CREATING A PASSWORD PROTECTED FOLDER FOR WINDOWS' HOME VERSION AND A PENDRIVE

PRATHAM PAWAR

Vasantdada Patil Prathisthan's College Of Engineering And Visual Arts
Sion- Mumbai (400070), India.

***Abstract*- This research addresses the limitations faced by users of basic versions of Windows, who lack the capability to create password-protected and hidden folders without requiring an upgrade to enterprise editions. We present a novel solution that enables users to establish secure folders within basic Windows platforms. Our approach involves the successful implementation of password protection and hidden attributes for folders in basic Windows versions. By disguising the secure folder as a system component file, its visibility to unauthorized users is reduced, enhancing its concealment. Furthermore, our solution ensures the portability of these secure folders, allowing them to be seamlessly transferred to compatible pen drives while retaining their protective features. Upon accessing the folder, users encounter a command-line interface that prompts them to enter a predefined password for entry. This rigorous authentication mechanism prevents unauthorized access to the folder's contents. Our research bridges the functionality gap between basic and enterprise Windows editions, providing enhanced security measures for users operating on basic platforms. The findings contribute to advancing Windows security practices, offering a practical solution for safeguarding sensitive data in everyday computing environments.**

***Keywords*: Authentication, folder security, batch scripting, hidden folder, data security.**

I. INTRODUCTION

In the contemporary digital age, the omnipresence of electronic devices exposes users to various threats, ranging from corruption to unauthorized access and misuse. Particularly vulnerable is the wealth of information stored within these devices, coveted by nefarious entities seeking to exploit vulnerabilities for personal gain or malicious intent. As such, safeguarding both the integrity of our devices and the confidentiality of the data they contain has become paramount. Trusting external applications or devices with sensitive data without stringent scrutiny poses a significant risk, as evidenced by the increasing prevalence of data breaches and cyberattacks across various platforms.

Within the realm of Windows operating systems, the disparity between basic or home versions and their enterprise-grade counterparts becomes apparent, particularly concerning the ability to create password-protected folders. Unlike the robust security features inherent in 'Enterprise' and 'Professional' editions, the basic iterations lack this fundamental capability, necessitating the installation of third-party applications for users seeking enhanced data protection. Recognizing this disparity as a barrier to effective data security, our research endeavours to bridge this gap by providing users of basic Windows versions with a straightforward and accessible solution for creating password-protected and hidden folders.

The primary objective of this project is to empower users of basic Windows platforms with the ability to fortify their data security without reliance on third-party software. By leveraging default system components and leveraging the simplicity of batch scripting, our approach ensures ease of implementation and accessibility for users of varying technical proficiencies. Furthermore, the versatility of our solution extends beyond desktop environments, enabling users to securely store data on portable media such as pen drives, thereby enhancing data security in everyday computing scenarios.

In this paper, we present a novel solution that enables users to establish secure folders within basic Windows platforms, effectively mitigating the inherent limitations of these operating systems. Through the successful implementation of password protection and hidden attributes, our solution ensures the confidentiality and integrity of sensitive data, without necessitating costly upgrades or reliance on external applications. By addressing this critical functionality gap, our research contributes to advancing Windows security practices, offering a practical and accessible solution for safeguarding sensitive data in everyday computing environments.

today's globalized world, international education has become a transformative experience, offering students the opportunity to explore diverse cultures, gain valuable skills, and broaden their horizons. However, embarking on the journey from university selection to successful settlement in a foreign land is not without its complexities and challenges [4]. International students often grapple with a multitude of decisions, including choosing the right university, assessing their acceptance probabilities, and securing suitable accommodation.

II. RELATED WORK

As In 2008, the authors Satishkumar L. Varma, Satishkumar S. Chavan, Sanjay N. Talbar aimed to address the need for securing sensitive data by proposing a method to hide, encrypt, and decrypt files and folders on Windows systems, ensuring privacy and security. They employed encryption algorithms such as AES and Blowfish, in addition to rootkit concealment techniques, to develop a Folder Lock method with added security features for file protection. While exploring various methods, they found that some did not fully meet user requirements, leading them to enhance their approach to provide better security for files and folders. Their work, titled "An Approach to Lock the Encrypted Files and Folders," presents a comprehensive solution to address the vulnerability of sensitive data on Windows systems.[1]

During the period of April 2015 to September 2015, authors Madhuri Akhand, Ankita Bijwe, Kajal Zade, and Karuna Borkar collaborated on the design of a folder security model employing a graphical password authentication scheme. Their innovative system, dubbed Pass Points, introduced a novel approach where users authenticate themselves by clicking on images. While this method offered a visually intuitive means of authentication, it also posed challenges. Users were required to remember their selected pass-images, introducing a potential usability obstacle. Additionally, ensuring secure authentication remained a significant concern. Their work, titled "Folder Security Using Graphical Password Authentication Scheme," contributes to the exploration of alternative authentication methods, shedding light on both their benefits and challenges [2].

In 2017, authors Chandni B Menon, Anju Joy, Emilda Emmanuel, and Dr Vince Paul introduced a novel approach to folder security with their Three Factor Authentication (3FA) system. Their system utilized three distinct factors for authentication: a passphrase, a physical device, and network connection. By incorporating Bluetooth connectivity and one-time password (OTP) technology, they aimed to enhance the security of folder access. This innovative methodology not only introduced multiple layers of authentication but also leveraged modern technologies to strengthen overall security measures. Their research, titled "Folder Security Using A Iterative Algorithm Through Bluetooth Connectivity Using One Time Password," presents a promising advancement in folder security systems, emphasizing the importance of multi-factor authentication in contemporary security practices [3].

In 2022, authors Raznida Isa, Shuhadah Othman, Muhammad Zulhelmiy Fadlie Ismail, and Noor Maizat embarked on the development of a Lock Folder Application with Graphical Password, aimed at bolstering security measures. Their approach involved the utilization of the Waterfall Model Methodology for project development, ensuring systematic and comprehensive progress throughout the development lifecycle. By incorporating a graphical password authentication mechanism, their application introduced an intuitive and visually engaging method for folder security. Their research, titled "The Development of a Lock Folder Application with Graphical Password," presents a significant advancement in folder security solutions, highlighting the integration of innovative authentication methods to enhance overall security [4].

In 2009, authors Osamu Matoba, Takanori Nomura, Elisabet Perez-Cabre, Maria S. Millan and Bahram Javidi presented a paper which gives an overview of utilizing optical techniques for encryption, security, and authentication by exploiting the various degrees f freedom in optical waveforms, including amplitude, phase, polarization, spectral content, and multiplexing. It reviews methods for encrypting and securing two-dimensional and three-dimensional data, emphasizing interferometric approaches for data recording and retrieval using optical or digital holography [5].

III. METHODOLOGY:

This research focuses on creating a password protected folder in basic/home versions of Windows operating systems without installing a third-party application or software and utilising the built-in features to enhance security and reduce this risk of storing data in an un-protected manner.
Figure 1 shows the execution flow of the code :

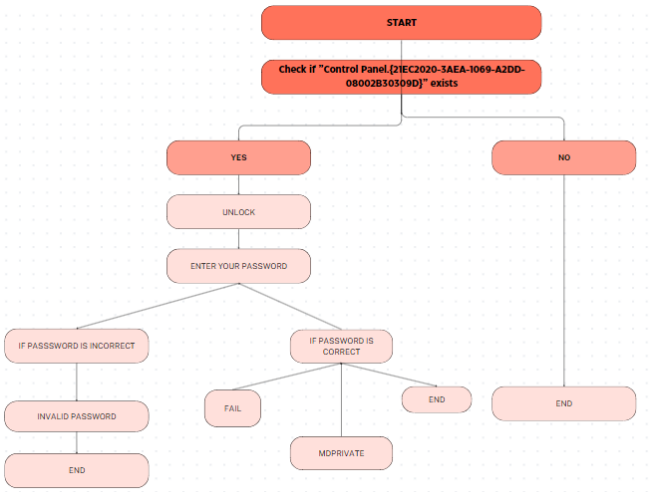

Fig.1 Code Workflow Diagram

```
@ECHO OFF
if EXIST "Control Panel.
{21EC2020-3AEA-1069-A2DD-08002B30309D}" goto
UNLOCK
if NOT EXIST Private goto MDPrivate
:CONFIRM
echo Are you sure to lock this folder? (Y/N)
set/p "cho=>"
if %cho%==Y goto LOCK
if %cho%==y goto LOCK
if %cho%==n goto END
if %cho%==N goto END
echo Invalid choice.
goto CONFIRM
:LOCK
ren Private "Control Panel.
{21EC2020-3AEA-1069-A2DD-08002B30309D}"
attrib +h +s "Control Panel.
{21EC2020-3AEA-1069-A2DD-08002B30309D}"
echo Folder locked
goto End
:UNLOCK
echo Enter password to Unlock Your Secure Folder
set/p "pass=>"
if NOT %pass%== YOUR-PASSWORD goto FAIL
attrib -h -s "Control Panel.
{21EC2020-3AEA-1069-A2DD-08002B30309D}"
ren "Control Panel.
{21EC2020-3AEA-1069-A2DD-08002B30309D}"
Private
echo Folder Unlocked successfully
goto End
:FAIL
echo Invalid password
goto end
:MDPrivate
md Private
echo Private created successfully
goto End
:End
```

Fig.2 Batch Script Code

Explanation for each command being used in code :

i. `@ECHO OFF: This command turns off the command echoing in the console, so the commands themselves won't be displayed as they are executed.
ii. `if EXIST "Control Panel.{21EC2020- 3AEA-1069-A2DD-08002B30309D}" goto UNLOCK: This line checks if the folder "Control Panel.{21EC2020-3AEA-1069-A2DD-
iii. 08002B30309D}" exists. If it does, it jumps to the UNLOCK section of the script.
iv. `if NOT EXIST Private goto NDPrivate: If the folder "Control Panel.
v. {21EC2020-3AEA-1069-A2DD-
vi. 08002B30309D)" doesn't exist, this line checks if a folder named "Private" exists. If it doesn't, it jumps to the MDPrivate section to create the "Private" folder.
vii. ` CONFIRM: This marks the beginning of a label named "CONFIRM," which is used to prompt the user for confirmation.

viii. `echo Are you sure to lock this
ix. folder? (Y/N)': This line displays a message asking the user if they are sure they want to lock the folder.
x. 'set/p "cho=>"': This line waits for the user to input a choice (Y/N).
xi. The next few lines use conditional statements ('if' statements) to determine the user's choice:
xii. If the user chooses 'Y' or 'y', it jumps to the LOCK section.
xiii. If the user chooses 'N' or 'n', it jumps to the `END` section to exit the script.
xiv. If the user enters anything else, it notifies them of an invalid choice and loops back to the 'CONFIRM section.
xv. `: LOCK: This marks the beginning of a label named "LOCK," where the folder locking process begins.
xvi. `ren Private "Control Panel.
xvii. {21EC2020-3AEA-1069-A2DD-
xviii. 08002B30309D)"': This line renames the "Private" folder to "Control Panel.{21EC2020- 3AEA-1069-A2DD-08002B30309D}" effectively hiding it.
xix. 'attrib +h +s "Control Panel.
xx. (21EC2020-3AEA-1069-A2DD- 08002B30309D}"': This line sets the attributes of the renamed folder to make it hidden (+h) and a system folder ('+s').
xxi. `echo Folder locked': This line notifies the user that the folder has been successfully locked.
xxii. `goto End: This line jumps to the 'End section to exit the script.
xxiii. UNLOCK: This marks the beginning of a label named "UNLOCK," where the folder unlocking process begins.
xxiv. `echo Enter password to Unlock Your Secure Folder': This line prompts the user to enter a password to unlock the folder.
xxv. `set/p "pass=>"': This line waits for the user to input a password.
xxvi. if NOT %pass%== YOUR-PASSWORD goto FAIL: This line checks if the entered password matches a predefined password. If it doesn't match, it jumps to the 'FAIL section. 17. `attrib -h -s "Control Panel. {21EC2020-3AEA-1069-A2DD- 08002B30309D}"': This line removes the hidden (-h`) and system (`-s') attributes from the locked folder, making it visible again. 18. `ren "Control Panel.{21EC2020-3AEA- 1069-A2DD-08002B30309D}" Private: This line renames the locked folder back to its original name, "Private," effectively unlocking it.
xxvii. echo Folder Unlocked successfully: This line notifies the user that the folder has been successfully unlocked.
xxviii. `goto End: This line jumps to the 'End section to exit the script.
xxix. `: FAIL: This marks the beginning of a label named "FAIL," which handles the case when the user enters an incorrect password.
xxx. `echo Invalid password': This line notifies the user that the password they entered is invalid.
xxxi. goto end: This line jumps to the End section to exit the script.
xxxii. ‘:MDPrivate': This marks the beginning of a label named "MDPrivate," which is executed if the "Private" folder doesn't exist.
xxxiii. `md Private: This line creates a folder named "Private."
xxxiv. `echo Private created successfully':
xxxv. This line notifies the user that the "Private" folder has been successfully created.
xxxvi. 'goto End': This line jumps to the 'End section to exit the script.
xxxvii. End: This marks the end of the script.

Steps to implement are as follows :

i. Open a new text file in the desired location of the locked folder.
ii. Find the text ‘YOUR PASSWORD’ and replace this text with the password you want for your folder.
iii. While saving this file, give it a name as per your convenience and save it with a ‘.bat’ extension. Also, in the file type list select the ‘all types’ options and save it.
iv. You will see a new folder is created, then delete this text file which contains the script.
v. Double click on the folder to access it.
vi. A prompt will pop up asking for the password, enter the text which you had replaced with ‘YOUR PASSWORD’ in step 2 and hit enter.
vii. A new folder with the name ‘Private’ will be visible.
viii. Store the data in that folder, and to lock it again double click on the grey color folder.
ix. Again a prompt will pop up but this time it will ask for your permission on whether to lock the folder or not. Just answer it as yes by entering ‘Y or y’ and hit enter. The folder is locked again.
x. To access the locked folder again, simply follow the step 5 and step 6.

IV. RESULT AND DISCUSSION

This research focuses on creating a password- This study introduces a solution to the limitations faced by standard Windows users who cannot create password-protected and hidden folders without upgrading to enterprise editions. It

proposes a method for establishing secure directories within standard Windows environments, incorporating password protection and concealment attributes. By disguising the secure folder as a system component file, its visibility to unauthorized users is minimized. Additionally, the solution ensures the portability of these secure folders, enabling seamless transfer to compatible flash drives while retaining protective features. Upon access, users encounter a command-line interface requiring a predefined password, thus preventing unauthorized entry. This research bridges the gap between standard and enterprise Windows editions, providing enhanced security measures for standard platform users and contributing to the advancement of Windows security practices.

Corresponding images depict the entire process being executed:

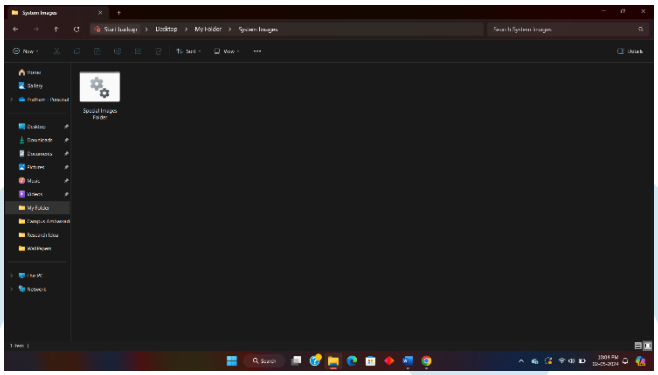

Fig.3 Batch folder

Fig 3 shows a batch folder being created which has the private folder hidden inside it.

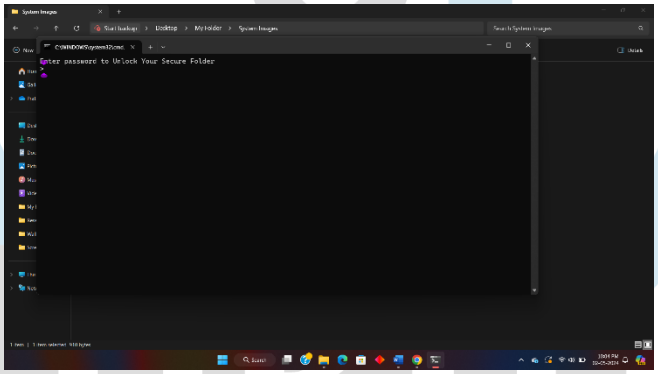

Fig.4 Prompt Asking For Password

Fig 4 shows the prompt which appears after double-clicking on the batch folder, asking for password. If correct password is not entered then private folder won't appear.

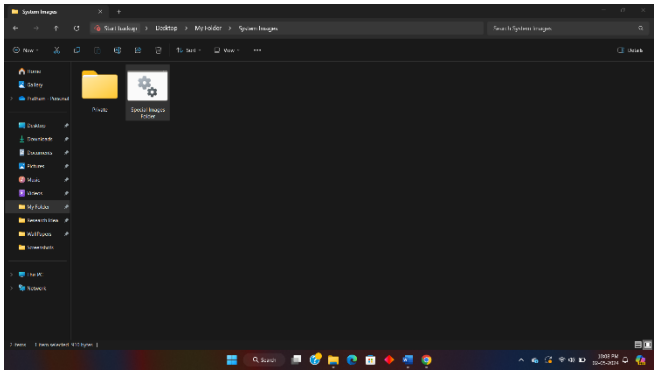

Fig.5 After Entering The Correct Password

Fig 5 clearly shows how the private folder is being visible after entering the correct password.

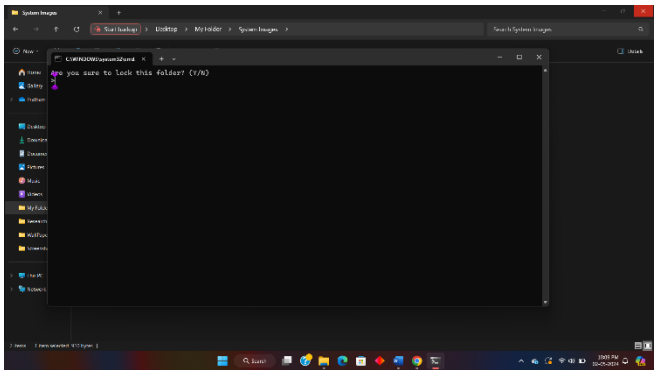

Fig.6 Asking For Confirmation Before Locking The Folder

Fig 6 exhibits the prompt coming up after double-clicking on the batch folder, asking for conformation to lock and hide the private folder.

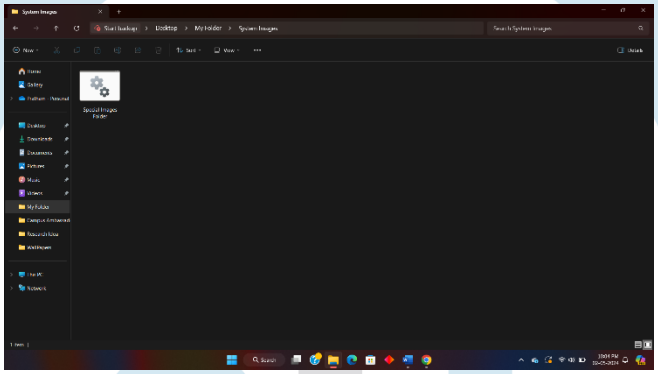

Fig.7 Folder Is Locked After Confirmation

Fig 7 shows that the private folder is locked and hidden after confirming the input from the user.

V.CONCLUSION

In conclusion, our research has shown a workable and approachable way to make hidden and password-protected folders in home versions of Windows operating systems without having to buy enterprise or professional editions or use third-party software. This technique provides an easy-to-use method that doesn't require complicated procedures or complicated algorithms for implementation. Moreover, the security of the protected folders is reinforced by the requirement of in-depth knowledge in batch scripting to potentially exploit this method. Our approach eliminates the need for extra financial investments or reliance on external software solutions by providing customers with better data security safeguards by bridging the gap between basic and advanced Windows editions. This ensures the confidentiality and integrity of critical information.

REFERENCES:

[1] S. L. Varma, S. S. Chavan, and S. N. Talbar, An Approach to Lock the Encrypted Files and Folders. .
[2] M. Akhand, A. Bijwe, K. Zade, and K. Borkar, Folder Security Using Graphical Password Authentication Scheme.
[3] C. B. Menon, A. Joy, E. Emmanuel, and V. Paul, Folder Security Using An Iterative Algorithm Through Blue-Tooth Connectivity Using One Time Password. .
[4] R. Isa, S. Othman, M. Z. F. Ismail, and N. M. M. Sabri, “The development of A lock folder application with graphical password,” in The European Proceedings of Multidisciplinary Sciences, 2022.
[5] O. Matoba, T. Nomura, E. Perez-Cabre, M. S. Millan, and B. Javidi, “Optical Techniques for Information Security,” Proc. IEEE Inst. Electr. Electron. Eng., vol. 97, no. 6, pp. 1128–1148, 2009.