The Usability of Emoji Pictures in Recognition Based Graphical Authentication for Mobile Devices

SA'ADATU GARBA KUTA[1], HASSAN UMAR SURU[2], MUHAMMAD SIRAJO ALIYU[3]
[1, 2, 3] *Computer Science Department, Kebbi State University of Science and Technology Aliero, Nigeria*

Abstract- ***Review on the use of emojis as an alternative to PIN entry and text passwords was conducted by analyzing the current state of emoji-based authentication. Mobile devices store a lot of personal data and despite all the technological progress, the usability and security of mobile authentication mechanisms did not significantly evolve, as a consequence, data protection is still an annoying and sometimes difficult task which requires an active contribution of the user. This Work explores emojis as graphical password alternative for user authentication. Most of the graphical authentication schemes provide longer authentication times and therefore emojis were chosen to be the alternative to reduce the lengthy authentication time and improve the memorability of the password. The usability and security evaluation have been conducted from a designed prototype system of emoji face (EF), passface (PF), animal emoji (AE), real animal (RA), food emoJI (FE), real food (RF), Object emoji (OE) and real object (RO) using java programming language. This is done to explore the differences among efficiency, effectiveness, and user preference. The findings showed an acceptable level of efficiency, effectiveness and user satisfaction of the proposed system. The emoji passwords Ware easy to remember, password creation and login are fast, and a positive user experience is also recorded. However, certain emojis were preferred by the participants.***

Indexed Terms- Animalemoji, Emojface, Foodemoji, Objectemoji, Passface, Realemoji

I. INTRODUCTION

An emoji is a digital image used in electronic communication (usually inline in text) that can represent things such as weather, vehicles, countries, food, animals etc. or express emotions, feelings, or activities [5]; [13]. The word emoji originates from Japanese where e means picture and moji stands for written character [13].

In 1999, the first emojis arrived on Japanese mobile phones. However, it was not before in 2009 that the first emojis were added to Unicode [6]. The Unicode Standard ensures consistent encoding, as well as trouble-free international exchange of characters and text, and is maintained by the Unicode Consortium [13].

Since emojis became part of Unicode and leading mobile Oss such as Apple's iOS and Google's Android introduced emoji keyboards the usage of emojis has increase on many social media platforms, the proposed study carried out the implementation using Java Programming language using various steps highlighted in the architecture of the system [6].

This was therefore designed such that the user either login as an existing user or register as a new user so as to have access to the developed system. Hence enable him or her into the system in other to provide username as an existing user. Going through, he/she provide by selecting number of password image, grid size. After that has been carried out, the developed system then prompt whether emoji has been selected or not. If Yes, the system preview your selected emojis else, the system takes you back through the process to get that done. Also, if the emoji is selected, press continues by comparing what is the database with the selected emojis for authentication. Finally, if both match, the system grants access else deny access. [3].

II. REVIEW OF RELATED LITERATURE

Emoji originated from smiley, which first evolved into emoticons, followed by emoji and stickers in recent years. Smiley first appeared in the 1960s and is regarded as the first expression symbols. Smiley is a yellow face with two dots for eyes and a wide grin

which is printed on buttons, brooches, and t-shirts. By the early 1980s, this symbol had become widespread, emerging as a permanent feature of western popular culture [3]. [3] also presented systematic reviews in related research on emoji, aimed to provide developmental process, usage features, functional attributes, and fields of research related to emoji. They opined that Emoji developed from emoticons, and have both emotional and semantic functions are influenced by and vary according to factors such as individual circumstances, culture, and platforms.

In [1]. Emoji pictures were used in writing password. The system combines graphical and textual-based passwords. This was done to strengthen the immunity of Passwords Against attackers. The 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.

[7] opined that emojis are not only used in normal communication between friends and family but also penetrate the professional sphere. It is also important to mention that they express ambiguity of meaning and lead to misunderstandings.

Emojis are not a new language developed by the technological adept younger generations, but instead are an evolution of older visual language systems that make use of digital technology to create greater layers and nuance in asynchronous communications. Furthermore, emojis are devices for demonstrating tone, intent and feelings that would normally be conveyed by non-verbal cues in personal communications but which cannot be achieved in digital messages. It is also evident from prior works and analyses of usage that there are universal meanings to Emojis [2].

The usability and security evaluation by [14] conducted to explore the differences among efficiency, effectiveness, memorability, user satisfaction, and password space and entropy have the findings of an acceptable level of efficiency, effectiveness and user satisfaction. In addition to achieve a resistance against the shoulder surfing attacks

A literature study on the use of emojis as an alternative to PIN entry and text passwords was conducted by [9]. They analyzed the current state of emoji-based authentication and proposed a novel password scheme called EmojiStory. In EmojiStory, passwords are created from predefined stories and emojis selected by the user. The security and usability of the system was evaluated through two online surveys, in which more than 1,700 participants took part. The results from the surveys suggest that EmojiStory offers good usability. The emoji passwords are easy to remember, password creation and login are fast, and a positive user experience is provided. The results also indicate that EmojiStory offers better security than PIN.

In a two-part user study, [12] investigated if and how emojis are suitable in the regular usage on web. Users were asked to create passwords that contained both regular alphanumeric characters and emojis. The study shows that users' primary selection strategy was to create meaningful relationships between the emoji and the rest of the password. It was also found that platform dependent renderings of emojis do not necessarily reduce usability, if the object represented by the emoji is distinctive enough. As websites are already starting to allow emojis in passwords, it is important to evaluate this step carefully.

A study artifact named emojiauth was developed to explore the implications of Emoji-based mobile authentication. A between-subjects study (n=53) conducted to compare EmojiAuth to PIN entry as a baseline. It was found that Emoji-Auth provides login times comparable to PIN and reasonable memorability. The result also indicate that once participants were familiar with EmojiAuth, they perceived EmojiAuth as providing a more positive user experience compared to PIN [10].

In a study by [4]. A clear majority of users reserves their emoji use for individuals with whom they experience close personal ties friends, family members, and intimate partners, hundreds of sentiments can be conveyed through the use of emojis within digital environments.

In the study of [8], a distant supervised learning approach was proposed where the training sentences are automatically annotated based on the emojis they

have. It shows that training classifiers on cheap, large and possibly erroneous data annotated using this approach leads to more accurate results compared with training the same classifiers on the more expensive, much smaller and error-free manually annotated training data. Our experiments are conducted on an in-house dataset of emotional Arabic tweets and the classifiers considered are: Support Vector Machine (SVM), Multinomial Naive Bayes (MNB) and Random Forest (RF).

[11] developed two concepts to combat shoulder surfing attacks in their study. First, the user must register if the registration does not exist. Second, the user must log in with a valid user ID and password. The password is a grouping of characters and numbers. Third, user has to cross image-based authentication where user can choose their password and this method have higher chances to offset each other. Password must match with the one at login time. In colour base authentication, there should be several colour base passwords and depending on the colour, you need to remember the password sequence. And it's like three-factor authentication. So, here is proposed a new graphical password authentication technique that is resilient to shoulder surfing and also to other types of probable attacks.

III. MATERIALS AND METHODS

- Methodology

A quantitative analysis using a Likert type scale questionnaire ranging from 1 to 5 was used for all the questions, where for all the ranking scores, a 5 score was the highest possible positive score that could be allocated and 1 the least score.

- Participants

68 participants were selected for the experiment. The participants chosen were selected from the undergraduate students of kebbi State University of Science and Technology Aliero by means of politely asking for the participants to show interest in the experiment after explaining the aim of the experiment. We decided not to select users with certain characteristics because we believe they have undergone several practical and assignments on high computer usage experience, high confidence in using computers and experience of using the internet. Linked to these, we specifically asked and confirm from the participants if there is anyone without internet browsing and computer usage experience of which no one affirmed to that. Also the subjects recruited had a mixture of male and female participants of at least 16 years.

- Tools Used

The following materials were used in the research:

- Two laptop computers both running Windows 10, 4GB RAM, 500GB HDD, a dual core 2.4330GHz processor, a 64-bit operating system and a 24-inch monitor,
- Firefox internet browser.
- Two Stop watches

- Experiment

In this study, several factors have been used to make the study more objective. These factors include:

1. Gender
2. Age group of participants.
3. Educational attainment of participants.

We have been keen to choose the appropriate number of participants of different ages and educational backgrounds (academic achievements). In our study, we chose more than 68 participants to test the authentication system. Age distribution of participants has been chosen based on the following classes:

1. Less than 16,
2. 16-25,
3. 26-35,
4. 36-45,
5. 46 and above

Also, the educational backgrounds (academic achievement) of participants have been chosen based on the following classes:

1. Primary education,
2. Secondary education,
3. Tertiary education,
4. None formal education

- Statistical Analysis

The data for this research was compiled using Microsoft excel and analyzed by statistical package for social sciences (SPSS) version. All the collected data was firstly explored with summary statistics.

Descriptive statistics such as percentages, frequency, mean, standard deviation, standard error of mean, minimum, and maximum distributions was used to present the characteristics of the results. Paired sample t-test was used to compare the mean values of the distributions of the same design type. For statistical analysis an alpha level of 0.05 was used.

- Task Procedure

In our research work we designed different modules of emoji's ranging from food, transports, animals, kitchen and pass faces. At the beginning, the participants were introduced to the procedure of the study, having completely familiarized themselves with how the prototype works. To generate a graphical password, the participants were required to register first and log into the prototype (see APPENDIX for all the screen shots). The figure 1 is a login panel of the software, this is the entry panel of the software, and the panel allows the user to register before start using the application. And participants can also increase the number of password images as well as the Grid size; hear we only used number of password 1 and number of grid size 3.

The figure 2 panel display only if Sign Up button is been pressed from the figure 3, it provide the user to enter his/her name which will allow the user to select and assign an emoji to the registered name or name used to register the user.

The user is expected to press continue button after entering his/her name. figure 4 display only after the user press continue, the pass image for step 1 is empty and cannot display anything image or emoji until the user press preview button.

The above figure 5 display after the user press preview button, the emoji's in the above panel will display and it will allow the user to select the preferred emoji that they want to use as password. Only correctly selected emoji will grant access to the system.

The figure 6 shows the selected or choosing emoji that the user selected as his/her emoji from this moment only this emoji face will be granted access login into the system.

The figure 7 panel is where the user will select an emoji as login detail required to login into a system, this panel is sensitive to every selected emoji and will use the selected emoji to compare with register emoji and verify before granting or deny access to the system.

The figure 8 shows that, the user has chosen wrong emoji as his/her login image and system sent an error message as "Authentication Failed. Please Try Again". By pressing OK button the application will automatically redirect the user to the figure 5

The figure 8 shows that, the user has selected the right emoji as login image and system responded with the message above as Authentication Successful.

IV. RESULTS AND DISCUSSION

- Results

A total valid number of participants that took part in the experiment were 68 (100%), this implies that there is no invalid data from the experiment. The major descriptive statistics are discussed accordingly.

- Demographic Information of the Subjects

Table 1 to Table 3 describes the demographic data of the respondents. Table 4.1 shows that most of the participants were male 50(73.5%) and female 18(26.5%).

Table 1: Gender of the respondents

Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	18	26.5	26.5	26.5
	Male	50	73.5	73.5	100.0
	Total	68	100.0	100.0	

Table 2 shows that 25% of the participants fall within the age bracket of (16-25) years, 36.8% fall within (26-37) years, 22.1% fall within (36-45) years, 4.4% of the participants are <16 years and lastly 11.8% are 46 years and above.

Table 2: Age distribution of the respondents

Age Group

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	(16 -25)	17	25.0	25.0	25.0
	(26-35)	25	36.8	36.8	61.8
	(36-45)	15	22.1	22.1	83.8
	<16	3	4.4	4.4	88.2
	46 and above	8	11.8	11.8	100.0
	Total	68	100.0	100.0	

Table 3 shows the educational background of the respondents of which only 2.9% has no formal education, about 8.8% has primary education, 26.5% has secondary edution while 61.8 has tertiary education background.

Table 3: Educational background of the respondents

Education

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	None	2	2.9	2.9	2.9
	Primary	6	8.8	8.8	11.8
	Secondary	18	26.5	26.5	38.2
	Tertiary	42	61.8	61.8	100.0
	Total	68	100.0	100.0	

- Sign up Time

The below table (Table 4) is a sample statistics showing the mean, standard deviation and standard error of mean of the sign up time. The first column contains the list of the pairs namely pair 1, pair 2, pair 3 and pair 4. Second column contains the categories of password types, the EF, PF, AE, RA, FE, RF, OE and RO stand for Emoji face, pass faces, animal emoji, real animal, food emoji, real food, object emoji and real object respectively. The third Column have mean as the heading with 32.28 as mean time for EF sign up time, 35.97 for PF sign up time, 31.79 for AE sign up time 36.66 for RA sign up time, 32.25 for FE sign up time, 34.97 for RF sign time, 31.46 for OE sign up timeand 35. 51 for RO sign up time respectively. The fourth, fifth and sixth columns contains numbeer of participants, standard deviation and standard error of mean for the corresponding mean of the password categories respectively

Table 4: Paired sample statistics for sign up time

Paired Samples Statistics

Variables	categories	Mean	N	Std. Deviation	Std. Error Mean
Pair 1	EF Sign up Time	32.28	68	12.300	1.492
	PF Sign up Time	35.97	68	14.225	1.725
Pair 2	AE Sign up Time	31.79	68	11.858	1.438
	RA Sign up Time	36.66	68	16.047	1.946
Pair 3	FE Sign up Time	32.25	68	11.976	1.452
	RF Sign up Time	34.97	68	14.653	1.777
Pair 4	OE Sign up Time	31.46	68	12.184	1.478
	RO Sign up Time	35.51	68	14.530	1.762

- Login Time

The below table (Table 4.5) is a sample statistics showing the mean, standard deviation and standard error of mean of the login time. The first column contains the list of the pairs namely pair 1, pair 2, pair 3 and pair 4. Second column contains the categories of password types, the EF, PF, AE, RA, FE, RF, OE and RO stand for Emoji face, pass faces, animal emoji, real animal, food emoji, real food, object emoji and real object respectively. The third Column have mean as the heading with 30.28 as mean time for EF login time, 33.97 for PF login time, 31.79 for AE login time 36.66 for RA login time, 30.25 for FE login time, 35.97 for RF login time, 31.46 for OE login time and 34. 51 for RO login time respectively. The fourth, fifth and sixth columns contains numbeer of participants, standard deviation and standard error of mean for the corresponding mean of the password categories respectively

Table 5: Paired sample statistics for login time

Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	EF Login Time	30.28	68	10.300	1.392
	PF Login Time	33.97	68	12.225	1.625

Pair 2	AE Login Time	31.79	68	11.858	1.438
	RA Login Time	36.66	68	16.047	1.946
Pair 3	FE Login Time	30.25	68	10.976	1.352
	RF Login Time	35.97	68	15.653	1.877
Pair 4	OE Login Time	31.46	68	12.184	1.478
	RO Login Time	34.51	68	13.530	1.662

- User Preferences

The below table (Table 4.6) is a sample statistics showing the mean, standard deviation and standard error of mean of the rank scores. The first column contains the list of the pairs namely pair 1, pair 2, pair 3 and pair 4. Second column contains the categories of password types, the third Column have mean as the heading with 3.85 as mean rank for EF rank score, 2.50 for PF rank score, 3.76 for AE rank score 2.22 for RA rank score, 3.66 for FE rank score, 2.42 for RF rank score, 3.54 for OE rank score and 2.32 for RO rank score respectively. The fourth, fifth and sixth columns contains numbeer of participants, standard deviation and standard error of mean for the corresponding mean of the password categories respectively

Table 6: Paired sample statistics for rank scores

Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	EF Rank Score	3.85	68	.981	.119
	PF Rank Score	2.50	68	1.153	.140
Pair 2	AE Rank Score	3.76	68	1.094	.133
	RA Rank Score	2.22	68	.975	.118
Pair 3	FE Rank Score	3.66	68	1.045	.127
	RF Rank Score	2.41	68	1.096	.133
Pair 4	OE Rank Score	3.54	68	1.099	.133
	RO Rank Score	2.32	68	1.112	.135

- Discussion

In comparison with other similar techniques of graphical password, there are both benefits and disadvantages in Secure Image Emoji. At first glance, many participants believed it was too complicated; nonetheless, the system's learning and practice created the opposite feeling, as it was easy to use and acceptable to most participants.

According to [5], efficiency can be measured in a number of ways, such as the time to complete a given task, or the number of keystrokes required to complete a given task. Efficiency of password was measured as the proportion of participants who logged into the prototype in certain of time. Details of time to sign up and time to login into prototype were captured in this study.

To answer the first research question (R_A), this study compared the usability and performance of emoji faces with real images on a prototype design of password creation and login. The data was initially explored by looking at the distributions and overall pattern. A parametric test (two sample t-test) was conducted since the initial examination suggested that there was enough normality in the data. For statistical analysis an alpha level of 0.05 was used.

To answer the second research question (R_B). The mean time when signing up a password (figure 4) for the EF was at 32.28 seconds as compared with PF 35.97 seconds. This can be explained that participants were faster in the sign up for emoji faces than the pass faces. In the sign up for AE and RA at 31.79 and 36.66 also indicate that participants wee faster in creating password for AE. In the same vein FE and RF at 32.25 and 34.99 shows that participant's time to sign up was faster in FE. And lastly participants were faster in OE (31.46) than RO (35.51) seconds. T-test for total sign up time (appendix C) shows there is statistically significance difference between the eight test conditions. By examining the time data in full (Table 4), it can be seen that the mean time difference between passwords of the same design type was identified although not to a significant effect.

The questionnaire data show that participants prefer the passwords that have emojis than those of the real objects

This indicates that signing up with emojis is faster than that of real objects. This is primarily because the picture superiority effect of images and emojis helped

them in memorizing their password. Further analysis on logging time can be supported by the total mean values of all the eight test conditions. Figure 4.5 shows that the mean values of login time for emoji face, animal emoji, food emoji and object emoji were lower than that of pass faces, real animal, real food and real object respectively which indicates that the former were faster and this Answers the third research question (R_C)

In terms of Efficiency, Participants were timed in their use of graphical password application from the start of password registration to completion of the login process. In system application, this process comprised of clicking the 'Register' button, selecting one image, clicking 'Select' button, choosing and dragging four desired emojis onto the image, clicking 'Next' button, memorizing the location of emojis, clicking 'Confirm' button and finally, finishing the registering process by clicking on 'Yes' button.

Details of time to register password in application were captured in this study as presented in Table 4.

For the rank scores, the descriptive statistics in table 4.6 above indicates that the EF, AE, FE and OE rank scores (M=3.85, SD=0.981), (M=3.76, SD=1.094), (M=3.66, SD=1.045) and (M=3.54, SD=1.099) respectively have the highest mean ranks across the eight test designs. A paired sample T-test was conducted to check the mean rank scores; the results show that there is statistically significant difference in rank scores between the four emoji designs as compared with the real images $t(67) = 6.973, 7.927, 5.758, 6.779$, $p < 0.001$ (two-tailed) respectively for all the emojis and this Answers the fourth research question (R_D).

CONCLUSION

This research offered a helpful system for authenticating graphical password application by pairing real images with emoji pictures. The primary input is the introduction of recognition based graphical methods that use emojis in order to resist several common threats to security without sacrificing the usability of graphical password. The findings of the results show that the system is efficient, effective and reach the user satisfaction.

RECOMMENDATION

The results indicate that Emojis offers better usability than real or actual images. However, certain emojis were preferred by the participants. Therefore, further research is needed to compare observed bias in the passwords with that of other authentication systems. We also advise that further studies on the memorability provided by Emoji should be conducted. Also, in the real world, people own multiple passwords which are used in various applications. Therefore, it might be of interest to study how many emoji passwords a person can remember over a longer period of time.

Furthermore, this thesis only statistically evaluated the usability of Emojis, but does not test whether the findings also apply in practice. Consequently, it might be interesting to investigate how resistant Emoji is to automated guessing attacks such as brute-force or dictionary attacks.

Further research should also be focused on tolerance area of the images. The use of big images or tolerance reduction is a simple way to extend password space. Again, in future work, a comprehensive guideline for the development and verification of images and emojis, including a long-term assessment of these practices, should be included. The security of system must also be examined closely and how attackers can take advantage of the emergence of hotspots.

APPENDIX

Figure 1: new user registration and existing user login

Figure 2: new user registrations

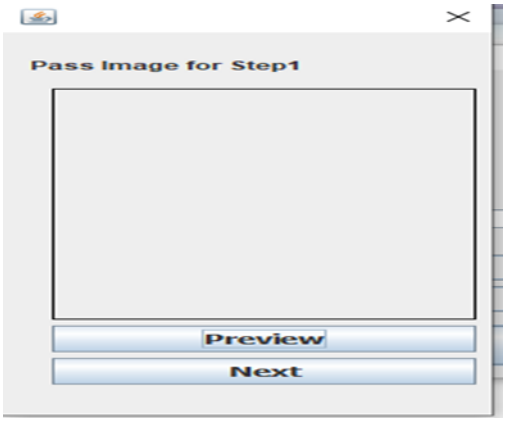

Figure 3: pass image selection module

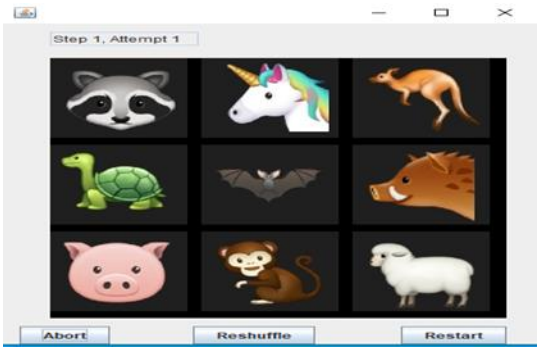

Figure 4: image selection

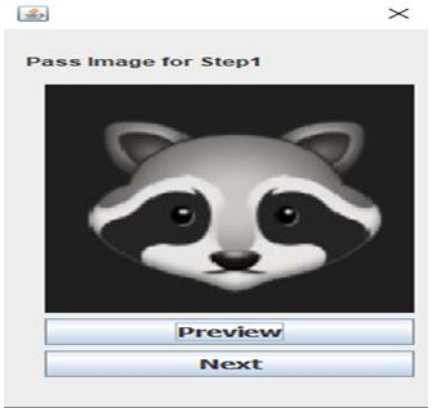

Figure 5: password setup

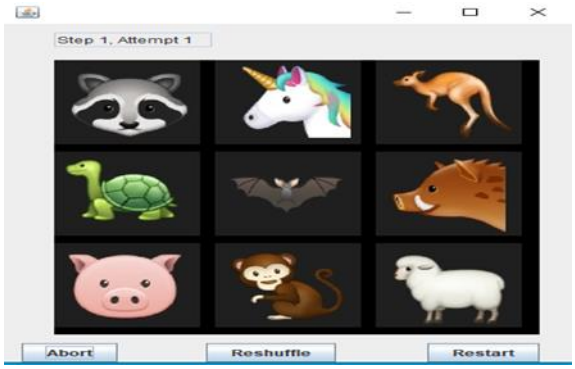

Figure 6: image grid to be selected

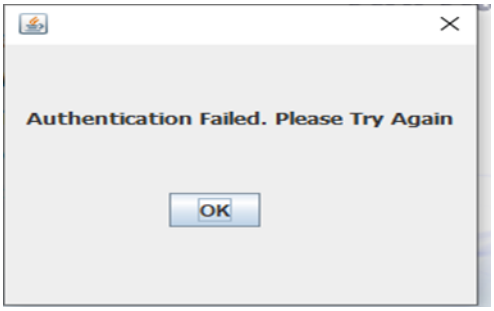

Figure 7: user authentication failed if the emoji selected did not match

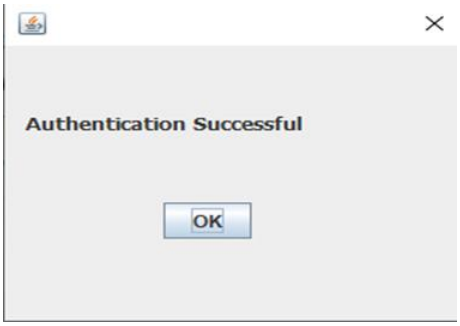

Figure 8: user authentications successful if the emoji selected match

REFERENCES

[1] M. A. F.Al-husainy, , & R. A Malih,.- Using Emoji Pictures To Strengthen the Immunity of Passwords Against Attackers. *European Scientific Journal*, *11*(30), pp 153–165 2015

[2] H.Alshenqeeti, - Are Emojis Creating a New or Old Visual Language for New Generations? A Socio-semiotic Study. *Advances in Language and Literary Studies*, *7*(6). https://doi.org/10.7575/aiac.alls.v.7n.6p.56 2016.

[3] Q.Bai, Q. Dan, , Z.,Mu, & M. A. Yang,- Systematic Review of Emoji: Current Research and Future Perspectives. *Frontiers in Psychology*, *10* October. https://doi.org/10.3389/fpsyg.2019.02221. 2019.

[4] N. L. Bliss-Carroll, - *The nature, function, and value of emojis as contemporary tools of digital interpersonal communication*. pp 1–76. https://digitalcommons.gardner-webb.edu/english_etd. 2016.

[5] Cambridge Dictionary. *emoji*. https://dictionary.cambridge.org/dictionary/ nglish/emoji. Last accessed: 24.04.2018. 2018.

[6] M.Davis, & P.Edberg, - Unicode Emoji. *Unicode Technical Standard 51*.Tech. rep. Technical Standard 51 (5). 2017.

[7] P.Fakulta, *Západočeská univerzita v Plzni Fakulta filozofická Analysis of the usage emoji in Internet communication on WhatsApp Západočeská univerzita v Plzni Fakulta filozofická Bakalářská práce Analysis of usage emoji in Internet communication on WhatsApp Aneta Ma*. University of West Bohemia. 2022.

[8] W.,Hussien, M. Al-Ayyoub, , Y.,Tashtoush, & M Al-Kabi,.- *On the Use of Emojis to Train Emotion Classifiers*. http://arxiv.org/abs/1902.08906. 2019.

[9] M.,Kjellevand, & M.. Rauhut,- *Evaluating the Security and Usability of Emoji-Based Authentication*. *June*. 2018

[10] L.,Kraus, R.,Schmidt, M.,Walch, F.,Schaub, & S.Möller,- On the use of Emojis in mobile authentication. *IFIP Advances in Information and Communication Technology*, *502*, pp 265–280. https://doi.org/10.1007/978-3-319-58469-0_18. 2017

[11] P.,Nandi, & D. P. Savant,. - Graphical Password Authentication System. *International Journal for Research in Applied Science and Engineering Technology*, *10*(4), pp 1759–1765. https://doi.org/10.22214/ijraset.2022.41621. 2022

[12] T.,Seitz, F.,Mathis, & H. Hussmann, - The bird is the word: A usability evaluation of emojis inside text passwords. *ACM International Conference Proceeding Series*, pp 10–20. https://doi.org/10.1145/3152771.3152773. 2017.

[13] Unicode Consortium. - Submitting Emoji Proposals: Evidence of Frequency. http://unicode.org/emoji/selection.html#frequency-evidence. Last accessed: 27.05. 2018.

[14] N S.Zabidi, , N. M.Norowi, , & R. W Rahmat,. - On the use of image and emojis in graphical password application. *International Journal of Innovative Technology and Exploring Engineering*, *8*(8), pp 379–385. 2019.