European Proceedings of
Multidisciplinary Sciences
EpMS

www.europeanproceedings.com

e-ISSN: 2421-826X

DOI: 10.15405/epms.2022.10.56

ICONSPADU 2021
International Conference on Sustainable Practices, Development and Urbanisation

FILE HIDING WEB APPLICATION (FHWA) USING IMAGE STEGANOGRAPHY

Noraliza Azizan (a)*, Farah Farzana Abdul Aziz (b), Nor Shamshillah Kamarzaman (b), Norhayati Abdul Jamil (a), Jaaz Suhaiza Jaafar (b), Amirul Naim Mohd Shafiee (b)
*Corresponding author

(a) Kolej Universiti Poly-Tech MARA, Jalan 6/91 Taman Shamelin Perkasa, 56100 Kuala Lumpur, Malaysia, noraliza@kuptm.edu.my
(b) Kolej Universiti Poly-Tech MARA, Jalan 6/91 Taman Shamelin Perkasa, 56100 Kuala Lumpur, Malaysia

Abstract

File hiding is a process of hiding any files in computer from being accessed by anyone. This process is necessarily used in order to prevent any snoopers from accessing private and confidential files. Today, various extant file hiding applications existed but there is unfriendly user issue arises where only certain files can be hidden. Some of the applications can hide text file only and some others can only hide image files. Thus, it is difficult for users to hide any file of their choice because they need to use more than one tools or applications that support the file type. This paper presents File Hiding Web Application (FHWA) which can be used to hide any type of files using image steganography as a security mechanism. This application is developed using Agile methodology and Visual Studio Code is used to build the system as the code editor. Programming languages like Tailwind CSS, Semantic UI and JavaScript including Node.js, ReactJS and Next.js are used for frontend and backend development while MongoDB is used to store the databases. Based on user acceptance testing, the result shows on average 98% of the respondents are able to use FHWA to hide any type of files and reveal them successfully.

Keywords: File hiding, security, steganography

https://doi.org/10.15405/epms.2022.10.56
Corresponding Author: Noraliza Azizan
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

1. Introduction

In today's era of technology, computers have already become part of human lives. We use them for many reasons, most importantly is to help with human tasks. One of computer's main function is the storage capability where it provides huge advantage to human being. We store lot of data, information and result in computer today compare to physical file in a cabinet. The dependency of human on computer has led to a new wave of associated security issues and threats (Surya, 2014). When there are sensitive and private information, criminals follow. Without proper security measurements, unauthorized file access may happen.

Apart from adopting cryptography method, we developed File Hiding Web Application (FHWA) using another security technique which is image steganography method. This method allows user to hide any type of file into an image file. While current applications only focus on certain type of files that can be hidden, FHWA can hide any file types. Some of existing applications can hide only text messages and some others can only hide image files (Shafiee, 2020). Thus, it is difficult for users to hide any file they wish to keep secret because they need to use more than one tools or applications that support the file type to be hidden. Therefore, the significance of this development is users can hide any file type that they want, including text message, image, audio, video, and document by using only one application.

Hiding a file with steganography technique alone is not enough because it only can hide the secret data but do not encrypt it. Thus, we also implemented cryptography technique in this application where users can secure the hidden file using encryption method. Users can set a password to lock the hidden file and only authorized users can decrypt it. Any file hidden in the image can be revealed (steganalysis) or opened after the user successfully unlock the hidden file. Steganalysis is an important part of steganography as it is a process to identify the secret message.

In this paper, we will be focusing more on the image steganography method rather than discussing further about encryption technique. We then presented the finding from user acceptance testing which disclosed on average 98 percent of the respondents are successful in using FHWA to hide private and confidential files inside an image file with both encryption and cryptography techniques. They also can reveal the hidden files with no problem.

2. Problem Statement

There are three problem statements discussed in this paper, which are:

2.1. Only limited file type that can be hidden

Most of current systems provide only one type of file that can be hidden. Some systems can only hide text messages and other systems can only hide image files. This can be a tedious task for users because they need to find different hiding tools or software to hide any file type that they want. User may give up to hide their confidential information since it cost time to search for a tool that can hide any specific file type (Semilof & Clark, 2018).

https://doi.org/10.15405/epms.2022.10.56
Corresponding Author: Noraliza Azizan
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

2.2. Unauthorized user can easily finds and view the hidden file

Some of the current systems did not provide encryption or password to lock the hidden file. Kessler (2015) mentioned that when the hidden file does not have any password or encryption to open it, the process of hiding data is simply pointless. It is still not secure even the user already hides the data because an intruder may detect the secret information easily and find a solution to conceal or reveal it since the hidden file is not encrypted. Without encrypting this hidden file, it will make it easier for intruders to obtain secret data.

2.3. Revealing process is not provided and only certain file types can be revealed

Most of the current systems do not provide the revealing process of the hidden files. Although some current systems provide the revealing process, the system can only reveal certain types of files. This can be difficult for users because they cannot reveal the hidden file easily since some current systems did not provide the revealing process (Stone, 2017). Other than that, since some of the current systems only can hide certain file types, then the system also only could reveal certain types of hidden files. Thus, they need to find different revealing tools or software to reveal the hidden files inside the image file.

3. Research Questions

i. Can a user hide any file type inside an image using FHWA?
ii. Only authorized users can read or viewed the hidden files in FHWA?
iii. Can authorized users reveal any type of files hidden inside the image file using FHWA?

4. Purpose of Study

4.1. To enable a user to hide any type of file inside an image

This paper discusses how a user can hide any type of files or information into another file which is an image file. To make this happen, image steganography technique is used in FHWA. With this technique, the user will be able to hide and unhide the secret file. Other than that, users can hide any type of file including text message, image, audio, video, and any document type together with the image data.

4.2. To ensure that hidden files are read or viewed only by authorized users

The paper also highlighted how FHWA enables the users to set a password and encrypt their hidden files. Only the user who has the encryption key or password can decrypt the hidden file. This will ensure that unauthorized users are unable to read or view the hidden file.

4.3. To allow an authorized user to reveal any hidden file types

With FHWA, only authorized users can reveal the hidden files (any types). To develop this process, the reverse image steganography technique known as steganalysis is implemented. Both steganography and steganalysis are discussed below in this paper.

https://doi.org/10.15405/epms.2022.10.56
Corresponding Author: Noraliza Azizan
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

5. Research Methods

5.1. Steganography

Steganography refers to a method intended to hide interactions between the two communicators. The words steganography is composed specifically of Greek terms στεγανός, covered and γραφία, writing (Telsy, 2020). According to Taha et al. (2019), steganography defines as how a secret message is kept hidden in a cover message in such a manner that its existence is completely hidden. It is also can be referred to as the art or activity of hiding a file, image, audio, or message within another file which is image, audio, or video. The secret message could be in the form of a text file, an image, a ciphertext, or something that can be interpreted as a bit. Thus, the main objective of steganography is to communicate privately with secret information through the cover file.

Steganography can also be used in command and control protocols for malware, including reading content from image files accessible by sharing and social media platforms (Murphy, 2019). Therefore, the use of steganography is actually to hide confidential or secret data from unauthorized users. For example, information that is not supposed to be revealed to others can be protected using steganography. Sensitive information, such as financial records, can also be concealed in a cover object and stored on a private computer. It needs appropriate conditions to make steganography techniques effective (Lake, 2019).

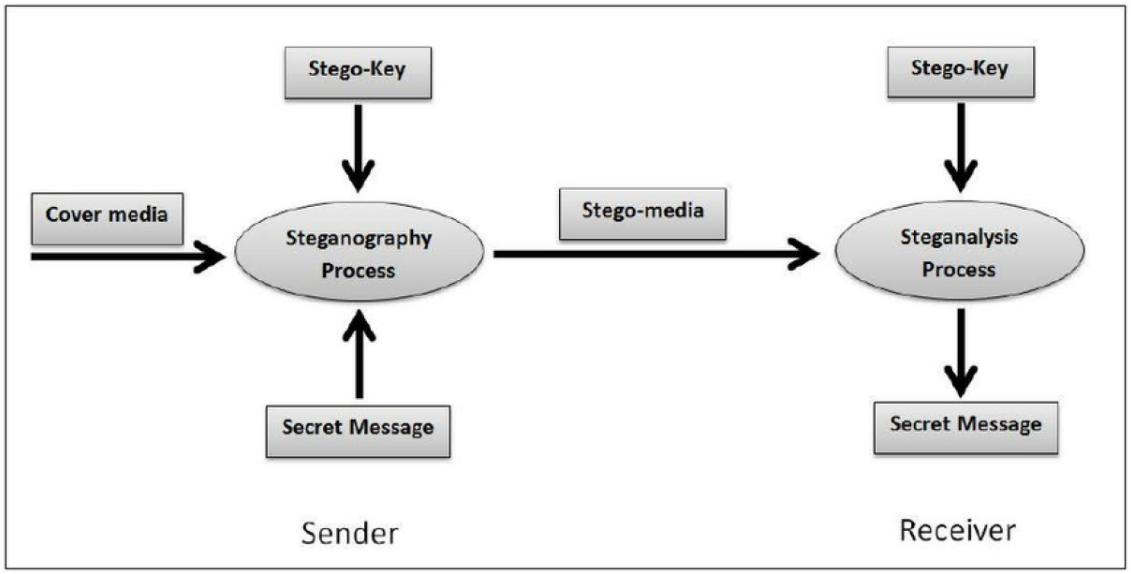


Figure 1. Main diagram of steganography (Al Sadi, 2015)

Figure 1 shows the process of steganography and steganalysis where it involves interaction between two individuals which are sender and receiver. The steganography process is executed when the sender hides the secret message by using a stego-key or password in a cover media such as an image. On the receiver site, the steganalysis process will be executed if the receiver has the stego-key and the secret message sent by the sender will be revealed.

https://doi.org/10.15405/epms.2022.10.56
Corresponding Author: Noraliza Azizan
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

Steganalysis is the process of identifying or discovering the secret messages or we can say it is the reverse process of steganography. Since FHWA includes this process to reveal the hidden message, steganalysis is one of the important processes in this development. This process aims to evaluate if the file or any other medium contains a secret message and if the result is positive, the hidden message contained in the medium can be revealed (Telsy, 2020).

In this application we used an image as a cover to hide the secret data. According to Ives (2017), there are several steganography techniques for hiding the data, however, with the intention of hiding files within images, only two methods were feasible which are hiding file data within the image data and adding file data together with the image data.

The first method replaces irrelevant image data with information to be concealed. Normally this approach works by hiding the data in the Least Significant Bits (LSB) of the image color component. Therefore, the size of the file shall remain the same as the data or secret message is just replaced, not added (Olomo Rachael, 2019). This will ensure that the steganography is tough to locate. However, only a very small amount of secret information can be covered in each image.

For the second method, it can retain full image quality thus increase the overall file size. By adding secret data to an unnoticed part of the file, such as after the logical end of the image, any amount of data can be concealed (Douglas et al., 2017). Therefore, the user may add secret data in the cover image without regarding the file size of the secret data which is different from hiding the data in the Least Significant Bits (LSB) where it can hide an only a small amount of secret information. However, this approach is easier to detect as the file size increases and the file can be analyzed to reveal secret information.

FHWA uses the second approach as it enables users to hide any number of files in the image, regardless of the image resolution. Besides that, FHWA uses end of file (EOF) markers to incorporate data that will not normally be found in an image format. The EOF markers for images file types include PNG: AE426082, JPEG: FFD9, and GIF: 3B. Hence, there should be no information after the EOF marker, so any data that is stored after the marker will be ignored by software when scanning the file. Other than that, we also implement the cryptography element in this development to secure the confidentiality of the hidden data.

5.2. Agile Development

FHWA make used of Agile Development methodology as shown in Figure 2. This approach prioritizes individual responsibility, short time frames for deliverables, consistent communication, feedback, and sustainable growth (Thattamparambil, 2020). This iterative agile approach is more versatile and its short-term iterations aim to develop the project on a small timeframe, with little preparation rather than a long-term strategy. It allows teams to adapt to randomness through systematic iterative work cycles, known as sprints (Azmee, 2017). Therefore, this method is very suitable and has been chosen for FHWA because it requires a short time to complete.

https://doi.org/10.15405/epms.2022.10.56
Corresponding Author: Noraliza Azizan
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

Figure 2. Agile development methodology phases

The planning and analysis phase mainly focuses on developing a plan according to the requirements which includes an analysis, design and testing plans to provide a clear path for the development process. This includes the construction of question to be asked in the questionnaire, which then have been distributed to 100 users (for user requirement). For analysis, we analyzed and identified the user requirements, system requirements and algorithms that will be implemented which are steganography and cryptography.

In second phase, we designed the flow of this application in the form of use case and flowchart diagram. We also designed the user interfaces which are simple, efficient, informative and user friendly.

After the best design has been selected, implementation started immediately by using several programming languages. We used Javascript like Node.js for backend while for frontend, Javascript library and framework such as ReactJS, Next.js were implemented. Specifically for User Interface (UI), we used Tailwind CSS, Semantic UI for designing the UI and we used MongoDB in setting up a database.

For testing phase, we implemented few testing which include unit, integration, system (both functional and non-functional) and user acceptance. In this paper, we will present the user acceptance testing results (from 60 respondents) as they can prove that FHWA can be used successfully in order to meet above objectives.

5.3. Design and Implementation

Figure 3 shows FHWA flowchart where it starts with entering the username and password to login to the system. The actors in this system are Administrator and Users. Administrator can manage users that have been registered in this system where they can view user details, add new users, update user details, and delete a user. Administrator also can perform the ‘hide files’ and ‘reveal files’ functions.

https://doi.org/10.15405/epms.2022.10.56
Corresponding Author: Noraliza Azizan
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

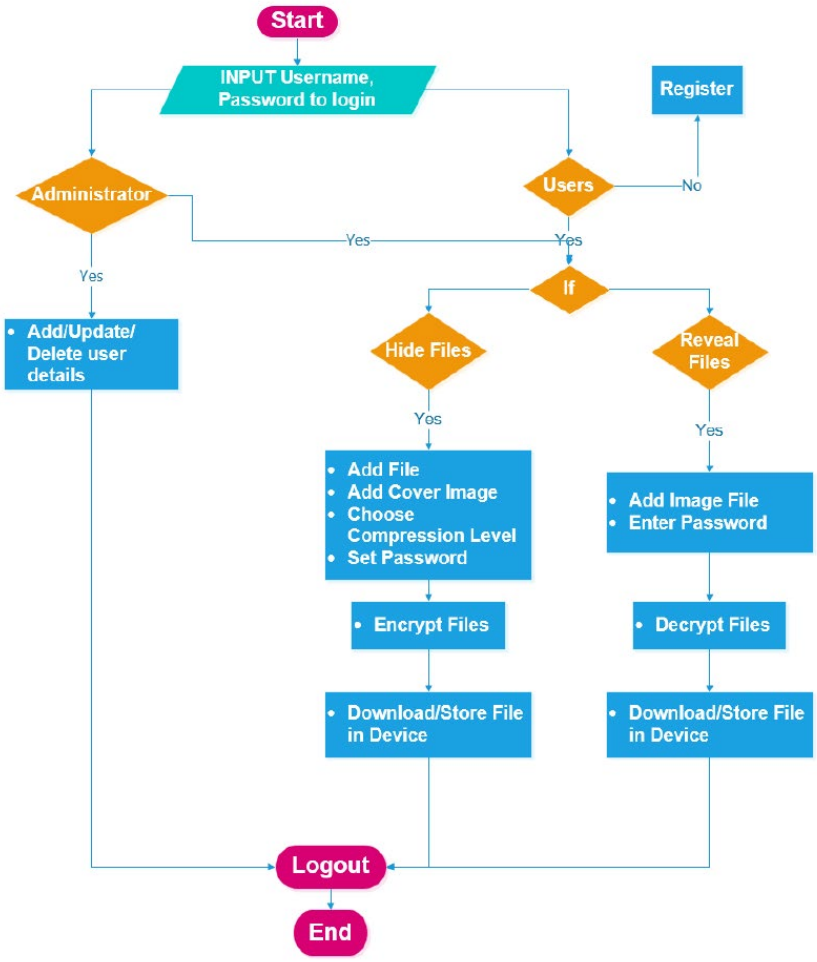


Figure 3. Flowchart diagram

For normal users, if they did not have a username and password to log in, they can proceed to the registration page. Once successfully registered, they can log in and proceed to hide files or reveal files. If the users choose to hide a file, then they must add any file that they want to keep confidential, add a cover image, choose the compression level, and set a password to encrypt the confidential file. After that, the process of hiding and encrypting the files should be successful. Then, users can proceed to download and store the file in their device or local storage.

If the users choose to reveal files, then they must add an image file that contains a secret file and enter the same password used to encrypt the secret files. After that, the process of revealing and decrypting the files should be successful. Users can also proceed to download and store the file in their device or local storage. Lastly, if administrators and users want to end the application sessions, they can log out from the system.

FHWA involves two main processes which are hiding files and revealing secret files. These processes use few algorithms and the steps of the processes are discussed below:

- Hiding the files

i. First, the image is read and all files will be read as an array buffer using FileReaderAPI. Then, the image will be converted into a Uint8Array which an array of 8-bit unsigned integers.

https://doi.org/10.15405/epms.2022.10.56
Corresponding Author: Noraliza Azizan
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

ii. Then, the files are archived using JSZip (a javascript library) to allow the compression process. The output of the ZIP file will be hidden inside the image.

iii. Next, to encrypt the ZIP files, the system uses SubtleCrypto API and encryption algorithm named symmetric Advanced Encryption Standard Counter Mode (AES-CTR). In this process, the plaintext password is imported to create a derivation key. Secure Hash Algorithm – 256 Bit (SHA-256) and a salt are used to hash the derivation key. The salt which is Uint8Array is taken from the start of the image to prevent a dictionary attack of passwords. Then, a new key is derived using Password-Based Key Derivation Function 2 (PBKDF2) algorithm and the files can be encrypted by using the new encryption key.

iv. After encrypting the ZIP files, the output is converted to another Uint8Array.

v. Now, the files are being hidden inside the image and being converted to a blob then it can be download and stored to the user's devices or local storage.

- Revealing the files

This process is similar to the hiding process but in the reverse step.

i. First, the file will be converted to a Uint8Array and read using the FileReader API.

ii. After the EOF marker has been discovered by iterating through the array, the files are immediately retrieved and followed the EOF marker. If no content follows the EOF marker, the image does not include any hidden files.

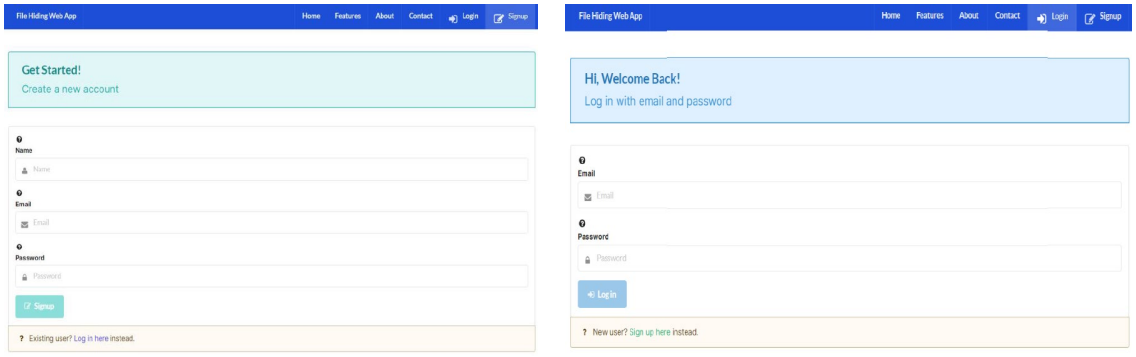
iii. The decryption technique to hide the ZIP file is the same as the technique used in the encryption process. However, to derive decryption, the derivation key is used with the AES-CTR algorithm to decrypt the data.

iv. After the ZIP file has been decrypted, JSZip is used to extract the files.

v. Finally, the extracted ZIP files that contain hidden messages or files can be downloaded and stored on user devices or local storage.

6. Findings

6.1. Interface Design

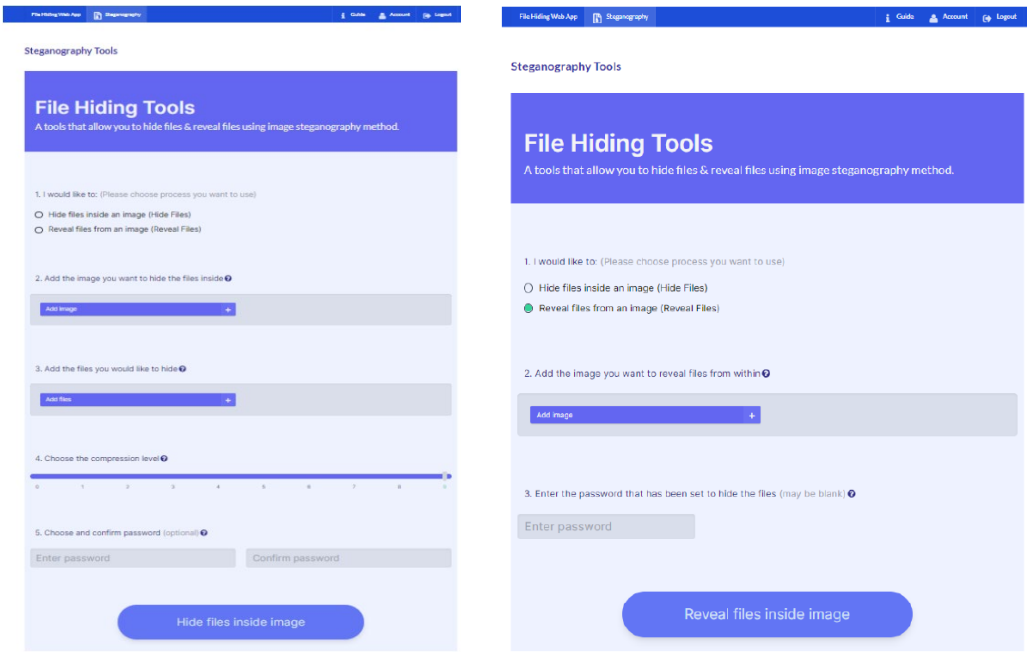


(a) (b)

Figure 4. (a) & (b) Sign-up and login interface

https://doi.org/10.15405/epms.2022.10.56
Corresponding Author: Noraliza Azizan
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

Figure 4 (a) shows sign-up page and Figure 4 (b) shows the login page of FHWA system. The sign-up page provides three information that needs to be filled in by the users which are the name, email, and password. If all the information that has been filled in is valid, a user should successfully be registered into the system after they click the 'Signup' button. Then, users can login to the system by filling the registered email and password.



(a) (b)

Figure 5. (a) & (b) Hiding and revealing files interface

Figure 5 (a) shows hiding files page and Figure 5 (b) shows the revealing files page of FHWA system. To hide files inside the image, users must click a radio button that is provided in question one which is the 'hide files inside an image'. After click it, users must click the 'Add files' button to add the files that they want to hide and choose the compression level to compress the files. The system also provides the user to set the password to encrypt the files. Then, click 'Hide files inside image' button and download button will be available. Users need to click the button to download and store the image files that contain hidden files into the user's devices or local storage.

To run the revealing files process, users must click a radio button that is provided in question one which is the 'Reveal files from an image'. Then, user can click 'Add image' button to add the image that they want to reveal the files from within and enter the same password that has been set. Click the 'Reveal files inside image' button and download button will be available. User must click the download button to download and store the hidden or revealed files into the user's devices or local storage.

6.2. User Acceptance Testing Result

Out of 100 questionnaires distributed to users, 60 were completed and used for this analysis.

https://doi.org/10.15405/epms.2022.10.56
Corresponding Author: Noraliza Azizan
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

Table 1. User acceptance testing

No.	Factor	Strongly Agree
1.	I can login and register into the application.	100%
2.	I am able to set a password to encrypt their hidden files inside an image file.	100%
3.	I (Authorized user only) can hide any file type inside an image file.	95%
4.	I (Authorized user only) can read, view or reveal the hidden files inside the image only by entering the correct password.	95%
5.	I can run the application smoothly.	100%
	Average	**98%**

Based on Table 1, we found that 100% of respondents can login and register into FHWA. Table 1 has shown an evidence which all of the respondents were able to set a password to encrypt their hidden files inside an image. FHWA shows that 95% of its respondents can hide their confidential files and can reveal the hidden files afterwards using image steganography technique. The remaining 5% were just not so sure what they have accomplished. This may be due to knowledge gap in information technology or it can be due to unfriendly user interface itself.

Since security is very important in this application, we asked the users to enter the correct and the incorrect passwords when revealing the hidden files. From Table 1, we can see that 95% of the respondents cannot reveal the hidden files inside the image without entering the correct password. Thus, it proves that the security feature was successfully implemented in FHWA

Table 1 also shows that all of the respondents agreed with this application where it runs smoothly. On average, we can say 98% of the respondents strongly agree that FHWA met its objectives.

7. Conclusion

Information security is vital to most organizations and even personal computer users. Customer data, financial records, personal data, bank account details, all of this data can be difficult to replace and possibly dangerous if it falls into the unauthorized person. According to Rout and Mishra (2014), it is frustrating if these data is lost due to disasters and calamities but losing it to hackers or malware attacks can have much greater implications.

With FHWA, users are able to hide any confidential file types inside an image and reveal them afterwards using encryption and image steganography techniques successfully. Thus, FHWA may help in solving the need to use more than one application when hiding any type of files from unauthorized users.

However, there are many more features that can be introduced such as building a mobile application. Today, smartphone is an important device in digital community. By developing the mobile application, users can obtain better experience and interaction when hiding confidential files in their mobile devices.

In addition, this application could be improvised by enabling user to save the image file that contains the confidential files themselves inside the user's cloud storage such as Google Drive. With this feature users can easily access their confidential files anytime, anywhere they wish.

https://doi.org/10.15405/epms.2022.10.56
Corresponding Author: Noraliza Azizan
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

Acknowledgments

We would like to thanks to Research Management Centre (RMC) of Kolej Universiti Poly-Tech MARA (KUPTM) for funding received under University Research Grant (URG).

References

Al Sadi, G. (2015). Image Steganography Approach. *International Journal of Computer Science and Mobile Computing*, *4*(8), 166–169. https://www.researchgate.net/publication/286452501_Image_Steganography_Approach

Azmee, H. (2017). Agile Methodology. *Academia*. Retrieved on October 3, 2020, from https://www.academia.edu/4383136/Agile_Methodology

Douglas, M., Bailey, K., Leeney, M., & Curran, K. (2018). An overview of steganography techniques applied to the protection of biometric data. *Multimedia Tools and Application, 77*, 17333–17373. https://doi.org/10.1007/s11042-017-5308-3

Ives, G. (2017). StegaPhoto. *Greg Ives.* Retrieved on October 3, 2020, from https://gregives.co.uk/projects/stegaphoto/

Jang-Jaccard, J., & Nepal S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*(5), 973-993. https://doi.org/10.1016/j.jcss.2014.02.005

Kessler, G. C. (2015). *An Overview of Steganography for the Computer Forensics Examiner*. Retrieved on October 3, 2020, from https://www.garykessler.net/library/fsc_stego.html

Lake, J. (2019). *What is steganography and how does it differ from cryptography?* Retrieved on October 3, 2020, from https://www.comparitech.com/blog/information-security/what-is-steganography/

Murphy, R. (2019, April 9). Steganography in the Modern Attack Landscape. *Vulners.com*. Retrieved on October 3, 2020, from https://vulners.com/carbonblack/CARBONBLACK:C186AD26DF614CF07B9F101FD1A259BF?utm_source=rss&utm_medium=rss&utm_campaign=rss

Olomo Rachael, S. M. (2019). Image Steganography and Steganalysis Based on Least Significant Bit (LSB). *Proceeding of ICTIT* (pp. 1100-1111). Springer Link.

Rout, H., & Mishra, B. K. (2014). Pros and Cons of Cryptography, Steganography and Perturbation techniques. *IOSR Journal of Electronics and Communication Engineering*.

Semilof, M., & Clark, C. (2018). *What is steganography*. Retrieved on October 3, 2020, from https://www.techtarget.com/searchsecurity/definition/steganography

Shafiee, A. N. (2020). *File Hiding Web Application.* KUPTM.

Stone, D. (2017). *What Causes a File to Suddenly Disappear?*. Retrieved October on 4, 2020, from https://smallbusiness.chron.com/causes-file-suddenly-disappear-74023.html

Taha, M. S., Mohd Rahim, M. S., Lafta, S. A., Hashim, M. M., & Alzuabidi, H. M. (2019). Combination of Steganography and Cryptography: A short Survey. *IOP Conference Series: Materials Science and Engineering, 518*(5)*,* 1-13. https://iopscience.iop.org/article/10.1088/1757-899X/518/5/052003

Telsy (2020, June 25). *Steganography: From Its Origins to the Present*. Retrieved on October 4, 2020, from https://www.telsy.com/steganography-from-its-origins-to-the-present

Thattamparambil, N. (2020, February 17). How to choose the research methodology best suited for your study. *Editage Insights*. Retrieved on October 3, 2020, from https://www.editage.com/insights/how-to-choose-the-research-methodology-best-suited-for-your-study?refer=scroll-to-1-article&refer-type=article