Associating User's Preference and Satisfaction into Quality of Experience: A Shoulder-surfing Resistant Authentication Scheme by Visual Perception

Juliana Mohamed[1], Muhamad Hanif Jofri[5]
Department of Information Technology
Center for Diploma Studies (CeDS)
Universiti Tun Hussein Onn Malaysia (UTHM)
Johor, Malaysia[1, 5]

Mohd Farhan Md Fudzee[2], Sofia Najwa Ramli[3], Mohd Norasri Ismail[4]
Faculty of Computer Science and Information Technology (FSKTM), Universiti Tun Hussein Onn Malaysia (UTHM),
Johor, Malaysia[2, 3, 4]

***Abstract*—Authentication acts as a secured method of usability concepts to certain transactions, especially for online banking transaction. Existing method is lacking in terms of usability, thus, making the goal of usability for authentication activities unsuccessful. A study has discovered some key concepts of usability in terms of Human Computer Interaction (HCI) by comparing two existing models of two different factors: environmental factors and display factors. An algorithm shows the authentication step during the online transaction activity. This paper is to prove that shoulder-surfing resistant authentication scheme that uses visual colour-blind mode-based model meets all the requirements of usability, hence, achieved the goal of usability of authentication. This study will bring forward an algorithm that examined the stated authentication scheme with the two factors, i.e environmental and display, during the authentication activity.**

***Keywords*—Authentication; usability; algorithm; model**

I. Introduction

Online banking application deals with varied issues of authentication, confidentiality, integrity and non-repudiation [1]. A secured application is highly dependent on the procedures of authentication to the online banking transaction. Authentication has been widely studied for its security and trustworthiness [1][2]. A success authentication method makes users satisfy with the services.

There are several methods of authentications that can be studied from [3][4]. These methods are highly related with users' experience and interface [5][6]. Authentication method is applied to most of authentication procedures during login process to any page or application, as well as in online transaction [7][8][9]. However, most of the studies are limited to usability towards users' experience and satisfaction [10][11]. This motivates us to investigate deeply to the authentication purposes and processes.

The objectives of this research are to: 1) identify shoulder surfing attack by utilizing users' visual perception model to the authentication; 2) propose a shoulder-surfing Resistant Authentication Scheme using Visual perception colour blind mode-based model and algorithm by taking into account users' quality of experience (QoE); and 3) analyze the proposed authentication scheme against usability, accessibility performance and shoulder surfing attack to the human computer interaction (HCI). Hence, the research is significant to the authentication step during the online transaction activity due to the shoulder-surfing attack.

This study will examine the usability in terms of human computer interaction (HCI) which is based on human preference and human satisfaction of quality of experience (QoE) [12][13]. This paper will be comparing the two existing authentication model that are based on environmental and display factors, and find the possible limitation of a compatible model of graphical-based authentication to the authentication activities.

II. Literature Review

There are two types of element that can give some impact readability: environmental factors and display factors [14] [15]. Regarding the surrounding environment, the users' reading experience is directly affected by ambient brightness, viewing angle, and distance. From here, the size of the visual image of an item created in the viewers' eyes is influenced by viewing distance. The users' eyesight has a strong correlation with ambient brightness. According to geometrical optics, the viewers' perception of brightness is determined by the viewing angle and distance [16]. In addition, display parameters such as resolution and colour scheme, as well as screen brightness are also among important influencing factors [17].

A. Hybrid Keypad

Human factor is the most crucial part while handling any online activities. Human preference and satisfaction have been widely discussed from the view of usability to the authentication. The existed model of authentication is called the Hybrid keypad [18][19]. The model creates coloured-hybrid-image keypads using superimposition. The keypad is developed automatically by appearing to the screen when user requests the one-time password (OTP). Fig. 1 depicts the existing model.

Fig. 1. The Existing Model of Hybrid Keypad.

Fig. 1 shows the illustration of Hybrid keypad. From the perspective of display factors, this model confuses the actual users when they keyed in their OT, due to two or more numbers that are overlapped on the keypad. However, the limitation of this model caused by environment factors is still uncertain, as to whether adding color-complementary components can further diminish the attacker's appearance and counteract the low frequency.

B. HideScreen

A researcher has developed HideScreen, utilizing human vision and optical system features, where users' on-screen information may be hidden from shoulder surfers [20]. That is, when the on-screen information (OSI) was viewed from outside of the specified range, HideScreen discretized the OSI into grid patterns in order to neutralize the low-frequency components, thus allowing the OSI to "blend into" the background. Fig. 2 shows the process of the grid patterns model.

The existing model, however, only allows spatial frequency by focusing on the protection of short texts and complex pictures on the screen, which is shown on soft keypad or keyboard. This limitation focuses solely on display factors. On the other hand, from the perspective of environmental factors, there have been various graphical schemes that are resistant or immune to shoulder-surfing but they have substantial usability problems, where most notably are in terms of time and effort required to log in. This paper will be discussing on the said problems. The comparison of the two factors is depicted in the Table I.

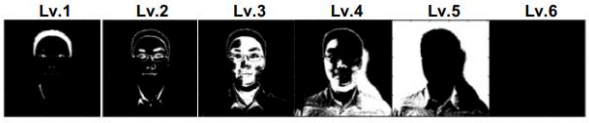


Fig. 2. The Existing Model of Grid Patterns.

TABLE I. COMPARISONS BETWEEN TWO FACTORS

Model	Environment factor	Display factor
Hybrid keypad	Adding colour-complementary components which can further diminish the attacker's appearance, and counteract the low frequency	Confusing to user due to overlapping numbers on the keypad
HideScreen	Substantial usability problems, most notably time and effort required to log in	Allows spatial frequency by focusing on the protection of short texts and complex pictures on the screen shown on soft keypad or keyboard
Shoulder-surfing resistant authentication scheme using visual colour-blind mode-based	Auto glare/auto hide which cannot be seen by shoulder surfer see from their angle	Using four colour-blind charts with eight-numbers combination

III. PROPOSED MODEL AND ALGORITHM

Due to the problems counter from the authentication type, a proposed model has been created to encounter the authentication problem. Shoulder-surfing resistant authentication scheme that uses visual colour-blind mode-based model was proposed to address the problem of shoulder surfing attack, in order to identify any suitable authentication approach, as well as to simulate and analyse the proposed mechanism in terms of usability of HCI. The proposed model was accessible from the smartphone screen with no hybrid keypad provided to the user.

A. Shoulder-surfing Resistant Authentication Scheme using Visual Colour-blind Mode-based Model

The model represents a set of four randomly colour-blind pictures in every session. Each picture contained two-digits number that was as similar as a TAC. Uniquely, the model enabled HideScreen or glare to the process by utilising the complex pixels of complementary Red, Green, Blue (RGB) colours of each picture whenever shoulder surfer sees to the actual user [21][22]. Users can access the proposed model from their smartphone screen. Fig. 3 illustrates the proposed authentication model.

During the transaction, users will request the one-time password (OTP) to the server. Server will react by randomly selecting four charts of colour-blind, with the combination of two number in each chart. Two matching colors were used for each chart to maintain the view of user perception. Next, the server will send the requested OTP to the users. Here, the OTP pictures will enable the auto glare or hide. The users must keyed in the OTP within 60 seconds since it will be automatically nullified after the period of time. The server will compare the keyed-in OTP with the one been sent. If the OTP is a matched, the authentication will be considered as successful, but if it is not, the users were to repeat the procedure. In addition, the proposed model can be used to all types of users including the one with colour vision deficiency.

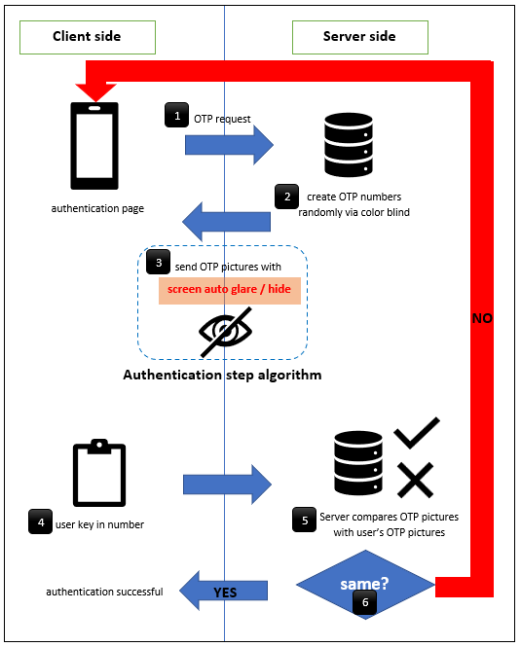


Fig. 3. Shoulder-surfing Resistant Authentication Scheme using Visual Colour-blind Mode-based Model.

B. *Shoulder-surfing Resistant Authentication Scheme using Visual Colour-blind Mode-based Algorithm*

The algorithm represents the focus area of authentication step during the activity. From Fig. 4, the method started with the number of incoming requests, then sorted out based on their priority and order. Later, the server will load and announce QoE offer upon initiation. This method assumed that the provider's system that handled the incoming requests has access to this data. The number of requests that can be fulfilled within the advertised waiting time can be estimated based on the current server load. Fig. 4 depicted to the authentication step of algorithm.

Algorithm 1: Authentication Step

INPUT: B, $\overline{U}$, s, E
OUTPUT: Settlement of (S_i)
BEGIN
1: $B \leftarrow t_i \in \overline{U}$
2: **FOR** t **DO**
3: $B \leftarrow \overline{U}$, s read colour-blind chart
4: Estimate B can be served within the E
5: **FOR** each B **DO**
6: **IF** B can be served within the E **THEN**
7: Authentication successful (B, S_i)
8: **ELSE**
9: Perform **'auto glare/auto hide'**
10: **IF** request within actual E **THEN**
11: Authentication successful (B, S_i)
12: **ELSE**
13: Request E from s
Authentication successful (B, S_i)
accepted by s
14: **END IF**
15: **END IF**
16: **END FOR**
END FOR
END

Fig. 4. Authentication Steps' Algorithm.

The programme will, then, extract the requests, their priorities, and the prospective providers server loads for each job, which was declared as the parameter to the algorithm. The authentication stage will further determine the total requests that can be fulfilled within the advertised E. Line 5 will, lastly, carry out the requests. As a result, the request for these duties will be completed. If this is not the case, the authentication step will request E from the provider in line 9 and conducted the "auto glare" or "auto hide" function. Table II depicted to the abbreviation from Algorithm 1.

TABLE II. LIST OF COMMONLY USED NOTATION

Notation	Description
B	Request
$\overline{U}$	OTP priority
E	Estimate time
s	Server load
T	Task
t_i	Number of tasks
S_i	Authentication settlement

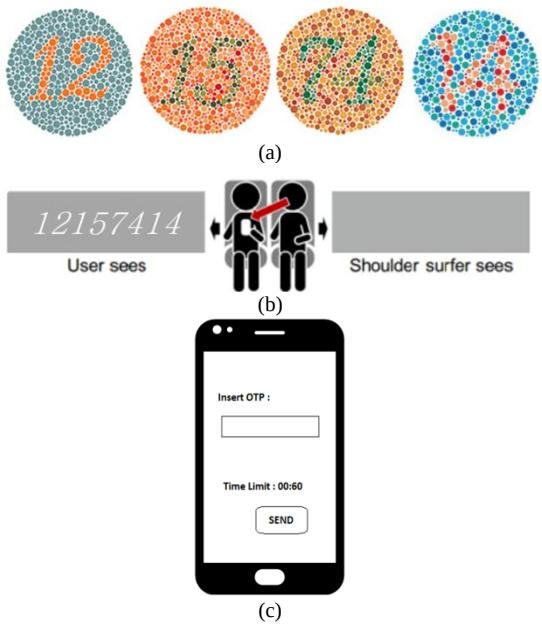
IV. EXPERIMENTAL SETUP

The study continued with simulation setup by using an application namely 'i-Smart Bank apps' which was developed using Android Studio and the database was supported by Firebase. This experiment was to show the authentication step during online transaction activities.

During the experiment, the users' reading experience was directly impacted by the ambient brightness, viewing angle, and distance. From here, the visual image of an item created in the viewers' eye was influenced by viewing distance. The users' eyesight has a strong correlation with ambient brightness. According to geometrical optics, the viewers' eyes perception of brightness is determined by the viewing angle and distance. Moreover, display parameters, such as resolution and colour scheme and screen brightness, are among important influencing factors.

Fig. 5(a), (b) and (c) illustrate steps involved during the authentication activities when users keyed in the one-time password. During the activity, the users will receive randomly chosen colour-blind chart with numbers to be keyed in. This activity will enable auto glare or auto hide which disallow shoulder-surfer to see what is happening to users' smartphone. Here, viewing angle and distance played an important role in determining whether the authentication will be succeeded or not. In addition, resolution and screen brightness also gave some influence to this activity.

Table III shows the measurement setup for this experiment. The relationship between luminance contrast and screen brightness will be discovered further in the study. These variables were chosen in order to test the algorithm for authentication procedures. The measurement setup testing was used to compare the algorithm step. This setup started with 10% to 100% for QoE of users' satisfaction.



(a)

(b)

(c)

Fig. 5. Simulation Setup, (a) Example of Server Database (b) Example of Shoulder Surfing and the Effect after Applying Hide Screen or Glare (c) Example of a User Interface.

TABLE III. MEASUREMENT SETUP

Display brightness	Contrast luminance
10	0.1
20	0.2
40	0.4
60	0.6
80	0.8
100	1.0

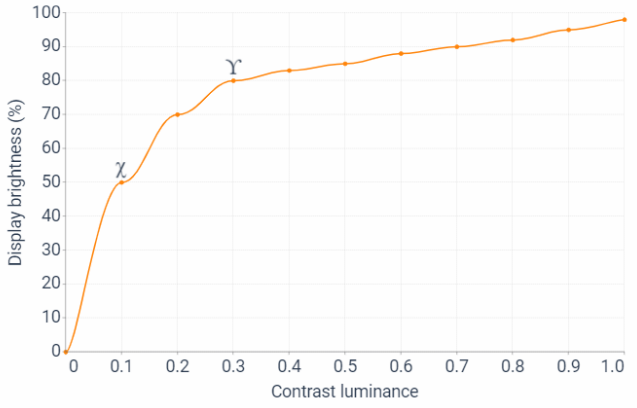


Fig. 6. Influence Trend to Human Vision (Display Brightness to Contrast Luminance).

Fig. 6 shows the contrast influence trend to human vision. From here, users' reading experience was found to be better when the contrast value is ϒ, with an improvement of 80%; but, when the contrast value is χ, the reading experience was extremely bad, with an improvement of just 50%, substantially impairing reading.

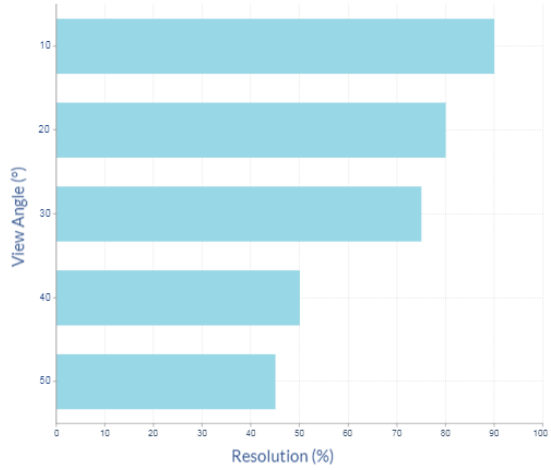


Fig. 7. Some Effect of Viewing Angle to Resolution.

Fig. 7 shows some effect of viewing angle to resolution. Users used i-Smart Bank apps at 10°, 20°, 30°, 40° and 50°, respectively while keeping the viewing distance of 20 cm, ambient brightness, and screen display content remained the same in order to verify the influence of viewing angle on the reading experience. As the viewing angle expanded, the users' relative visual performance fluctuated.

V. RESULTS AND DISCUSSIONS

The proposed model reviewed the experimental result of viewing angle by the shoulder-surfer and the authority users. This study also compares the limitation of existing models based on two factors: environmental factors and display factors. The environmental factor will be investigated based on view angle, meanwhile the display factor will be examined based on resolution of smartphone. The result is shown in the following table.

Table IV shows the test started at 0º of view angle. This experiment continued with another three different types of view angle. Users, as shown in Table II, were asked to hold their smartphone in different view angles. Another shoulder-surfer volunteer were standing at the same distance but with different view angle. This experiment started with some contents were displayed and the shoulder-surfer were asked to read it before the actual users. The test and its results were recorded.

From Fig. 8, the resolution of shoulder-surfer was increased up to 90% at a distance of 20 cm, proving that the experiment had no appreciable effects on users or the regular use. In comparison, the resolution values from shoulder-surfer at 20 cm to 40 cm were barely above the boundary but less than 60%. However, the resolution clearly decreased below the boundary at distances greater than 60 cm. Nevertheless, shoulder-surfers seldom position themselves at an angle less than 40 degrees when standing 20 cm to 40 cm from the screen. In actuality, a shoulder surfers' viewing angle is always wide when the distance between them is modest. As a result, when resolution values from shoulder-surfer dropped as viewing distance increased, their overall reading experiences are still excellent and much exceed the minimal resolution barrier at 50% in the case of real applications.

TABLE IV. EXPERIMENTAL SETUP ENVIRONMENT

View Angle (°)	Distance (cm)	Ambient Brightness
0	20	150
20	40	300
40	60	500
60	80	800

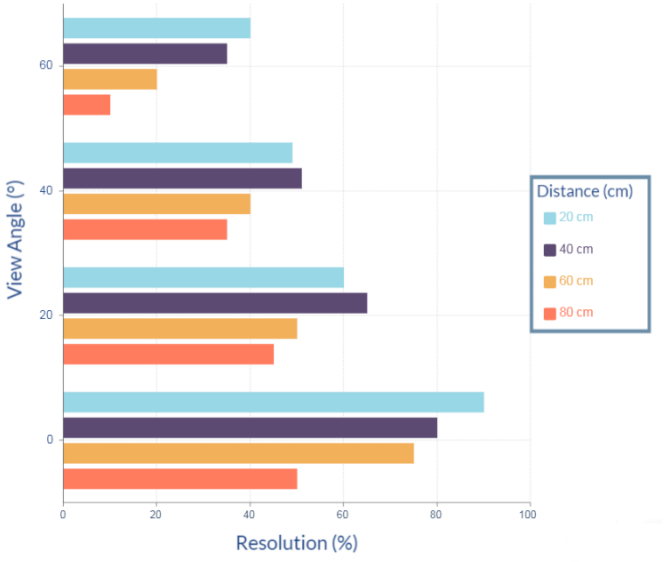


Fig. 8. Experimental Result from Resolution vs. View Angle.

The resolution values from shoulder-surfers at four viewing positions: (20 cm, 40°), (40 cm, 40°), (60 cm, 20°) and (80 cm, 20°) were close to 50% minimum boundary, while the resolution values located outside the four points area were significantly less than 50%. This suggests that a privacy space might be constructed, i.e when actual users are in a secure environment, reading is going well and the resolution value is higher than the required minimum of 50%. The shoulder-surfer will have a terrible reading experience, or may not even be able to read when they were outside of the safety zone. Furthermore, it should be emphasised that this security zone is not a permanent location. A safe zone is established provided that the farthest viewing distance for the user is 50 cm. Depending on the actual users' reading distance, which ranges from 20 cm to 80 cm, the safe zone narrows as the reading distance between the user and the screen decreases. In conclusion, the authentication procedure works well with the proposed model, and meets all requirements based on the key concepts of usability, thus, archive the users' preference and satisfaction to QoE.

VI. CONCLUSION

This study has discovered the key concepts of usability in terms of Human Computer Interaction (HCI) by comparing two existing model models with two factors: environmental factors and display factors. Shoulder-surfing resistant authentication scheme using visual colour-blind mode-based model is proven to meet all the requirements of usability, hence, achieved the goal of usability of authentication. Hopefully, in future, the study will be able to bring forward an algorithm by investigating the colour scheme, i.e the matching two complementary colours by the two factors of environmental factors and display factors during the authentication activity.

ACKNOWLEDGMENT

This research was supported by Universiti Tun Hussein Onn Malaysia (UTHM) through Tier 1 (H808).

REFERENCES

[1] Windasari, N. A., Kusumawati, N., Larasati, N., & Amelia, R. P. (2022). Digital-only banking experience: Insights from gen Y and gen Z. *Journal of Innovation & Knowledge*, *7*(2), 100170.

[2] Naem, E. A. A. (2020). *Enhance Graphical Password Authentication using One Time pad* (Doctoral dissertation, Sudan University of Science and Technology).

[3] Singh, A. K., & Gandhi, G. C. (2020). Computer Architecture: A New Weapon to Secure Web Services From Bots. *International Journal of Smart Security Technologies (IJSST)*, *7*(1), 41-48.

[4] Hamdy, M. (2021). A Comparative Study on Authentication Strategies of Various Online Banking Platforms.

[5] Zhou, L., Wang, K., Lai, J., & Zhang, D. (2021, November). Behaviors of Unwarranted Password Identification via Shoulder-Surfing during Mobile Authentication. In *2021 IEEE International Conference on Intelligence and Security Informatics (ISI)* (pp. 1-3). IEEE.

[6] Kakadia, D., & Ramirez-Marquez, J. E. (2020). Quantitative approaches for optimization of user experience based on network resilience for wireless service provider networks. Reliability Engineering & System Safety, 193, 106606.

[7] Kaushik, M., Rawat, A., Sisaudia, V., & Parashar, L. (2022, June). A Novel Graphical Password Scheme to Avoid Shoulder-Surfing Attacks in Android Devices. In *2022 2nd International Conference on Intelligent Technologies (CONIT)* (pp. 1-6). IEEE.

[8] Zhou, L., Wang, K., Lai, J., & Zhang, D. (2021, November). Behaviors of Unwarranted Password Identification via Shoulder-Surfing during Mobile Authentication. In *2021 IEEE International Conference on Intelligence and Security Informatics (ISI)* (pp. 1-3). IEEE.

[9] Bošnjak, L., & Brumen, B. (2020). Shoulder surfing experiments: A systematic literature review. Computers & Security, 99, 102023.

[10] Hassan, M. A., & Shukur, Z. (2021, January). A secure multi factor user authentication framework for electronic payment system. In *2021 3rd International Cyber Resilience Conference (CRC)* (pp. 1-6). IEEE.

[11] Bai, W., Pearson, M., Kelley, P. G., & Mazurek, M. L. (2020, September). Improving non-experts' understanding of end-to-end encryption: An exploratory study. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 210-219). IEEE.

[12] Kara, P. A., Tamboli, R. R., Shafiee, E., Martini, M. G., Simon, A., & Guindy, M. (2022). Beyond perceptual thresholds and personal preference: towards novel research questions and methodologies of quality of experience studies on light field visualization. Electronics, 11(6), 953.

[13] Fatima, K., Bawany, N. Z., & Bukhari, M. (2020, October). Usability and accessibility evaluation of banking websites. In *2020 International Conference on Advanced Computer Science and Information Systems (ICACSIS)* (pp. 247-256). IEEE.

[14] Sukaris, S., Renedi, W., Rizqi, M. A., & Pristyadi, B. (2021, February). Usage behavior on digital wallet: perspective of the theory of unification of acceptance and use of technology models. In *Journal of Physics: Conference Series* (Vol. 1764, No. 1, p. 012071). IOP Publishing.

[15] Bâce, Mihai, Alia Saad, Mohamed Khamis, Stefan Schneegass, and Andreas Bulling. "PrivacyScout: Assessing Vulnerability to Shoulder Surfing on Mobile Devices." Proceedings on Privacy Enhancing Technologies 1 (2022): 21.

[16] Chandrakanth, P., Chavan, S., Verghese, S., Gosalia, H., Raman, G. V., Shettigar, C. K., & Narendran, V. (2022). Smartphone Gonioscopy With a Magnifying Intraocular Lens: A Cost-effective Angle Imaging Device. *Journal of Glaucoma*, *31*(5), 356-360.

[17] Elliott, M. A., Nothelfer, C., Xiong, C., & Szafir, D. A. (2020). A design space of vision science methods for visualization research. *IEEE Transactions on Visualization and Computer Graphics*, *27*(2), 1117-1127.

[18] Anthonio, H., & Kam, Y. H. S. (2020, December). A Shoulder-Surfing Resistant Colour Image-based Authentication Method Using Human Vision Perception with Spatial Frequency. In 2020 15th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 1-5). IEEE.

[19] Binbeshr, F., Kiah, M. M., Por, L. Y., & Zaidan, A. A. (2021). A systematic review of PIN-entry methods resistant to shoulder-surfing attacks. *computers & security*, *101*, 102116.

[20] Hodes, L. N., & Thomas, K. G. (2021). Smartphone screen time: inaccuracy of self-reports and influence of psychological and contextual factors. *Computers in Human Behavior*, *115*, 106616.

[21] Guido, R. C. (2022). Wavelets behind the scenes: Practical aspects, insights, and perspectives. *Physics Reports*, *985*, 1-23.

[22] Pridmore, R. W. (2021). Complementary colors: A literature review. Color Research & Application, 46(2), 482-488.