Understanding Dark UI Patterns in the Mobile Ecosystem: A Case Study of Apps in China

Mengyi Long
Sun Yat-sen University
longmy5@mail2.sysu.edu.cn

Yue Xu
Sun Yat-sen University
xuyue73@mail2.sysu.edu.cn

Jiangrong Wu
Sun Yat-sen University
wujr28@mail2.sysu.edu.cn

Qihua Ou
Sun Yat-sen University
ouqh@mail2.sysu.edu.cn

Yuhong Nan*
Sun Yat-sen University
nanyh@mail.sysu.edu.cn

ABSTRACT

Dark User Interface (DUI) refers to deceptive UI that lets users do something they do not intend to do, such as clicking and opening an advertisement. Previous research has shown that DUI in mobile apps is becoming an increasing concern for app users. Meanwhile, due to the lack of a dominant app store such as Google Play, mobile apps in China are more difficult to regulate. As a result, user-harmful behaviors such as DUI are more likely to happen. In this paper, we systematically investigate the prevalence, distribution, and the impact of dark UI patterns (as DUI patterns for short) in the mobile ecosystem China. To this end, we first summarize a taxonomy of DUI patterns based on the UI layout, UI element, and user interactions in mobile apps. With this taxonomy, we implement a lightweight pipeline to identify various DUIs from a set of top 150 popular apps. The results of the analysis show that DUIs exist widely in modern applications, with different categories and contexts. Additionally, we extend our analysis to examine DUIs in mini-apps - an emerging type of mobile apps that is with great popularity in China. Our research highlights a number of stealthy dark UI patterns that may bring confusion, or even harmful impacts to app users. Additionally, we show that better regulation and user awareness of DUI in mobile applications are urgently needed.

CCS CONCEPTS

• **Security and privacy → Software and application security**; **Usability in security and privacy**.

KEYWORDS

mobile security, usable security, dark UI pattern, mobile advertisement

ACM Reference Format:
Mengyi Long, Yue Xu, Jiangrong Wu, Qihua Ou, and Yuhong Nan. 2023. Understanding Dark UI Patterns in the Mobile Ecosystem: A Case Study of Apps in China. In *Proceedings of the 2023 ACM Workshop on Secure and Trustworthy Superapps (SaTS '23), November 26, 2023, Copenhagen, Denmark.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3605762.3624431

*Corresponding author: Yuhong Nan

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
SaTS '23, November 26, 2023, Copenhagen, Denmark
© 2023 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 979-8-4007-0258-7/23/11…$15.00
https://doi.org/10.1145/3605762.3624431

1 INTRODUCTION

User interface (UI) plays a critical role on the digital lives of modern society, as it is the basic interaction channel between human and computer systems. For mobile apps, ensuring the design of unambiguous UIs is with great importance to app usability, quality, and even security. However, previous research [26, 7, 20] has revealed that a growing number of app designers intentionally utilize deceptive UI design elements to influence users' behavior contrary to their intentions, such as persuading users to make unnecessary purchases or granting unwarranted permissions. This type of UI is commonly referred to as Dark UI (DUI).

(a) An example of fake button which triggers user unwanted behaviors.

(b) Disguised Advertisement whose layout is similar to normal in-app content.

Figure 1: Typical examples of Dark UI (DUI) in mobile apps.

While being harmful to app users, DUIs can facilitate product promotions or increase ad revenues [22] for app developers and advertisers. Figure 1(a) illustrates a typical example of DUI, where advertisers design fake buttons that visually resemble regular buttons without real functionalities. Users may inadvertently click on these misleading buttons in an attempt to leave the current interface, which actually triggers the advertisement. Besides, for some apps (particularly free apps) that rely on advertising as income, the developers themselves may actively design deceptive DUIs to trick users into clicking fake buttons, as seen in Figure 1(b). Since users are more likely to click on normal content and ignore the advertisement, the app developer disguised the advertisement as

normal content, making it challenging for users to differentiate between the two.

In terms of detecting, or defense against DUIs, prior research mostly focused on DUIs in traditional platforms such as PC and Web browser. For example, Harry Brignull [1] proposed new types of DUIs, such as adding extra products to the shopping card and can only be canceled under restricted scenarios. Furthermore, prior research [28, 24] analyzed numerous web pages to determine the prevalence and underlying intentions of DUI. Due to differences in the UI design between PC and mobile platforms, the DUI patterns in mobile apps could be significantly different. In terms of user altitudes to DUIs, prior research [3] has underscored the serious impact of this issue on users' daily experiences. There is a growing demand for effective solutions to regulate DUIs in the mobile ecosystem to meet users' expectations.

Our work. In our study, we conducted the first systematic study on the dark UI patterns in the Chinese mobile apps. Owing to China's distinct mobile ecosystem (e.g., Google-Play not available), DUI exhibits unique patterns in terms of prevalence and diversity in Chinese Apps. Most prior related studies focused on apps and DUIs in English, their findings and conclusions might not fit the case of Chinese apps. To this end, our research conduct an exploratory study to assess the prevalence and implications of DUI patterns within popular Chinese mobile apps. We first summarize a taxonomy of DUIs for mobile apps by classifying the DUIs based on various metrics, such as the UI layout, UI element placement, and user interactions. The instances of summarized patterns include *Fake Button*, *Misleading Text*, *Missing Exit*, etc (See Section 3 for more details). Furthermore, we design a semi-automatic pipeline to identifying various DUIs in mobile apps. The pipeline utilizes various detection mechanisms such as computer-vision, textual semantics to facilitate locating DUIs from a large number of screenshots. With the help of this pipeline, we performed an analysis over the top-150 popular Chinese apps to investigate the prevalence of DUIs.

Our research uncovered several interesting findings about DUIs in the Chinese mobile ecosystem. For example, 82% of the apps in our dataset have at least one DUI. The total number of DUI instances in these apps reaches 819. Besides, our research showed a positive correlation between the number of DUIs and the app's popularity. In other words, top popular apps, which are supposed to be trustworthy, contain more DUIs in practice. In addition to typical mobile apps, we also extend our research by looking at DUIs in mobile mini apps [15], which are hosted in super apps like WeChat. Our research aims to provide a better understanding of the implications of these deceptive design practices, not only for researchers but also for industry stakeholders and the wider user community.

In summary, this paper makes the following contributions:

- We propose a new taxonomy of DUI patterns in mobile apps, covering 11 different types.
- We design and implement a lightweight pipeline to facilitate DUI identification in mobile apps.
- We perform an extensive analysis of DUI patterns on 150 popular apps in China.

2 BACKGROUND

DUI. Dark user interface (DUI) refers to a deceptive design strategy employed by developers to manipulate user behavior and actions [29]. DUI exploits psychological vulnerabilities and cognitive biases [2], leading users to inadvertently click on ads, subscribe to services, or perform other actions they did not intend to take. A prominent feature of DUI in mobile ecosystems is that regardless of intentional manipulations by developers, there is no negative impact on normal business processes if users choose not to engage with the prompted behavior.

DUIs in mobile apps. Compared to those deceptive UI patterns in desktop environments (e.g., PC browsers), the main goal of DUI in the mobile ecosystem is to foster user engagement [19]. Developers strive to attract user attention and encourage users to actively participate in various app events [27], such as downloading updates, participating in activities, and granting permissions. Still, these events are not mandatory for users' regular app usage. For instance, when the user makes a purchase, developers may incorporate multiple notification options, seemingly asking the user to grant notification permission to stay informed about the order status. Ordinary users may assume that selecting at least one notification option is necessary, unaware that it does not impact their order. Moreover, if developers gain notification permission, they can continue to promote their products and send information to users.

By implementing DUI patterns, app developers can increase app usage frequency and gain greater access to users' information [18]. However, from the users' perspective, most of them cannot identify DUI patterns [33]. This approach disregards their primary intentions, disrupts normal use, and can even harm their interests [17, 9]. As a vast majority of people today extensively use mobile devices and may be more easily influenced [7], finding an effective solution to enhance accessibility and counteract such DUI patterns in mobile applications becomes urgent and crucial.

Related Policies and Regulations. Due to the negative impact of DUI on end-users' normal usage, the reputation of mobile applications, and even the overall mobile ecosystem, institutions and governments worldwide are investing considerable efforts in regulating DUI through legal and policy measures. In 2016, the European Parliament passed the General Data Protection Regulation (GDPR) [10], which forces the pre-ticket boxes should not be interpreted as a user choice or implied consent. Consent requests must be distinguishable from other user interface design elements. Regulators in China also published a series of policies aimed at banning DUI patterns [32, 11], such as malfunctioned buttons for closing and exiting apps, automatic download and install apps without user consent, as well as misleading content which deceive users into clicking on. Unfortunately, there is a gap between the app implementation and legislation enforcement, as regulators lack an effective to identify DUI patterns [31] promptly. At the same time, the patterns of DUI covered by relevant policies fall far short of the new DUIs devised by developers. The disorganized and ever-changing application

(a) Disguised Layout (b) Overlapped Placement (c) Asymmetric Button (d) Misleading Text (e) Induced Icon (f) Missing Exit (g) Fake Button (h) Easy Trigger

Figure 2: Typical examples of DUI patterns related to UI layout and element

ecosystem contributes to the amorphous nature of the DUI pattern issue, posing challenges for policymakers in addressing this complex problem [25]. As a result, existing regulations and enforcement mechanisms are still insufficient to stop the proliferation of DUI in the mobile ecosystem.

3 A TAXONOMY OF MOBILE DARK UI PATTERN

In this section, we present a taxonomy to categorize and organize dark UI patterns in mobile apps. As shown in Figure 3, we classify DUIs in mobile apps into three sub-categories, namely, Dark UI Layout, Dark UI Element, and Dark User Interaction.

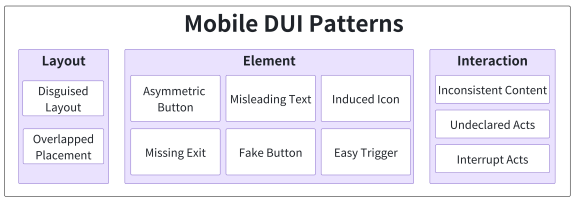


Figure 3: A Taxonomy of Mobile Dark UI Patterns

3.1 Dark UI Layout

The layout of UI plays a crucial role in determining how users perceive and interact with apps [6]. App developers grasp the importance of a meticulously designed layout and thus optimize the placement of DUI elements to confuse and entice users.

Disguised Layout. App developers adopt a layout for DUI elements that closely resembles the design of regular content. This design blurs the distinction between actual content and advertisement, making the elements appear as ordinary content rather than obvious advertisements. As an example shown in Figure 2(a), the advertisement portion marked in red closely resembles the normal content section marked in green. It may be challenging for users to distinguish between the two. So users may be more likely to click on the advertisement.

Overlapped Placement. App developers strategically place elements in user interest during typical app interactions. Unfortunately, these elements may not align with users' preferences or intentions, but users cannot avoid or ignore them. Figure 2(b) illustrates a typical example, where the red packet icon is placed right above the normal interactive elements, making it easily visible to the user. Even worse, when users attempt to click on the normal elements, it is very likely that they will accidentally touch the red packet icon.

3.2 Dark UI Elements

To effectively influence users' behavior, app developers invest considerable effort in the design of the elements of DUI, ensuring they are attention-grabbing and persuasive.

Asymmetric Button. Developers manipulate button size and color attributes to make user-beneficial buttons less noticeable while enhancing visibility and prominence for buttons aligned with their intentions. For example, the exit button in Figure 2(c) (i.e., content within the red rectangle) is challenging for users to notice due to its small size and low contrast to the background. On the contrary, the approval button (marked within the green rectangle) is prominently displayed with a large size and a bright color, ensuring it can be noticed immediately. Therefore, users' attention may quickly drawn to the approval button, rather than the exit button.

Misleading Text. App developers may utilize a series of misleading text to influence users' behavior [14]. For example, they may use emotive words like "cruel to leave" (shown in Figure 2(d)) to induce guilt in users and persuade them to cancel their original intentions. Additionally, developers may utilize exaggerated or ambiguous statements to create a false sense of obligation, such as the statement, "apply for a credit card just needs three minutes and will enjoy benefits" (shown in Figure 2(d)). These texts make users erroneously believe that the behavior is easy and is necessary for normal usage, so they will be more willing to participate.

Induced Icon. App developers add additional icons, such as gestures, to let users think that they should follow the provided guides and interact with the designated icons accordingly. However, these icons are extra and lack practical significance to induce users into specific behaviors. As shown in Figure 2(e), the gesture button (marked within a green rectangle) directs users to click and participate in a promotion campaign.

Missing Exit. App developers do not design a close or exit button in the UI. Even though users can exit the interface by clicking the

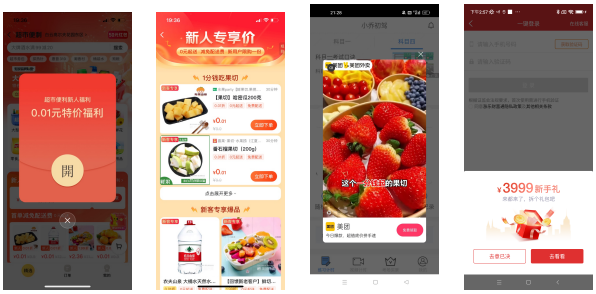
back button or a blank space, they are still susceptible to inadvertently clicking on the highlighted button instead.

Fake Button. Unlike the aforementioned *Disguised Layout*, which mimics normal content while retaining actual functionality, fake buttons lack genuine functionality and they are merely graphical elements. Since users cannot distinguish them from genuine buttons, they often unwittingly click on these deceptive buttons, boosting advertising click-through rates or following the designers' intentions. For example, the advertisement includes the close and confirm buttons (marked within red rectangles in Figure 2(g)). Clicking on these buttons results in users inadvertently clicking on the advertisement itself.

Easy Trigger. App developers design easy-to-touch trigger methods to increase user engagement, such as shaking the phone to view details. However, these judgment criteria are imprecise and can occur during regular usage, resulting in unintentional clicks or unintended jumps. For example, the splash screen advertisement in Figure 2(h) uses the trigger strategy of twisting the phone to jump. However, app user may unconsciously trigger this strategy during normal use if they are not stationary, leading to unintended interactions. Note that the pattern of *Easy Trigger* is unique mobile apps as it relies on specific sensor/hardware (e.g., gyroscope).

3.3 Dark User Interaction

App users may encounter DUIs which encompassing a series of UIs [8]. These DUI patterns consist of a sequence of carefully crafted UIs, each intended to guide and manipulate user behavior in specific ways.



(a) Inconsistent Content (b) Inconsistent Content (c) Undeclared acts (d) Interrupt Acts

Figure 4: Typical examples of DUI patterns categorized by user interaction

Inconsistent Content. Unlike dark UI layout and dark UI element that involve only one interface, *Inconsistent Content* includes multiple user interfaces. More specifically, in this scenario, app developer may entice users with an offer or benefit upon clicking the initial interface. However, the subsequent interface that follows the interaction fails to fulfill the promised expectations. For example, the interface in Figure 4(a) claimed that users can get bonus rewards after clicking on it. However, when users click on it, the app presents a product promotion (see Figure 4(b)).

Undeclared Acts. App developers partially conceal the subsequent actions triggered by a button click. Consequently, when users interact with the button, unannounced actions may automatically initiate, such as immediate app installation or redirection to another application, disrupting the user's intended and expected normal usage. As Figure 4(c) shows, users can not aware that they will be directed to another app after clicking the advertisement.

Interrupt Acts. Once users reach a specific UI, app developers implement successive pop-up advertisements to capture users' attention, creating an impression that the content is essential and valuable. This deliberate design may alter users' original behavior, persuading them to engage and ultimately fulfill developer's intention. Figure 4(d) provides a typical example where users intending to leave the interface, but interrupted by a pop-up advertisement. The pop-up advertisement utilizes *Misleading Text* and *Asymmetric Button*, attempting to retain users' exit.

4 DUI DETECTION

Challenges. There are two critical challenges related to detecting DUI patterns in mobile apps. Firstly, to gain a comprehensive understanding of DUI patterns in the mobile ecosystem, it is necessary to collect a large number of UI screenshots of different mobile apps. While several prior research [23] have been conducted on DUI patterns, their datasets are not specifically targeting DUI patterns in mobile apps. Secondly, even for the same DUI pattern in different apps, their technical implementations could be significantly different. Therefore, a generic approach to identifying all categories of DUIs is extremely difficult. Moreover, detecting the pattern of *Dark User Interaction* requires understanding the contextual semantic information, which is also a non-trivial task to be completed automatically.

4.1 Approach

Our research first obtains a large number of app screenshots for DUI detection. This is done by utilizing Monkey [34], an automated app exploration tool. Given the complicated patterns of DUIs, most of them require expertise knowledge for confirmation. However, we employ the following steps/techniques to facilitate this process.

CV-based Identification. We employ a CV-based machine learning model to identify part of DUIs. This is because part of the DUIs shares unique visual features that can be learned by an ML model. For example, previous research [3] employed Yolo [36], an object detection framework to identify *Asymmetric Button* - a subset of DUIs. In our research, we extend the CV-based model used in DARPA [3], by labelling and training more types of DUIs.

Text-based Identification. Several types of DUIs can be identified by matching the consistency between the textual semantics and UI elements. For example, for *Fake Button*, we inspect whether certain keywords (e.g., "open a red packet") corresponds to a valid button by analyzing the layout structure of the UI. For *Misleading Text*, we first employ OCR [5] to extract all texts from the UI screen. Then, if certain keywords (e.g., "confirm", "OK") appears on the UI, we label such screenshots as highly suspicious and perform manual inspection. In addition, we use text such as "ad" to filter out all

advertising content from normal app content. This enables us to efficiently perform manual inspection over the rest screenshots.

Manual Identification. Finally, we perform manual inspection to check and confirm all screenshots which are suspect to be DUIs. For example, we capture the last interface during the automation running process before the application jumps. Based on these interfaces, we manually identify the pattern of *Undeclared Acts*.

5 UNDERSTANDING DUIS IN THE WILD

In this section, we report our analysis of DUI patterns in the mobile ecosystem of China, such as the prevalence of DUIs and their distribution across different apps.

5.1 Dataset

We collect the top 150 downloaded apps from Wandoujia [35], one of China's most popular app stores. Figure 5 provides an overview of the distribution of app categories.

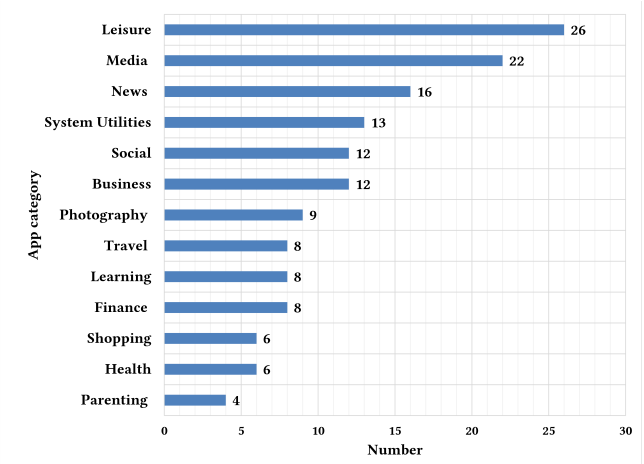


Figure 5: Distribution of apps in different categories

We utilize UI-Automator [12] to run and explore apps automatically. UI-Automator allows us to automate intelligent interactions with UI elements, facilitating access to various user interfaces and collecting valuable information such as UI screenshots and their background XML files. Through this process, we have collected a total number of 4,266 unique UI screenshots for further analysis.

Note that due to various limitations, such as app exploration coverage and UI complexity, our research can not comprehensively report all DUIs in the analyzed apps. For example, due to the extensive manual effort required for analyzing these apps, our measurement focuses on seven types of DUIs discussed in Section 3. By reviewing the captured screenshots, our research provides a lower-bound of DUIs in these apps.

5.2 Distribution of DUI patterns in popular apps

We find that 82% of the apps have at least one DUI pattern. The distribution of these patterns within popular apps we gathered is presented in Table 1. Our analysis reveals that among all the DUI patterns identified, the *Asymmetric button* pattern emerges as the most prevalent, with approximately 78% of apps having this design, demonstrating the trend of developers intentionally inducing users with *Asymmetric Buttons*. Conversely, the *Fake Button* is the least common, with only three apps having the design. The infrequency of *Fake Buttons* may be attributed to law enforcement agencies' proactive handling of *Fake Buttons*, prompting developers and advertisers to avoid their usage deliberately [30]. However, due to the lack of specific research and supervisory targeting of these patterns, simple yet effective DUI patterns like the *Undeclared Acts* and *Misleading Text* are still widely employed. Their continued usage spans various situations, making them prevalent in the mobile ecosystem.

Table 1: Distribution of DUI patterns in popular apps

DUI patterns	Interface		App	
	number	percentage	number	percentage
Disguised Layout	41	0.96%	6	4.00%
Asymmetric Button	619	14.51%	117	78.00%
Misleading Text	3	0.07%	29	19.33%
Missing Exit	18	0.42%	14	9.33%
Fake Button	44	1.03%	3	2.00%
Easy Trigger	12	0.28%	12	8.00%
Undeclared Acts	28	0.66%	23	15.33%

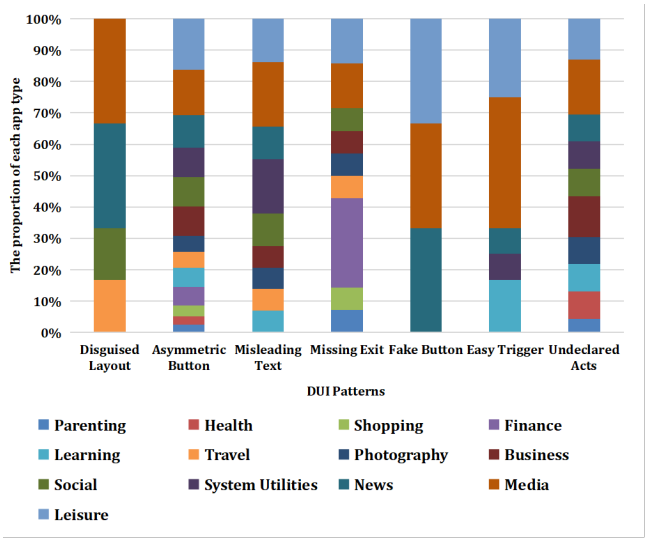


Figure 6: Distribution of app categories in each DUI pattern

Figure 6 shows the distribution of DUI patterns in different categories of apps. Notably, the Leisure and Media categories are more likely to contain DUI patterns. This could be attributed to the nature of these applications, which often aim to attract and engage users, leading to a higher probability of incorporating such patterns to maximize user interactions. An intriguing insight emerges with the *Easy Trigger* pattern, seen predominantly in Media apps, reflecting the integration of sensor-based interactions.

5.3 Distribution of DUIs in different contexts

In addition to understanding the distribution of DUIs in different apps, we are also interested in the likelihood of DUI patterns occurring within specific application contexts. To achieve this, we present a comprehensive examination of the prevalence of various DUI patterns within three interface contexts: "Splash Screen", "Home Page" and "Other". We categorize the previously acquired interfaces with DUI patterns based on this criterion.

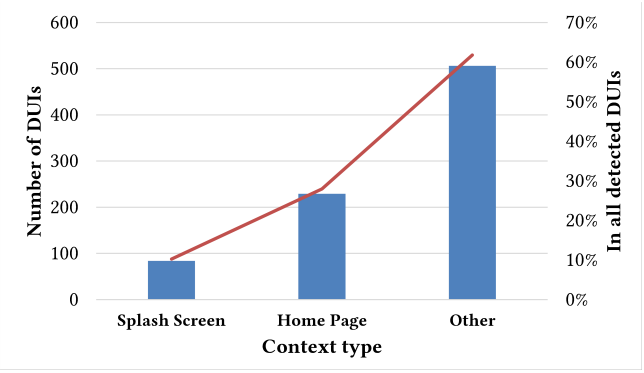


Figure 7: Locations where DUIs appear in apps

Figure 7 shows our results. Notably, because running an app once would only generate a single screenshot of a splash screen interface, the available sample data for this category remains naturally constrained. So, the 84 screens present in the splash screen interface category hold substantial significance, indicating that most app developers will design DUI patterns on splash screens. In addition, the most intriguing insight arises from the "Other" category, which has 506 instances of DUI patterns. This broad category encompasses a diverse range of interface elements and interactions, reflecting developers' creative and adaptable nature in employing DUI patterns. This underlines that DUI patterns are not confined to specific contexts but extend throughout the entire app experience, sometimes in unexpected areas users might overlook.

5.4 DUIs in Mini-apps

In recent years, along with traditional(native) apps, mini-apps have also gained prominence in people's daily lives. Previous research has unveiled a variety of attack patterns affecting users in the mini-program ecosystem [21]. To broaden our investigation, we extend our scrutiny to the mini-app ecosystem. From the top 150 app dataset, we select the top 50 apps, among which 20 apps included mini-apps in WeChat, highlighting the widespread popularity and prevalence of mini-apps in the mobile ecosystem.

Table 2 depicts the case of DUIs in mini-apps. Although there are no *Fake Button* and *Easy Trigger* in mini-apps, compared to traditional apps, mini-apps exhibit a higher occurrence of *Undeclared Acts* and *Disguised Layout* patterns. One reason for this trend is that since mini-apps depend on WeChat, many often want to direct users to jump to their apps. Moreover, compared to apps that undergo reviews by application markets before release, mini-apps face fewer regulations, creating a more ambiguous and gray area. As a result, there tends to be a higher occurrence of Disguised Patterns within mini-apps.

Table 2: Distribution of DUI patterns in mini-apps

DUI patterns	App number	App percentage
Disguised Layout	7	35.00%
Asymmetric Button	15	75.00%
Misleading Text	4	20.00%
Missing Exit	3	15.00%
Fake Button	0	0.00%
Easy Trigger	0	0.00%
Undeclared Acts	5	25.00%

5.5 DUIs V.S. App Popularity

There's an assumption that well-known apps would better eliminate DUI patterns. To investigate this, we divided the apps into three groups: 0-50, 51-100, and 101-150, based on their rankings. Then, we compare the DUI patterns present among these groups.

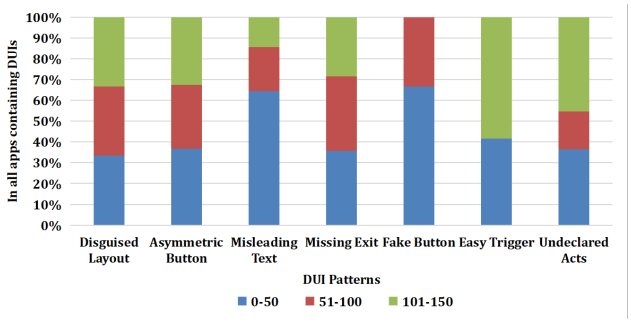


Figure 8: Distribution of three app popularity groups in each DUI pattern

Figure 8 shows the comparison results. Across the app groups, some DUI pattern emerges regardless of app ranking. For instance, the proportions of different groups in DUI patterns like *Disguised Layout*, *Asymmetric Button* and *Missing Exit* are nearly identical, indicating that their situation might not be influenced solely by app popularity. However, specific patterns, such as *Fake Button* and *Easy Trigger*, display a decline in instances or even absence in well-known app groups. In contrast, patterns like *Misleading Text* and *Fake Button* tend to appear more frequently in well-known apps.

This analysis suggests that while app popularity might influence specific DUI patterns to some extent, the effectiveness of eliminating these patterns varies significantly based on various factors. These factors could include the developers' intent and the overall design philosophy of the application. It's not merely about the popularity and word-of-mouth an app has; instead, it's about the commitment of developers to adhere to ethical design practices and the vigilance of regulatory bodies in enforcing policies.

5.6 DUIs in variations of the same app

While evaluating different apps, we observed that developers may design and publish various versions of the same app, such as special editions for seniors and the elderly. These versions are marketed to offer users a faster and more comfortable app experience, with optimizations like improved performance, faster loading speed, and larger font sizes for enhanced usability. As a result, we are interested in exploring whether there are differences in the presence of DUI patterns between these different versions of the same app.

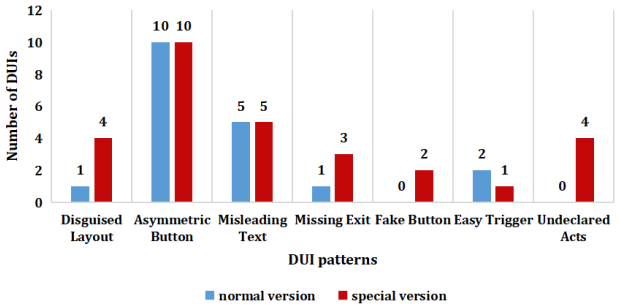


Figure 9: DUIs in variations of the same app

We selected ten apps from our app dataset and analyzed their different versions, as shown in Figure 9. Interestingly, contrary to the developers' claims, we found that there are, in fact, more DUI patterns in the special versions compared to the normal versions. This observation could be attributed to two possible factors. Firstly, since such special apps are not the primary products to be promoted, developers may not prioritize user reviews and retention considerations. Consequently, they may seek to maximize benefits and incorporate various DUI patterns to entice users. Secondly, these special apps receive less attention and regulation compared to their more widely-used counterparts, allowing for the inclusion of more DUI patterns.

5.7 Discussion and Future Work

Root cause of DUIs. The root cause of DUI lies in the pursuit of maximizing the benefits of app developers and advertisers. Nowadays, in the Chinese market, most apps are free apps, so developers need to set up different strategies within their apps to gain revenue. For example, app developers can partner with advertisers or use ad networks to maximize the earning potential [13], and app developers often integrate in-app purchases or VIP models to encourage users to make in-app purchases, providing an ongoing source of income for developers. Therefore, app developers may strategically use DUI patterns to increase advertisement clicks and enhance user engagement, ultimately driving higher app profits.

DUIs in other regions. Although our research focuses on DUI patterns in China, similar situations are also prevalent in mobile ecosystems in other regions. For example, DUIs are also widespread in apps in India [4]. Moreover, the lack of relevant data protection legislation in India [16] may exacerbate the use of dark patterns, as developers may exploit the absence of robust regulations. In Europe, while the GDPR serves as a legislative tool to regulate application behavior and safeguard user data, its enforcement in the context of dark patterns remains a challenge [31]. The global nature of mobile applications requires a comprehensive and coordinated effort to address the widespread issue of DUI patterns. Therefore, harmonizing regulatory frameworks across regions, strengthening enforcement mechanisms, and fostering greater awareness among users and developers are essential to tackling the DUI issue. By promoting transparency and protecting user rights, we can ensure a more user-centric and ethical mobile application ecosystem.

Countermeasure and Future work. Our pipeline offers an effective means to regulate the prevalence of DUI patterns. Through the development of automatic dynamic testing methods and targeted models for detecting DUI patterns, regulators can efficiently filter a large number of apps, swiftly identifying problematic ones that require further investigation. However, there are certain limitations in our current countermeasure, such as the inability to analyze contextual information and the insufficiency of datasets, which limits us from analyzing certain DUI patterns. Given these constraints, our future work aims to optimize the pipeline to cover a more diverse range of DUI patterns. This ongoing improvement process will enable us to provide even more comprehensive insights into the prevalence and impact of DUI patterns in the mobile application ecosystem.

6 CONCLUSION

Our research focused on DUI patterns in the mobile ecosystem, particularly in China. We first introducing a novel taxonomy that categorizes various DUI patterns in the ecosystem. Then, we establish a pipeline and evaluate DUIs in popular apps and mini-apps in China. Analysis results show the widespread presence of various DUIs in today's mobile application landscape. Therefore, better regulation and user-awareness of DUIs in mobile apps are in urgent need.

ACKNOWLEDGMENTS

We would like to thank the anonymous reviewers for their detailed and valuable comments. This work is supported in part by Guangdong Basic and Applied Basic Research Foundation (2023A1515012971), and the Fundamental Research Funds for the Central Universities, Sun Yat-sen University (No.22lgqb26).

REFERENCES

[1] Harry Brignull. 2023. Types of deceptive pattern. https://www.deceptive.design/types. (2023).
[2] Christopher Burr, Nello Cristianini, and James Ladyman. 2018. An analysis of the interaction between intelligent software agents and human users. *Minds Mach.*, 28, 4, (Dec. 2018), 735–774. DOI: 10.1007/s11023-018-9479-0.
[3] Zhaoxin Cai, Yuhong Nan, Xueqiang Wang, Mengyi Long, Qihua Ou, Min Yang, and Zibin Zheng. 2023. Darpa: combating asymmetric dark ui patterns on android with run-time view decorator. In *2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 480–493. DOI: 10.1109/DSN58367.2023.00052.
[4] Alind Chauhan. 2023. Annoying pop-ups you can't get rid of: why govt is going after 'dark patterns'. https://indianexpress.com/article/explained/explained-sci-tech/govt-dark-patterns-explained-8698289/. (2023).
[5] 2020. Chineseocr lite - a chinese optical character recognition tool. https://github.com/DayBreak-u/chineseocr_lite. (2020).
[6] Liqiong Deng and Marshall Scott Poole. 2010. Affect in web interfaces: a study of the impacts of web page visual complexity and order. *MIS Q.*, 34, 711–730. https://api.semanticscholar.org/CorpusID:25739392.

[7] Linda Di Geronimo, Larissa Braz, Enrico Fregnan, Fabio Palomba, and Alberto Bacchelli. 2020. Ui dark patterns and where to find them: a study on mobile applications and user perception. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (CHI '20). Association for Computing Machinery, Honolulu, HI, USA, 1–14. ISBN: 9781450367080. DOI: 10.1145/3313831.3376600.

[8] Feng Dong, Haoyu Wang, Li Li, Yao Guo, Tegawendé F. Bissyandé, Tianming Liu, Guoai Xu, and Jacques Klein. 2018. Frauddroid: automated ad fraud detection for android apps. In *Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering* (ESEC/FSE 2018). Association for Computing Machinery, Lake Buena Vista, FL, USA, 257–268. ISBN: 9781450355735. DOI: 10.1145/3236024.3236045.

[9] 2022. Epic forced to pay record-breaking $520 million fine for violating children's privacy and engaging in dark pattern deception. https://gizmodo.com/epic-fortnite-gaming-ftc-dark-patterns-1849910901. (2022).

[10] European Parliament and Council of the European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council. of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119, 4.5.2016, p. 1–88, (May 4, 2016). Retrieved Apr. 13, 2023 from https://data.europa.eu/eli/reg/2016/679/oj.

[11] State Administration for Market Regulation of China. 2023. Administrative measures for internet advertising. (2023). Phttps://www.gov.cn/gongbao/2023/issue_10506/202306/content_6885261.html.

[12] Google. Year of publication. Uiautomator. Android Open Source Project. (Year of publication). https://developer.android.com/training/testing/ui-automator.

[13] Michael C. Grace, Wu Zhou, Xuxian Jiang, and Ahmad-Reza Sadeghi. 2012. Unsafe exposure analysis of mobile in-app advertisements. In *Proceedings of the Fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks* (WISEC '12). Association for Computing Machinery, Tucson, Arizona, USA, 101–112. ISBN: 9781450312653. DOI: 10.1145/2185448.2185464.

[14] Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L. Toombs. 2018. The dark (patterns) side of ux design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (CHI '18). Association for Computing Machinery, Montreal QC, Canada, 1–14. ISBN: 9781450356206. DOI: 10.1145/3173574.3174108.

[15] Lei Hao, Fucheng Wan, Ning Ma, and Yicheng Wang. 2018. Analysis of the development of wechat mini program. *Journal of Physics: Conference Series*, 1087. https://api.semanticscholar.org/CorpusID:188887688.

[16] Siri Harish†. 2022. Yes, or yes? the reality of dark patterns. https://www.sconline.com/blog/post/2022/08/15/yes-or-yes-the-reality-of-dark-patterns/. (2022).

[17] 2020. How facebook and other sites manipulate your privacy choices. https://www.wired.com/story/facebook-social-media-privacy-dark-patterns/. (2020).

[18] Tim Kollmer and Andreas Eckhardt. 2023. Dark patterns. *Business & Information Systems Engineering*, 65, 2, (Apr. 2023), 201–208. DOI: 10.1007/s12599-022-00783-7.

[19] Irina Lgotina. 2023. Banned dark patterns vs permitted tricks for mobile apps. https://adapty.io/blog/dark-patterns-and-tricks-in-mobile-apps. (2023).

[20] Tianming Liu, Haoyu Wang, Li Li, Xiapu Luo, Feng Dong, Yao Guo, Liu Wang, Tegawendé Bissyandé, and Jacques Klein. 2020. Maddroid: characterizing and detecting devious ad contents for android apps. In (WWW '20). Association for Computing Machinery, Taipei, Taiwan, 1715–1726. ISBN: 9781450370233. DOI: 10.1145/3366423.3380242.

[21] Haoran Lu, Luyi Xing, Yue Xiao, Yifan Zhang, Xiaojing Liao, Xiaofeng Wang, and Xueqiang Wang. 2020. Demystifying resource management risks in emerging mobile app-in-app ecosystems. *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*. https://api.semanticscholar.org/CorpusID:222266008.

[22] Jamie B. Luguri and Lior Jacob Strahilevitz. 2019. Shining a light on dark patterns. *Behavioral & Experimental Economics eJournal*. https://api.semanticscholar.org/CorpusID:202481408.

[23] S M Hasan Mansur, Sabiha Salma, Damilola Awofisayo, and Kevin Moran. 2023. Aidui: toward automated recognition of dark patterns in user interfaces. *2023 IEEE/ACM 45th International Conference on Software Engineering (ICSE)*, 1958–1970. https://api.semanticscholar.org/CorpusID:257496896.

[24] Arunesh Mathur, Gunes Acar, Michael J. Friedman, Eli Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan. 2019. Dark patterns at scale: findings from a crawl of 11k shopping websites. 3, CSCW, Article 81, (Nov. 2019), 32 pages. DOI: 10.1145/3359183.

[25] Arunesh Mathur, Mihir Kshirsagar, and Jonathan Mayer. 2021. What makes a dark pattern... dark? design attributes, normative considerations, and measurement methods. In (CHI '21) Article 360. Association for Computing Machinery, Yokohama, Japan, 18 pages. ISBN: 9781450380966. DOI: 10.1145/3411764.3445610.

[26] Thomas Mejtoft, Erik Frängsmyr, Ulrik Söderström, and Ole Norberg. 2021. Deceptive design: cookie consent and manipulative patterns. In *34th Bled eConference: Digital Support from Crisis to Progressive Change, June 27 - 30, 2021, Online Conference, Proceedings*. Andreja Pucihar, Mirjana Kljajic Borstnar, Roger W. H. Bons, Helen Cripps, Anand Sheombar, and Doroteja Vidmar, (Eds.) University of Maribor Press / Association for Information Systems, 36. https://aisel.aisnet.org/bled2021/36.

[27] Alberto Monge Roffarello and Luigi De Russis. 2022. Towards understanding the dark patterns that steal our attention. In *Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems* (CHI EA '22) Article 274. Association for Computing Machinery, New Orleans, LA, USA, 7 pages. ISBN: 9781450391566. DOI: 10.1145/3491101.3519829.

[28] Carol Moser, Sarita Y. Schoenebeck, and Paul Resnick. 2019. Impulse buying: design practices and consumer needs. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (CHI '19). Association for Computing Machinery, Glasgow, Scotland Uk, 1–15. ISBN: 9781450359702. DOI: 10.1145/3290605.3300472.

[29] Arvind Narayanan, Arunesh Mathur, Marshini Chetty, and Mihir Kshirsagar. 2020. Dark patterns: past, present, and future. *Commun. ACM*, 63, 9, (Aug. 2020), 42–47. DOI: 10.1145/3397884.

[30] 2021. Notification regarding the list of removed apps violating user rights. https://www.gov.cn/xinwen/2021-12/12/content_5660255.htm. (2021).

[31] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. 2020. Dark patterns after the gdpr: scraping consent pop-ups and demonstrating their influence. In (CHI '20). Association for Computing Machinery, Honolulu, HI, USA, 1–13. ISBN: 9781450367080. DOI: 10.1145/3313831.3376321.

[32] Standing Committee of the National People's Congress of the People's Republic of China. 2018. Advertising law of the people's republic of china. (2018). https://www.gov.cn/guoqing/2021-10/29/content_5647620.htm.

[33] Justin W. Owens, Evan M. Palmer, and Barbara S. Chaparro. 2014. The pervasiveness of text advertising blindness. *Journal of Usability Studies archive*, 9, 51–69. https://api.semanticscholar.org/CorpusID:59184325.

[34] 2023. Ui/Application Exerciser Monkey. https://developer.android.com/studio/test/other-testing-tools/monkey. (2023).

[35] 2023. Wandoujia. https://www.wandoujia.com. (2023).

[36] 2022. YOLO - An Object Detection Algorithm. https://github.com/ultralytics/yolov5. (2022).