IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 4, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304031 |

Image Pixel Based Mobile Devices Unlocking System

Dr.R.Nagarajan[1], Hari S[2]

[1]Assistant Professor, PG & Research Department of Computer Science, Sri Ramakrishna College of Arts & Science, Coimbatore, India

[2]UG Student, PG & Research Department of Computer Science, Sri Ramakrishna College of Arts & Science, Coimbatore, India

ABSTRACT: In digital imaging, a pixel picture element is a smallest addressable element in a raster image, or the smallest addressable element in an all points addressable display device so it is the smallest controllable element of a picture represented on the screen. Techniques are disclosed for providing an image pattern unlock mode in electronic touch sensitive devices. The image pattern unlock mode can display an unlock screen to the user, prompting the user to arrange or create or otherwise select a specific image pattern in order to unlock the device. The customizable image pattern may include any uniquely identifiable unlocking pattern including a combination of images, or even a single image selected from an image group.In this system, new unlocking method is developed based on image pixel which offers the high security model. The unlocking mechanism may include images gathered from the user's photo collection and/or one or more online profiles, and the unlock pattern could be a selection of such images. In other embodiments, a combination of color and images can also be used, such as matching colors to images. When the user has arranged the proper image pattern, the device unlocks and may be used. If the correct image pattern is not arranged, the device remains locked

KEYWORDS: Image, EDA, Touch points, machine learning,

I. INTRODUCTION

Electronic display devices such as tablets, Readers, mobile phones, smart phones, personal digital assistants (PDAs), and other such touch screen electronic display devices are commonly used for displaying consumable content. The content may be, for example, an eBook, an online article or blog, images, a movie or video, a map, just to name a few types. Such display devices are also useful for displaying a user interface that allows a user to interact with an application running on the device. The user interface may include, for example, one or more touch screen controls and/or one or more displayed labels that correspond to nearby hardware buttons.

The touch screen display may be backlit or not, and may be implemented for instance with an LED screen or an electrophoretic display. Such devices may also include other touch sensitive surfaces, such as a track pad (e.g., capacitive or resistive touch sensor) or touch sensitive housing (e.g., acoustic sensor). The electronic display devices such as tablets, Readers, and smart phones are commonly used for displaying user interfaces and consumable content. The user of such devices can typically consume the displayed content with relative ease. In some instances, the user may wish to lock the device while it is not being used. While available device locking techniques are commonly provided with touch screen devices for such purposes, an image pattern unlock mode as described herein may provide a secure and more intuitive computing device unlock technique, or otherwise enhance the user experience.

Thus, and in accordance with an embodiment of the present invention, image pattern unlocking techniques are disclosed for use in electronic touch screen devices. In some embodiments, after an electronic device has been locked, placed into sleep or power-saving mode, or restarted, the user must first unlock the device before it can be used again. Such a locking function provides security, helping to prevent unauthorized use of the device. By implementing the image pattern unlocking techniques described herein, the user may further personalize the unlocking function.In one specific example, when a device is locked the device may display an unlock screen whenever a user indicates a desire to begin using the device.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304031 |

II. RELATED WORK

While the mobile device is locked, a touch gesture having a pre-defined shape is detected on a touch screen of the mobile device independently of the initial position of the touch gesture on the touch screen. In this way, detection of the touch gesture causes the particular action to execute while keeping the mobile device locked. In future the scheme can be combined with the face recognition and fingerprint authentication. Using NFC, SmartTag is a small token that has read/write capabilities to/from the phone when it is in close proximity to the phone.This is convenient if there are multiple users or if the phone is used in different locations. When traveling abroad, one could easily use a SmartTag with a profile in which expensive roaming is disabled.

III. PROPOSED METHODOLOGY

Access to data included in the mobile device is permitted when the presence of an authentication device having the proper authentication information is received by the mobile device. The disclosed embodiments relate generally to the field of policy and security implementation on computing devices. More specifically, embodiments described herein provide a system and method for implementing security features and policies between paired devices. A possible danger and/or inconvenience of utilizing devices such as handheld and/or mobile electronic devices is that if the handheld and/or mobile device is lost or stolen, the finder or thief may access all of the financial and/or personal information on the device. Currently a variety of methods are used to protect data on such devices, most commonly the utilization of the entering of a password and/or the entering of a combination of user name and password. However, it has been shown that the use of a password and/or the inconvenience that a user must input a password each time the information is to be accessed has been shown to be undesirable.

In the first instance, it has been shown that passwords may be circumvented by a variety of techniques known and practiced by computer savvy persons, hackers, and the like. Further, in the event that a person wishes to access specific information using the portable electronic device, it is often an inconvenience that the person accessing the information is required to input a password each time such information is requested and/or desired. Accordingly, there is a need to provide an ability to protect data on a mobile electronic device without the use of a password or other conventional means. There is also a need for a mobile electronic device that includes a separate access device which allows access to secured information on the mobile electronic device. Further, there is a need for a wireless access device that is separate from the mobile device and allows access to the personal and/or financial information on the device when the device is within a close proximity of the mobile device. Further still, there is a need for a method of providing access to personal and/or financial information on the mobile device by the utilization of a wireless access device.

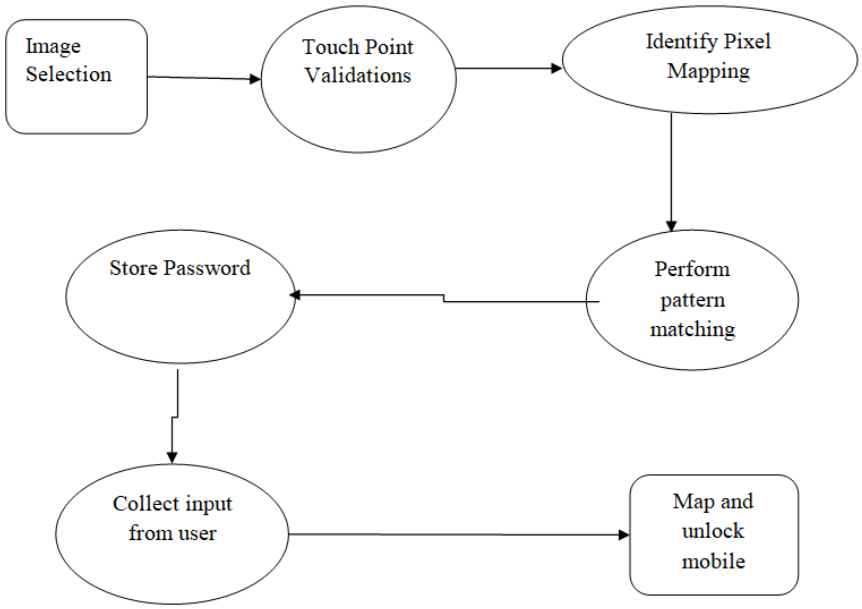

Fig-1 System Architecture

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304031 |

IV. RESULT AND DISCUSSION

The lock screen module is configured to receive an input to authenticate the user and/in response to the authenticated input, unlock the mobile device, and further comprising gesture definition module that, when the mobile device is unlocked, is configured to receive the touch gesture entered by the user that, when detected by the gesture interpretation module, causes the lock action module to execute the particular action, whereby detection of the user-defined shape securely authorizes execution of the particular action while the lock screen view is displayed at the touch screen

Figure 2- Mobile Unlocking Interface

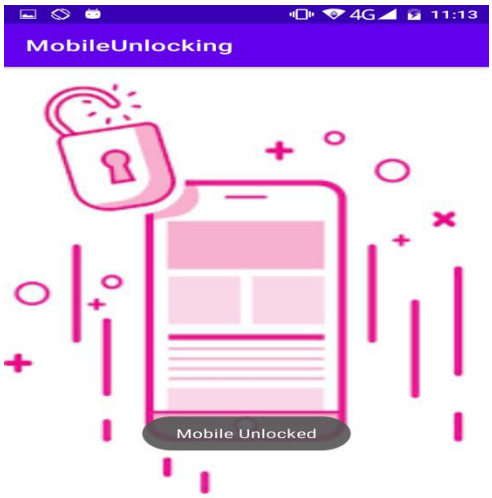

Figure 3 Unlocked Mobile UI

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304031 |

REFERENCES

1. Sun, C., Wang, Y. and Zheng, J., 2014. Dissecting pattern unlock: The effect of pattern strength meter on pattern selection. *Journal of Information Security and Applications*, *19*(4-5), pp.308-320. Aviv, A.J., Budzitowski, D. and Kuber, R., 2015, December. Is bigger better? Comparing user-generated passwords on 3x3 vs. 4x4 grid sizes for android's pattern unlock. In *Proceedings of the 31st Annual Computer Security Applications Conference* (pp. 301-310)Kunda, D. and Chishimba, M., 2018. A survey of android mobile phone authentication schemes. Mobile Networks and Applications, pp.1-9.
2. Tsai, Y.C. and Yang, C.H., 2013. Physical forensic acquisition and pattern unlock on Android smart phones. In Future information communication technology and applications (pp. 871-881). Springer, Dordrecht.
3. Tsai, Y.C. and Yang, C.H., 2013. Physical forensic acquisition and pattern unlock on Android smart phones. In Future information communication technology and applications (pp. 871-881). Springer, Dordrecht.
4. Chaitanya, G.K. and Raja Sekhar, K., 2021. Verification of pattern unlock and gait behavioural authentication through a machine learning approach. International Journal of Intelligent Unmanned Systems.
5. Saxena, N., Uddin, M.B., Voris, J. and Asokan, N., 2011, March. Vibrate-to-unlock: Mobile phone assisted user authentication to multiple personal RFID tags. In 2011 IEEE International Conference on Pervasive Computing and Communications (PerCom) (pp. 181-188). IEEE.
6. Hintze, D., Hintze, P., Findling, R.D. and Mayrhofer, R., 2017. A large-scale, long-term analysis of mobile device usage characteristics. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 1(2), pp.1-21.
7. Ibrahim, N. and Sellahewa, H., 2017, February. Touch gesture-based authentication: A security analysis of pattern unlock. In 2017 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA) (pp. 1-8). IEEE.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details