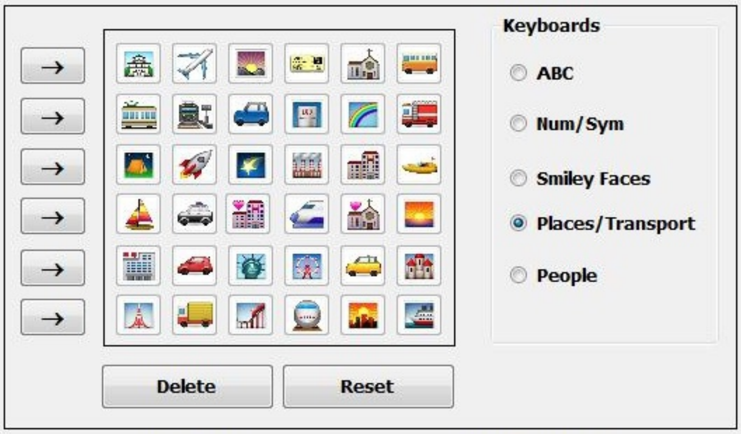
○ Num/Sym

○ Smiley Faces

○ Places/Transport

○ People

Figure 4: Login session: randomly distribute all characters over the cells of each keyboard



Keyboards

○ ABC

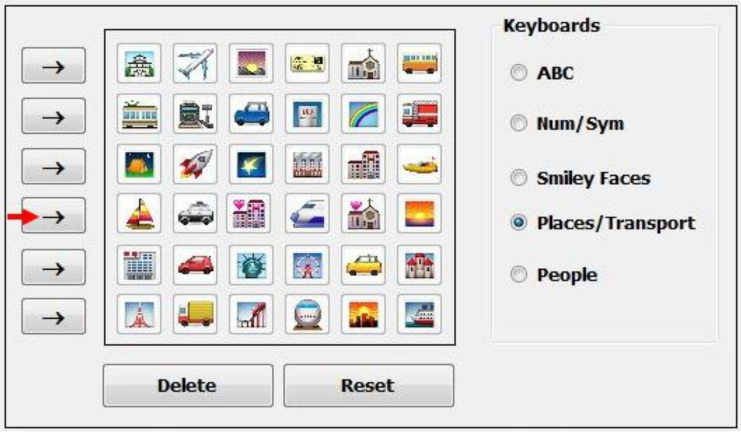
○ Num/Sym

○ Smiley Faces

● Places/Transport

○ People

Figure 5: Login session: Step 1



Keyboards

○ ABC

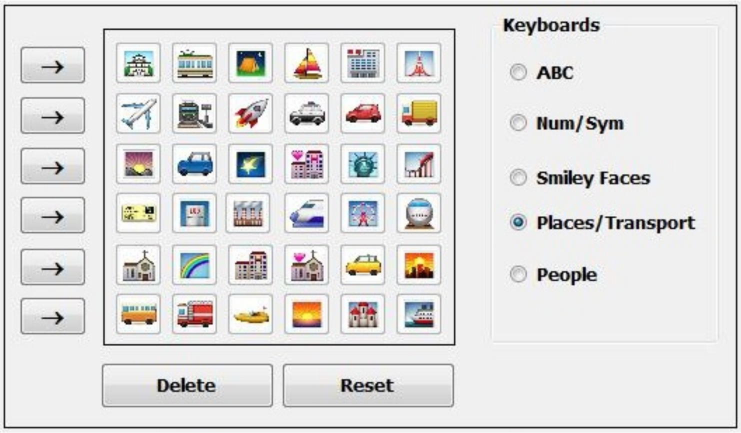
○ Num/Sym

○ Smiley Faces

● Places/Transport

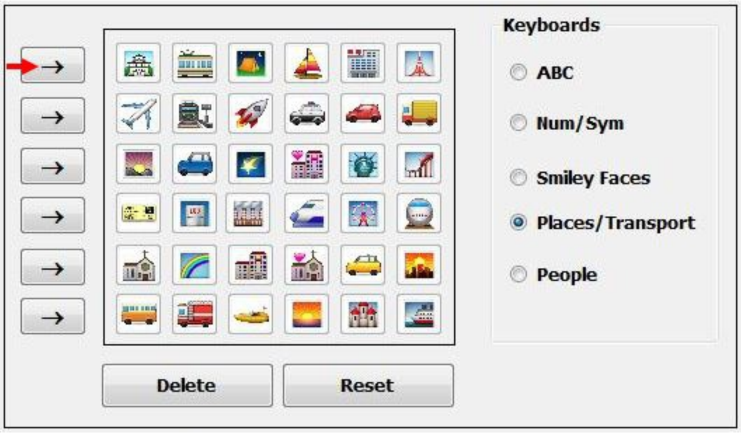
○ People

Figure 6: Login session: Step 2



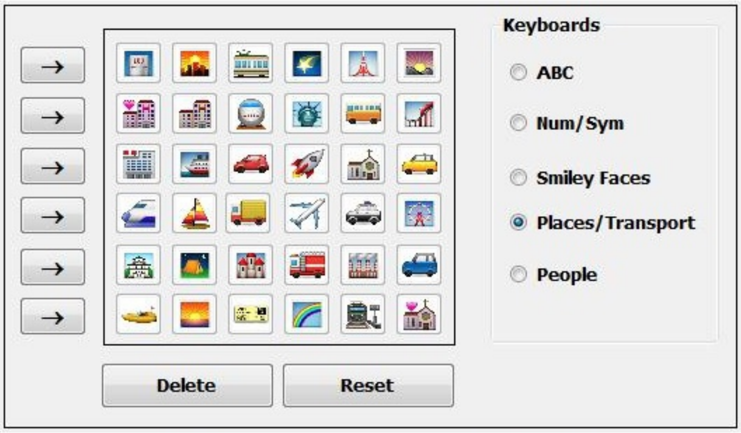
Keyboards
○ ABC
○ Num/Sym
○ Smiley Faces
● Places/Transport
○ People

Figure 7: Login session: Step 3



Keyboards
○ ABC
○ Num/Sym
○ Smiley Faces
● Places/Transport
○ People

Figure 8: Login session: Step 4

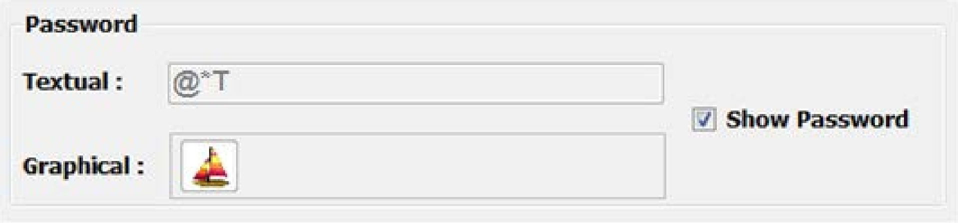


Keyboards
○ ABC
○ Num/Sym
○ Smiley Faces
● Places/Transport
○ People

Figure 9: Login session: Step 5

As we see in the above figure, each Emoji picture (character) in the new password will be represented as three bytes (i.e., three ASCII codes). These codes represent **Table code**, **Row code** and **Column code** of the selected Emoji picture by the user, as mentioned in the preparation operation above. The system stores the three bytes (codes) of all characters of the password in its database. The selected character by the user in the above steps is ⛵, and its code (the three bytes of it), that have been determined previously by the authentication system in the preparation operation, are **@*T** (see fig. 10).

This will keep the space required to store passwords in small size in comparison with the space used in most graphical password schemes. The same five steps above will be used to enter each character in the new Emoji password.



Password

Textual : @*T

☑ Show Password

Graphical : ⛵

Figure 10: Graphical and Textual representation codes of the password's character

Analysis and Discussion

In the era of competitive in information technology, information security management becomes one of the most important and necessary issues facing individuals, companies, institutions and even governments. User authentication considers the first defence against security breaches. Therefore, the system has been built carefully to achieve the following goals:

1) The use of Emoji pictures in writing password helps users to use the recent and common technology used in most smartphones and other handheld devices.

2) The use of Emoji pictures in writing password gives high feasibility in the user authentication systems. This makes the new password stronger and difficult to guess by attackers through increasing the range of symbols that used in writing each character of the password. In other word, By raising the complexity of the password (i.e., number/range/key-space of available symbols used by user in writing each character of the password from 64 ASCII characters in traditional (textual) password to be in 256×3 ASCII for each character in the password).

3) The use of Emoji pictures in writing password makes the new password more secure and hard for others to locate it and obtained by making it easy for users deal with their own passwords. Using Emoji pictures in password allows users choosing a set of words or (sentence) refers to the meanings of the Emoji pictures but not the same characters (Emoji pictures) used. Then the users can deal with their password in a more safe way by writing the sentence on the notebook or storing it in a file on the computer storage unit. This will remove any doubts about the nature/reality of the characters being used in the password. For more clarification about this powerful point see fig. 11.

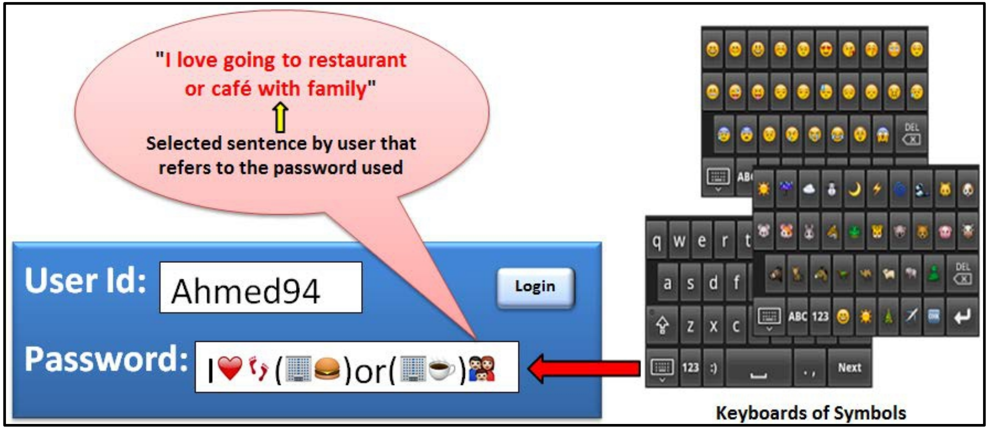

"I love going to restaurant or café with family"
⇧
Selected sentence by user that refers to the password used
User Id:
Ahmed94
Login
Password:
Keyboards of Symbols

Figure 11: Using Emoji pictures in writing password

4) The use of Emoji pictures in writing password makes the new password easier to remember by the user than before. Recent scientific researches proved that the human brain has an ability to remember images more than random texts. Using Emoji pictures in writing password helps users to link these Emoji pictures with a set of meaningful words or with a sentence. In addition to that, user became has an ability to deal with the sentence that refers to the real password through writing it in a notebook or storing it in the computer storage unit without need to write the password itself. This will keep the real password away from theft by attackers (see fig. 11).

5) The proposed user authentication system facilitates the session of entering a password for the user and makes this session enjoyable and more resistant against the shoulder surfing attacks. This is achieved in the system through there isn't any clicking on the chosen characters in the system keyboards.

6) The proposed authentication system does not use a large storage space to store the new Emoji password when it is comparing with the most graphical passwords.

Conclusion

User authentication is a substantial component in most information security contexts. A user authentication system was proposed in this paper based on using Emoji pictures in writing password through giving the users a new model for entering their passwords. The system tried provide users an enjoyable and secure authentication system by combining graphical and textual-based passwords to exploit the best advantages of both worlds. The analysis and discussion of the features of the proposed system showed that the system succeed in achieving most of the goals to get the good user authentication system.

Acknowledgement

The authors appreciate the deanship of scientific research at Middle East University for funding this research.

References:

Ahmad Almulhem.(2011). ' A Graphical Password Authentication System'. World Congress on Internet Security (WorldCIS-2011), London, UK, 21-23.

Brostoff S. and Sasse M. (2000) 'In People and Computers XIV – Usability or Else'. Proceedings of HCI. Sunderland, U.K..

Delphin Raj K M. and Nancy Victor. (2014). 'A Novel Graphical Password Authentication Mechanism'. International Journal of Advanced Research in Computer Science and Software Engineering, 4, (9), September.

Jansen W., Gavrila S., Korolev V., Ayers R. and Swanstrom R. (2003). 'Picture Password: A Visual Login Technique for Mobile Devices'. NISTt NISTIR 7030. http://csrc.nist.gov/publications/nistir/nistir-7030.pdf

Mathur, A. (2011). 'Improved password selection method to prevent data thefts'. International Journal of Scientific & Engineering Research, 2, (6). http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.301.8248&rep=rep1&type=pdf

Ms.Kiran P. Lokhande and Ms.Vimmi Gajbhiye. (2014). 'Extended Text and Color Based Session Password Security against Shoulder Surfing and Spyware' Journal of Emerging Technologies and Innovative Research (JETIR), 1, (7).

Nithya. (2014). 'GRAPHICAL PASSWORD'. International Journal of Computer Science and Information Technology Research, 2, (3). http://searchsecurity.techtarget.com/definition/graphical-password

'Passlogix', (2005, June). www.passlogix.com.

Priti Jadhao and Lalit Dole. (2013). 'Survey on Authentication Password Techniques'. International Journal of Soft Computing and Engineering (IJSCE), 3, (2).

'Real User Corporation', (2007). Passfaces TM, www.realuser.com.

Saraswati B. Sahu and Angad Singh. (2014). 'Survey on Various Techniques of User Authentication and Graphical Password'. International Journal of Computer Trends and Technology (IJCTT), 16, (3).

Sobrado L. and Birget J. (2007). http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm.