International Journal of Synergy in Engineering and Technology
UNIVERSITY COLLEGE TATI
IJSET

Development of Image Shredder Tool

Wan Ainul Alyani Wan Mohamed, Akhyari Nasir, Ahmad Daniel Mohamad Hatta*

Faculty Computer Media and Technology Management, UC TATI, Kemaman, Terengganu.
*Corresponding author: ainualyani@uctati.edu.my

KEYWORDS

Image Shredder Tool
Multimedia Security
Image Distortion

ABSTRACT

Image media distortion is a process which media is damaged so that it cannot be viewed any longer. The tool distorts the image by overwriting metadata header. Even with a single overwritten data, the image will be damaged. Consequently, a tool that allows to make corrupted images restorable even after being deleted in Recycle Bin is important to be developed because there are numerous risks that people might face if personal photos are leaked to the wrong hand. Thus, the objective of this paper is to develop a tool in shredding several types of image media. PADI model involves four phases including Planning, Analysis, Development and Implementation in developing the tool. As a result, all image file types that has been chosen can be shredded using Image Shredder Tool. Some of the file types can be viewed by Image Shredder Tool and can be shredded using Image Shredder Tool. The file types are BMP, GIF, JPEG, PNG and TIFF.

1.0 INTRODUCTION

In this digital era, users in cyberspace does not really concern about image security (B., Holi, & Murthy, 2016). Today, various people utilize the distinctive applications to image data transfer. Most people, by far, use their images for various customers using the social application. The attacks on these social applications include copying or hacking important data. In fact, it normally happens to users who use their mobile phones, tablets, etc. Thus, the objective of this paper aims to develop a shredder tool to fight these attacks.

The security frameworks used is either encryption or steganography, or the combination of both. There is diverse securable image encryption that is made especially for protection against unauthorized access. Any transfer over the internet has important data such as military, security associations, social or adaptable applications. Hence image security is necessary. The commonly used security mechanisms are DFT, DCT, DWT, etc. The transfer of image using unsecured network will pose following attacks such as active and passive attacks. Active attacks consist of few data stream modification or false data stream creation. Meanwhile, passive attacks use the data but do not affect the system resources.

For instance, users in cyberspace are not aware about the dangers of image theft. If personal photo gets stolen, the thief can do horrible things which include blackmailing for sexual desire. When an image media is deleted in a device such as laptop or computer or even deleted in the

Received April 2021; received in revised form May 2021; accepted June 2021.

Recycle Bin, it can be recovered by someone who has advanced computer knowledge. Hence, a data sanitization tool ensures an image cannot be used even when it is recovered after being deleted in the Recycle Bin. As a result, it is important to be develop a tool to prevent that as it poses numerous risks like hackers obtaining your photos for the wrong reasons.

A data sanitization method is the specific way a data destruction program or file shredder overwrites the data on a hard drive or other storage device. Data sanitization methods are often referred to as data erasure methods, data wipe methods, wipe algorithms, and data wipe standards. Most data destruction programs support multiple data sanitization methods (Diego Galar, 2017).

1.1 Techniques

There are four techniques used to distort an image media will discussed in this paper for examples: Steganography, Write Zero, DoD 5220.022-M and Gutman method:

a. Steganography

Steganography is the art of hiding the fact that communication is taking place, by hiding a piece of information in another information. In this case, many different carrier file formats can be used, but digital images are the most popular ones as they are frequently used on the Internet. For hiding secret information in images, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the steganography technique used (Morkel, Eloff, Olivier, 2005).

Although Steganography technique can distort an image media and can be used for this project, there are still some problems regarding this technique. Although this technique distorts an image by completely altering the image, the main structure of the original image is still there. In addition, this technique is more complex to be implemented than the shredding method.

b. Write Zero

Write Zero data sanitization method may not stop the most advanced hardware-based recovery methods from extracting at least some of the deleted data, but it is likely to prevent all software-based file recovery methods from lifting information from the drive (Fisher, 2016). The Write Zero data sanitization method is, expectedly, implemented in the following way:

Pass 1: Writes a Zero

Write Zero uses only one character to overwrite data in the disk. It is enough to sanitize file in a disk but not really efficient. This is because if only a single write pass is done, and the software does not verify that every piece of erased data, then the method is not going to be as effective as other methods that do. As quoted in an article titled ‘What Is the Write Zero Method?’ by lifewire.com, “if using a Write Zero on one drive and it verifies that all the data has been overwritten, then you can be confident that the information is less likely to be recovered than if the same data were overwritten with the Random Data method but did not verify that each sector was replaced with random characters.”

c. DoD 5220.022-M

The DoD 5220.22-M is a software-data sanitization method used in various file shredder and data destruction programs to overwrite existing information on a hard drive or other storage device (Fisher, 2016). The DoD 5220.22-M data sanitization method is usually implemented in the following way:

Pass 1: Writes zero and verifies the write.
Pass 2: Writes one and verifies the write.
Pass 3: Writes a random character and verifies the write.

DoD 5220.22-M is an efficient way to sanitize data but there is too much phase in overwriting data. This method might take a period of time to finish processing a single file especially if the file is big. As quoted by lifewire.com in an article titled 'DoD 5220.22-M Data Wipe Method [US DOD Wipe Standard]', for a large hard drive, Write Zero usually take much less time to finish than DoD 5220.22-M, which will be much quicker than one like Gutmann which might run through over 30 passes."

d. Gutmann method

The Gutmann method was developed by Peter Gutmann in 1996. It is one of the sanitization methods to shred files and destruct data. This method also overwrites the existing data on a hard disk or any other storage device (Fisher, 2016). The Gutmann data sanitization method is often implemented in the following way:

Pass 1-35: Writes a random character. But then uses a complex pattern of overwriting from Pass 5 to 31.

Gutmann method were developed way back in late 1900 which made it incompatible with the latest hard drives or in simpler words, this method is outdated. As quoted by lifewire.com, "the hard drives in use at that time used different encoding methods than the ones were used today, so most of the passes the Gutmann method performs are completely useless for modern hard drives." This method has been acknowledged by Gutmann himself to be obsolete on modern drives since hard drive technology has changed vastly since he initially developed it.

2.0 EXPERIMENTAL PROCEDURE

Development of Image Shredder Tool was developed based on Planning, Analyzing Information, Design, Implementation (PADI) model process. The significance of this method is that it is more compatible to be used with this application. Additionally, all of the project's requirement and flow chart had been identified. After that, all tool interfaces are being design to show the overall connection and flow of the system. This section of discusses four fundamental phases as Figure 1.

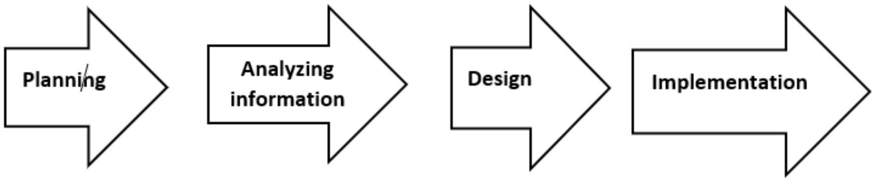


Figure 1: PADI Model Process

2.1 Planning

First and foremost, information regarding image theft is gathered from related article and research paper about how dangerous it is if our photo were stolen by someone with malicious intent. That being said, it was decided after that to create a tool that ensures an image to be unreadable even after it is being deleted from the device's Recycle Bin. The flow process is showed in Figure 2. When the tool is launched, the interface of the tool will appear to the user. Next, the user can browse through the image media from their device to find and select desired image to be shred. After the user upload the image that they specifically want to be sanitized, the image will be displayed on the picture box labeled, "Image Display" on the interface. Then, the user can confirm the selected image and click on the "start" button to begin shredding process on the image file. If the process has completed successfully, the picture box will display a broken file icon on the "image display" box. If it unsuccessful, the user will be notified.

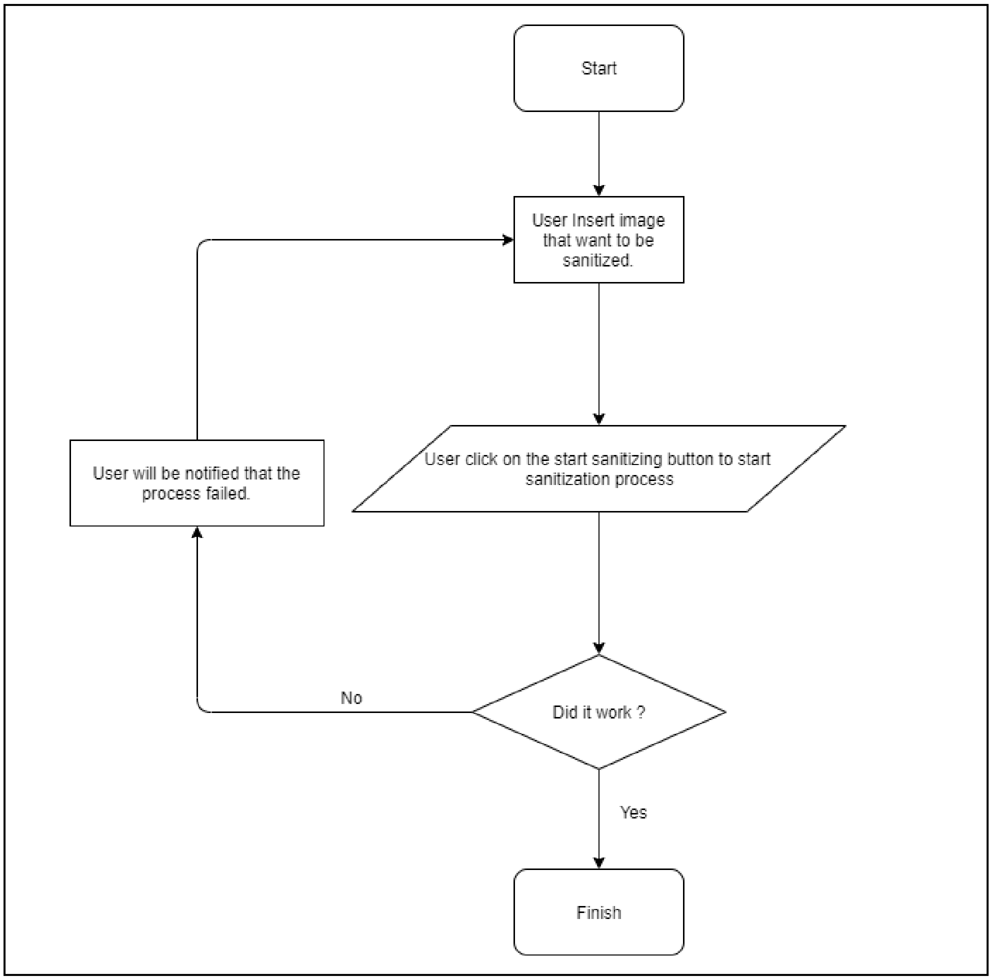

Start
User Insert image that want to be sanitized.
User click on the start sanitizing button to start sanitization process
User will be notified that the process failed.
Did it work ?
No
Yes
Finish

Figure 2: Flowchart for Travel Agent module

Figure 3, Figure 4 and Figure 5 below shows the storyline of how the planned interface is successful and failed Image Media Shredder.

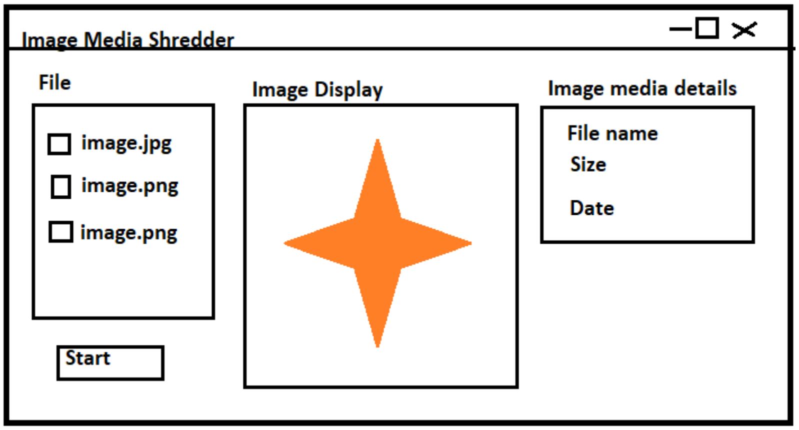
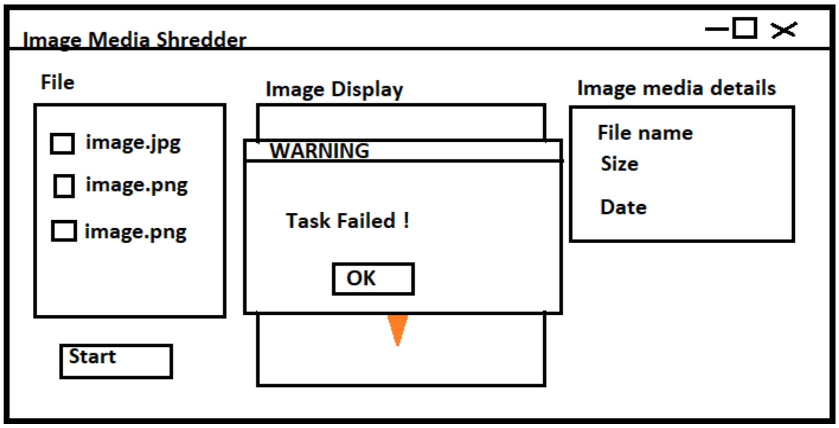


Figure 3 Planned interface



Task Failed !

Figure 4 If the process failed

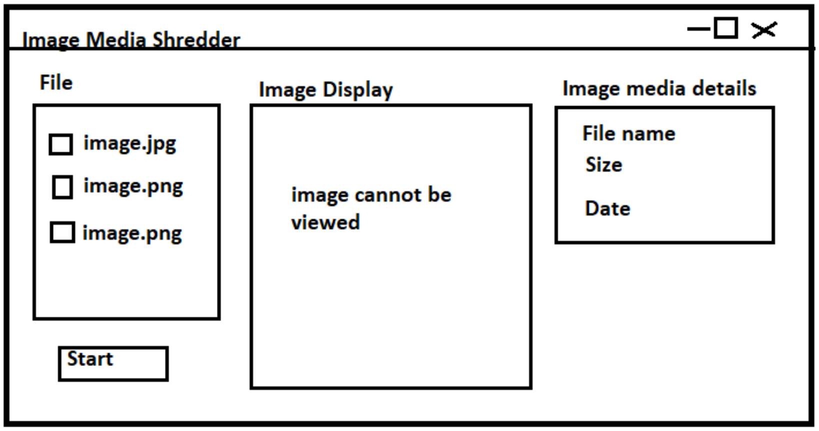


image cannot be viewed

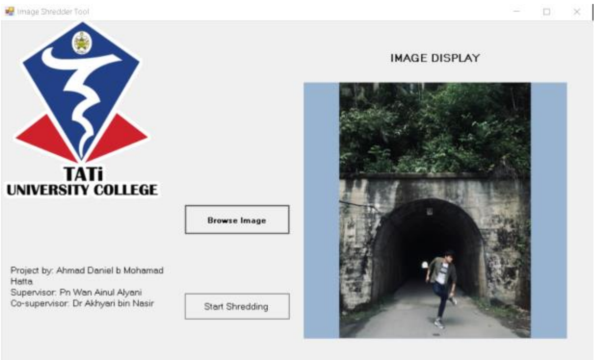
Figure 5 If the process successful

2.2 Analyzing Information

After that, the information gathered is analyzed to reveal possible solutions to help reduce cases on image theft from transpiring. There are several methods that can be implemented into the tool such as Dod, random number and steganography. After analyzing all the methods that could be used, finally write zero method is chosen. However, instead of inserting just a single 0 into the file image structure, the tool inserted a symbol to indicate that the file is completely broken and cannot be used or viewed anymore.

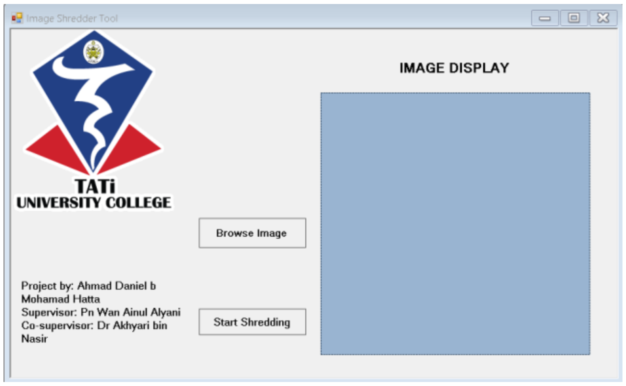
2.3 Design

This project was created using SharpDevelop 5.1 which uses C# coding language. SharpDevelop 5.1 does not require any log in information to be used. The Graphical User Interface (GUI) for the application was designed properly with its appropriate components in attractive manner as shown in Figure 6 and Figure 7.



Project by: Ahmad Daniel b Mohamad Hatta
Supervisor: Pn Wan Ainul Alyani
Co-supervisor: Dr Akhyari bin Nasir

Figure 6 Image shredder tool after uploading an image file



Project by: Ahmad Daniel b Mohamad Hatta
Supervisor: Pn Wan Ainul Alyani
Co-supervisor: Dr Akhyari bin Nasir

Figure 7 Image Shredder Tool after the image is being shred

2.4 Implementation

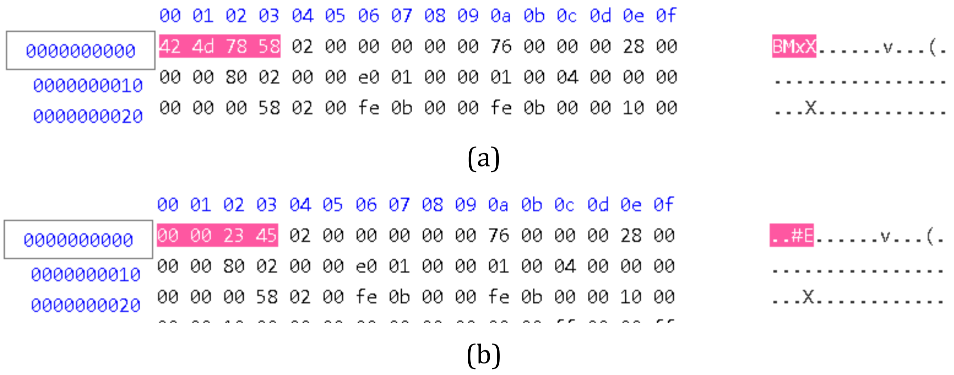
This phase is done after designing the interface. Image Shredder Tool development method was chosen to be employed which the tool needs to view the selected image file. Using SharpDevelop 5.1, the project is implemented by inserting the C# coding language.

3.0 RESULTS AND DISCUSSION

The findings of this project include the effectiveness of this tool in shredding several image media files. The image media file types that have been used are Bitmap Image (BMP), Graphic Interchange Format (GIF), Joint Photographic Expert Group (JPEG), Portable Network Graphic (PNG), Tagged Image File Format (TIFF), Portable Document Format (PDF), Scalable Vector Graphic (SVG),) and WEBP or pronounced as "Weppy". The data was presented in the form of figures for a clear and accurate results from the tool.

3.1 Bitmap Image (BMP)

Windows BMP is the native image format in Microsoft Windows operating systems. It supports images with 1, 4, 8, 16, 24, and 32 bits per pixel, although BMP files used are 16 and 32 bits per pixel. Besides, BMP also supports simple run-length compression for 4 and 8 bits per pixel. However, BMP compression is only used with large blocks with identical colours, making it very limited in value. It is rare for Windows BMP to be in a compressed format. Figure 8 shows the result of hex for original image of BMP and after shredding processing:



```
            00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
0000000000  42 4d 78 58 02 00 00 00 00 00 76 00 00 00 28 00    BMxX......v...(.
0000000010  00 00 80 02 00 00 e0 01 00 00 01 00 04 00 00 00    ................
0000000020  00 00 00 58 02 00 fe 0b 00 00 fe 0b 00 00 10 00    ...X............
```

(a)

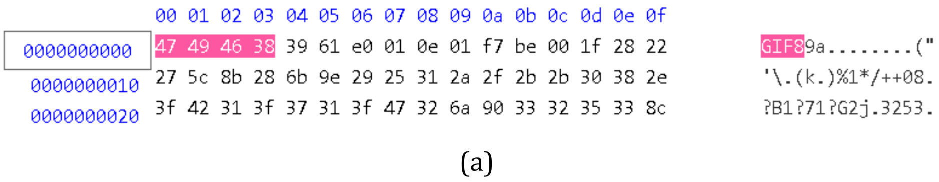
```
            00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
0000000000  00 00 23 45 02 00 00 00 00 00 76 00 00 00 28 00    ..#E......v...(.
0000000010  00 00 80 02 00 00 e0 01 00 00 01 00 04 00 00 00    ................
0000000020  00 00 00 58 02 00 fe 0b 00 00 fe 0b 00 00 10 00    ...X............
```

(b)

Figure 8: (a) The hex results for original image of BMP before the shredding process (b) The hex results for image of BMP after the shredding process

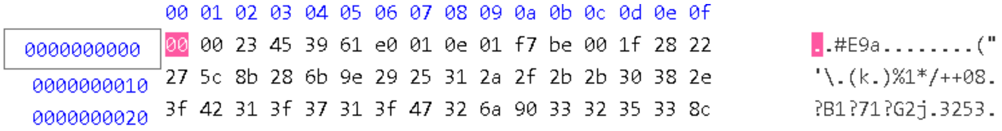
3.2 Graphic Interchange Format (GIF)

The GIF file format supports the 8-bit color graphics method of storing image information, where each pixel is represented by an 8-bit byte. This way, GIF makes it possible for a single image to refer to a palette of 256 different colors within the 24-bit RGB color space at any time. GIF is used mainly for storing plain images such as graphics or logos featuring solid areas of uniform color and well-defined edges. Figure 9 shows the result of hex for original image of GIF and after shredding process:



```
            00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
0000000000  47 49 46 38 39 61 e0 01 0e 01 f7 be 00 1f 28 22    GIF89a........("
0000000010  27 5c 8b 28 6b 9e 29 25 31 2a 2f 2b 2b 30 38 2e    '\.(k.)%1*/++08.
0000000020  3f 42 31 3f 37 31 3f 47 32 6a 90 33 32 35 33 8c    ?B1?71?G2j.3253.
```

(a)



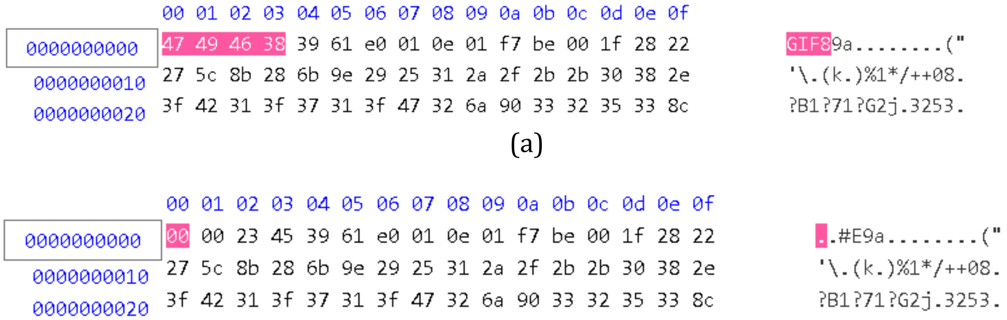
```
            00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
0000000000  00 00 23 45 39 61 e0 01 0e 01 f7 be 00 1f 28 22      ..#E9a........("
0000000010  27 5c 8b 28 6b 9e 29 25 31 2a 2f 2b 2b 30 38 2e      '\.(k.)%1*/++08.
0000000020  3f 42 31 3f 37 31 3f 47 32 6a 90 33 32 35 33 8c      ?B1?71?G2j.3253.
```

(b)

Figure 9: (a) The hex results for original image of GIF before the shredding process (b)The hex results for image of GIF after the shredding process

3.3 Joint Photographic Expert Group (JPEG)

JPEG is a lossy compression algorithm that has been constructed for the purpose of decreasing the file size of natural, photographic-like true-color images to the maximum possible extent without degrading the visual quality of the image in terms of human perception. Figure 10 shows the result of hex for original image of JPEG and after shredding process:



```
            00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
0000000000  47 49 46 38 39 61 e0 01 0e 01 f7 be 00 1f 28 22      GIF89a........("
0000000010  27 5c 8b 28 6b 9e 29 25 31 2a 2f 2b 2b 30 38 2e      '\.(k.)%1*/++08.
0000000020  3f 42 31 3f 37 31 3f 47 32 6a 90 33 32 35 33 8c      ?B1?71?G2j.3253.
```

(a)

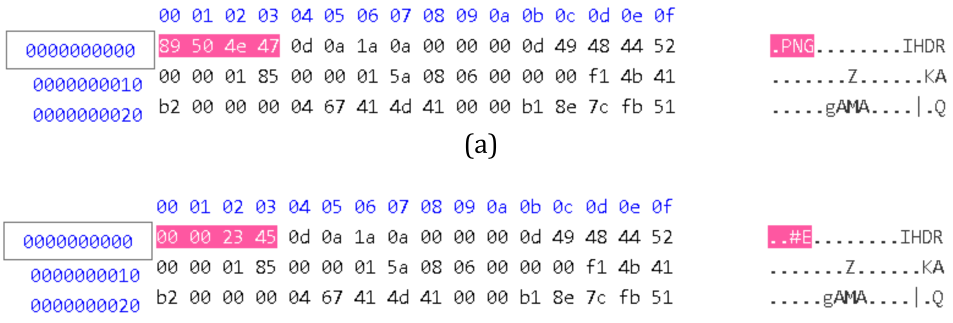
```
            00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
0000000000  00 00 23 45 39 61 e0 01 0e 01 f7 be 00 1f 28 22      ..#E9a........("
0000000010  27 5c 8b 28 6b 9e 29 25 31 2a 2f 2b 2b 30 38 2e      '\.(k.)%1*/++08.
0000000020  3f 42 31 3f 37 31 3f 47 32 6a 90 33 32 35 33 8c      ?B1?71?G2j.3253.
```

(b)

Figure 10: (a) The hex results for original image of JPEG before the shredding process (b)The hex results for image of JPEG after the shredding process

3.4 Portable Network Graphic (PNG)

PNG is designed to work well in online viewing applications, such as the World Wide Web, so it is fully streamed with a progressive display option. PNG is robust, providing both full file integrity checking and simple detection of common transmission errors. Additionally, PNG can store gamma and chromaticity data for improved color matching on heterogeneous platforms. Figure 11 shows the result of hex for original image of PNG and after shredding processing:



```
            00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
0000000000  89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52      .PNG........IHDR
0000000010  00 00 01 85 00 00 01 5a 08 06 00 00 00 f1 4b 41      .......Z......KA
0000000020  b2 00 00 00 04 67 41 4d 41 00 00 b1 8e 7c fb 51      .....gAMA....|.Q
```

(a)

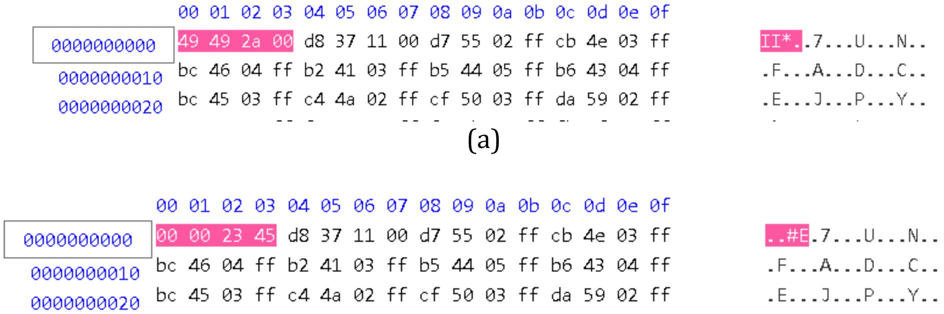
```
            00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
0000000000  00 00 23 45 0d 0a 1a 0a 00 00 00 0d 49 48 44 52      ..#E........IHDR
0000000010  00 00 01 85 00 00 01 5a 08 06 00 00 00 f1 4b 41      .......Z......KA
0000000020  b2 00 00 00 04 67 41 4d 41 00 00 b1 8e 7c fb 51      .....gAMA....|.Q
```

(b)

Figure 11: (a) The hex results for original image of PNG before the shredding process (b)The hex results for image of PNG after the shredding process

3.5 Tagged Image File Format (TIFF)

Tagged Image File Format or TIFF is a tag-based image file format developed for storing and interchanging bitmap images originating from scanner and desktop publishing applications. Figure 12 shows the result of hex for original image of TIFF and after shredding process:



```
            00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
0000000000  49 49 2a 00 d8 37 11 00 d7 55 02 ff cb 4e 03 ff      II*..7...U...N..
0000000010  bc 46 04 ff b2 41 03 ff b5 44 05 ff b6 43 04 ff      .F...A...D...C..
0000000020  bc 45 03 ff c4 4a 02 ff cf 50 03 ff da 59 02 ff      .E...J...P...Y..
```

(a)

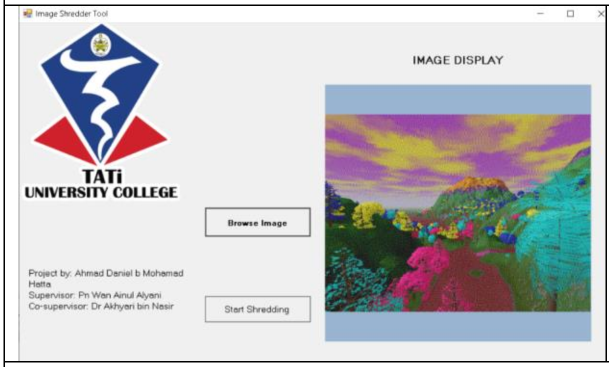
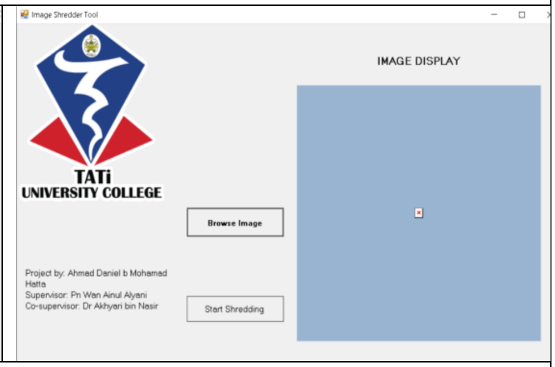
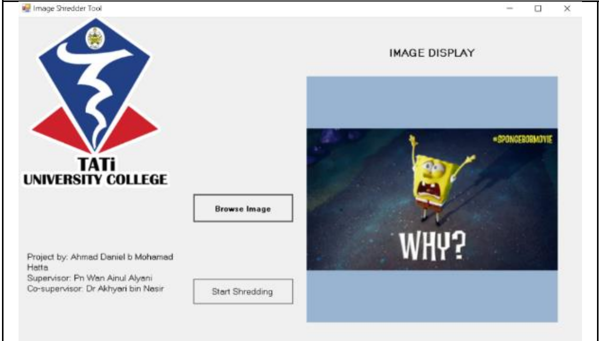
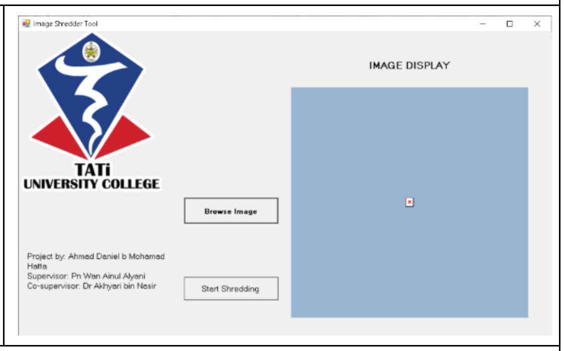
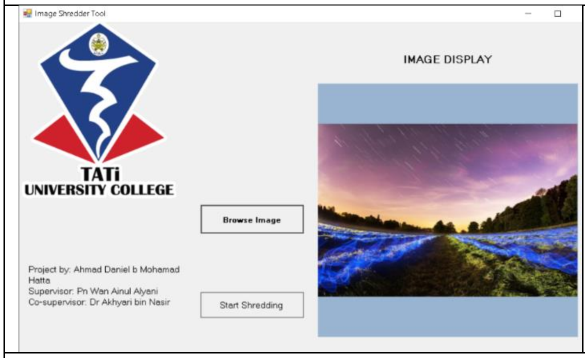
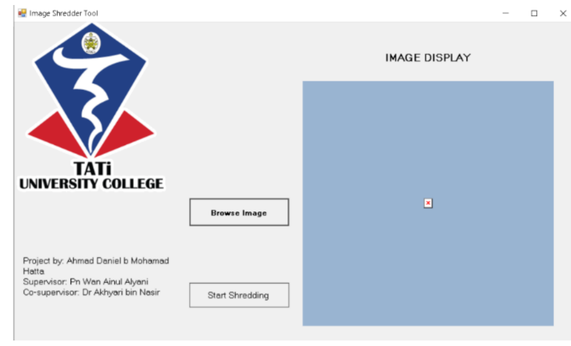
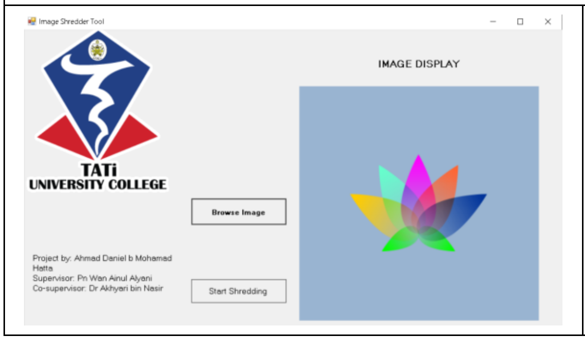
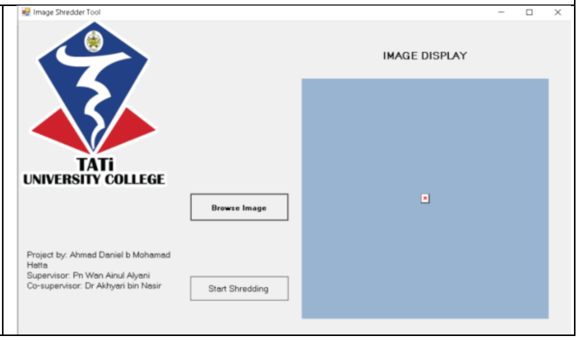
```
            00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
0000000000  00 00 23 45 d8 37 11 00 d7 55 02 ff cb 4e 03 ff      ..#E.7...U...N..
0000000010  bc 46 04 ff b2 41 03 ff b5 44 05 ff b6 43 04 ff      .F...A...D...C..
0000000020  bc 45 03 ff c4 4a 02 ff cf 50 03 ff da 59 02 ff      .E...J...P...Y..
```

(b)

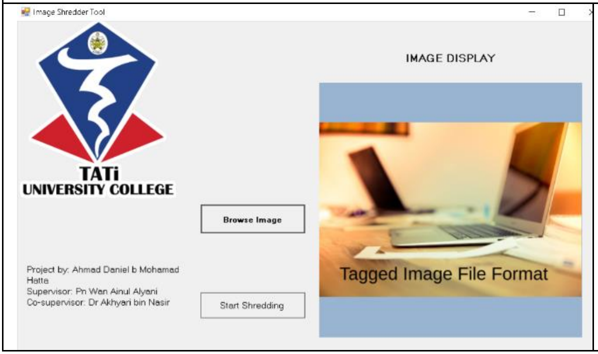
Figure 12: (a) The hex results for original image of TIFF before the shredding process (b)The hex results for image of TIFF after the shredding process

Table 1below shows the comparison before and after the image media file types of BMP, GIF, JPEG, PNG and TIFF being shredded using Image Shredded Tool.

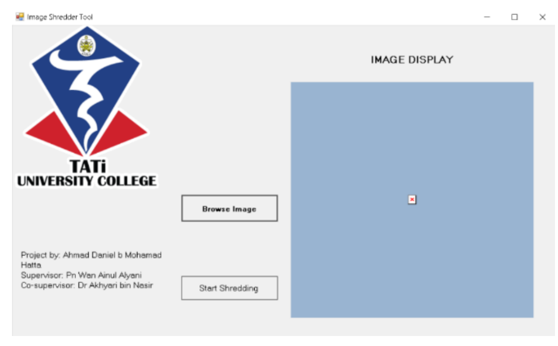
Table 1

BMP	
 Image Shredder Tool TATi UNIVERSITY COLLEGE IMAGE DISPLAY Browse Image Start Shredding Project by: Ahmad Daniel b Mohamad Hatta Supervisor: Pn Wan Ainul Alyani Co-supervisor: Dr Akhyari bin Nasir	 Image Shredder Tool TATi UNIVERSITY COLLEGE IMAGE DISPLAY Browse Image Start Shredding Project by: Ahmad Daniel b Mohamad Hatta Supervisor: Pn Wan Ainul Alyani Co-supervisor: Dr Akhyari bin Nasir
GIF	
 Image Shredder Tool TATi UNIVERSITY COLLEGE IMAGE DISPLAY #SPONGEBOBMOVIE WHY? Browse Image Start Shredding Project by: Ahmad Daniel b Mohamad Hatta Supervisor: Pn Wan Ainul Alyani Co-supervisor: Dr Akhyari bin Nasir	 Image Shredder Tool TATi UNIVERSITY COLLEGE IMAGE DISPLAY Browse Image Start Shredding Project by: Ahmad Daniel b Mohamad Hatta Supervisor: Pn Wan Ainul Alyani Co-supervisor: Dr Akhyari bin Nasir
JPEG	
 Image Shredder Tool TATi UNIVERSITY COLLEGE IMAGE DISPLAY Browse Image Start Shredding Project by: Ahmad Daniel b Mohamad Hatta Supervisor: Pn Wan Ainul Alyani Co-supervisor: Dr Akhyari bin Nasir	 Image Shredder Tool TATi UNIVERSITY COLLEGE IMAGE DISPLAY Browse Image Start Shredding Project by: Ahmad Daniel b Mohamad Hatta Supervisor: Pn Wan Ainul Alyani Co-supervisor: Dr Akhyari bin Nasir
PNG	
 Image Shredder Tool TATi UNIVERSITY COLLEGE IMAGE DISPLAY Browse Image Start Shredding Project by: Ahmad Daniel b Mohamad Hatta Supervisor: Pn Wan Ainul Alyani Co-supervisor: Dr Akhyari bin Nasir	 Image Shredder Tool TATi UNIVERSITY COLLEGE IMAGE DISPLAY Browse Image Start Shredding Project by: Ahmad Daniel b Mohamad Hatta Supervisor: Pn Wan Ainul Alyani Co-supervisor: Dr Akhyari bin Nasir

TIFF



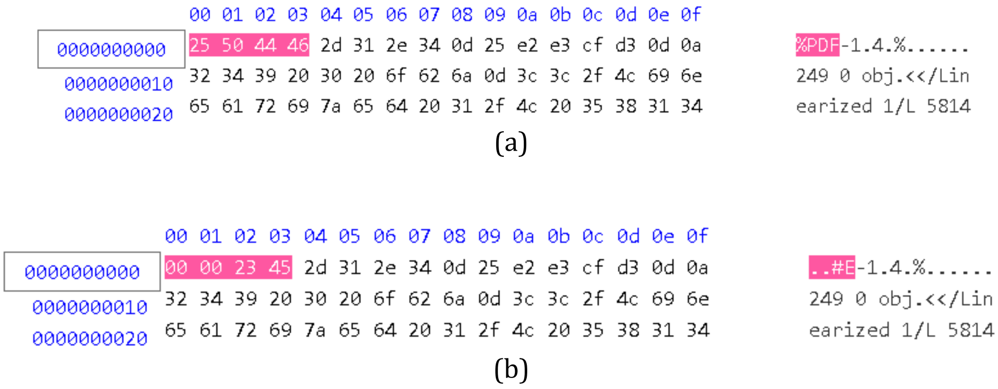
Project by: Ahmad Daniel b Mohamad Hatta
Supervisor: Pn Wan Ainul Alyani
Co-supervisor: Dr Akhyari bin Nasir



Project by: Ahmad Daniel b Mohamad Hatta
Supervisor: Pn Wan Ainul Alyani
Co-supervisor: Dr Akhyari bin Nasir

3.6 Portable Document Format (PDF)

The Portable Document Format (PDF) is a file format developed by Adobe in the 1990s to present documents, including text formatting and images, in a manner independent of application software, hardware, and operating systems. PDF files may contain a variety of content besides flat text and graphics including logical structuring elements, interactive elements such as annotations and form-fields, layers, rich media (including video content) and three-dimensional objects using U3D or PRC, and various other data formats. Figure 13 shows the result of hex for original image of PDF and after shredding process:



```
            00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
0000000000  25 50 44 46 2d 31 2e 34 0d 25 e2 e3 cf d3 0d 0a    %PDF-1.4.%......
0000000010  32 34 39 20 30 20 6f 62 6a 0d 3c 3c 2f 4c 69 6e    249 0 obj.<</Lin
0000000020  65 61 72 69 7a 65 64 20 31 2f 4c 20 35 38 31 34    earized 1/L 5814
```

(a)

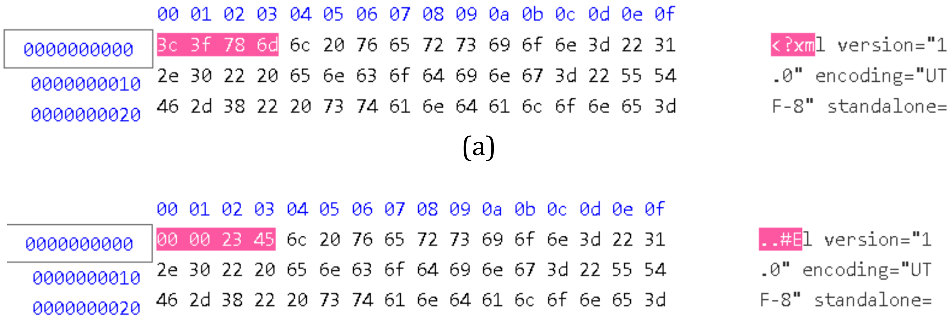
```
            00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
0000000000  00 00 23 45 2d 31 2e 34 0d 25 e2 e3 cf d3 0d 0a    ..#E-1.4.%......
0000000010  32 34 39 20 30 20 6f 62 6a 0d 3c 3c 2f 4c 69 6e    249 0 obj.<</Lin
0000000020  65 61 72 69 7a 65 64 20 31 2f 4c 20 35 38 31 34    earized 1/L 5814
```

(b)

Figure 13: (a) The hex results for original image of PDF before the shredding process (b)The hex results for image of PDF after the shredding process

3.7 Scalable Vector Graphic (SVG)

Scalable Vector Graphic is an XML-based file format that is used primarily on the web and has recently become more popular in creating content for cell phones and handheld wireless devices. SVG files are text-based, they can be edited easily, even after they have been exported and uploaded to a web server. Because of this ability, SVG files are used in data-driven, server-based workflows where customized content is a necessity. Figure 14 shows the result of hex for original image of SVG and after shredding process.



```
            00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
0000000000  3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31    <?xml version="1
0000000010  2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54    .0" encoding="UT
0000000020  46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d    F-8" standalone=
```

(a)

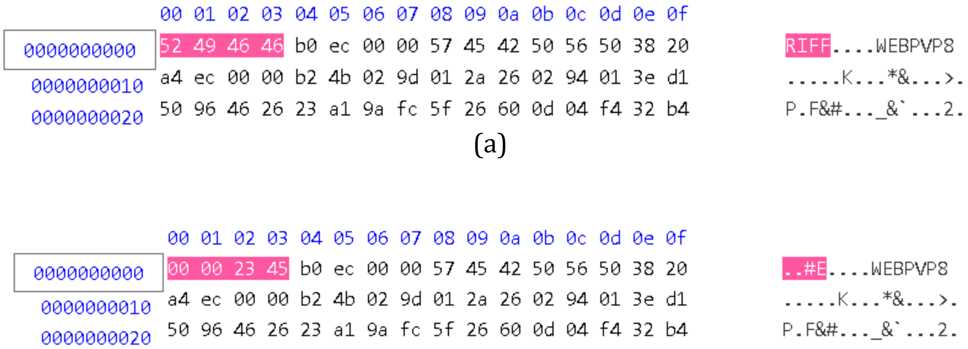
```
            00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
0000000000  00 00 23 45 6c 20 76 65 72 73 69 6f 6e 3d 22 31    ..#El version="1
0000000010  2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54    .0" encoding="UT
0000000020  46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d    F-8" standalone=
```

(b)

Figure 14: (a) The hex results for original image of SVG before the shredding process (b)The hex results for image of SVG after the shredding process

3.8 WEBP or Weppy

WebP is an image format employing both lossy and lossless compression. It is currently developed by Google, based on technology acquired with the purchase of On2 Technologies. As a derivative of the VP8 video format, it is a sister project to the WebM multimedia container format. Figure 15 shows the result of uploading and after shredding.



```
            00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
0000000000  52 49 46 46 b0 ec 00 00 57 45 42 50 56 50 38 20    RIFF....WEBPVP8
0000000010  a4 ec 00 00 b2 4b 02 9d 01 2a 26 02 94 01 3e d1    .....K...*&...>.
0000000020  50 96 46 26 23 a1 9a fc 5f 26 60 0d 04 f4 32 b4    P.F&#..._&`...2.
```

(a)

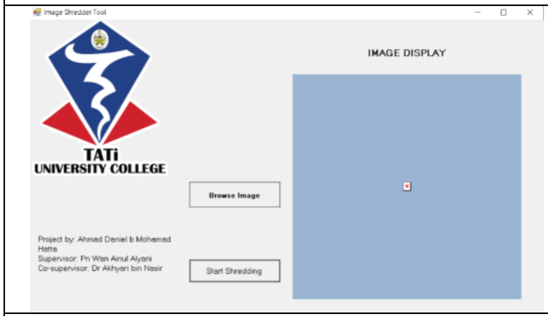
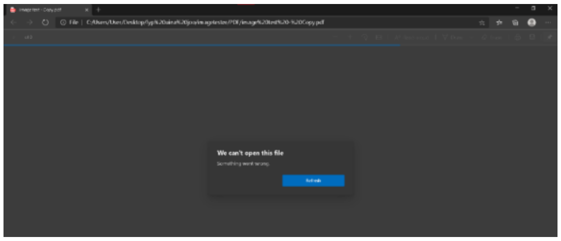
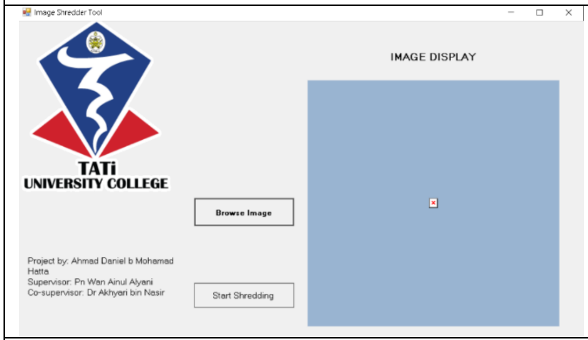
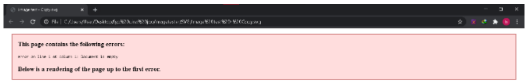
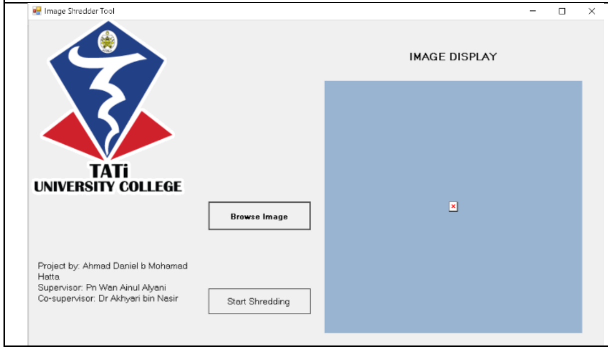
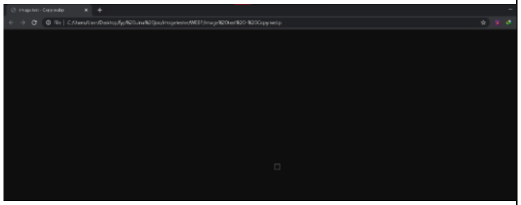
```
            00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
0000000000  00 00 23 45 b0 ec 00 00 57 45 42 50 56 50 38 20    ..#E....WEBPVP8
0000000010  a4 ec 00 00 b2 4b 02 9d 01 2a 26 02 94 01 3e d1    .....K...*&...>.
0000000020  50 96 46 26 23 a1 9a fc 5f 26 60 0d 04 f4 32 b4    P.F&#..._&`...2.
```

(b)

Figure 15: (a) The hex results for original image of PDF before the shredding process (b)The hex results for image of PDF after the shredding process

Table 2 below shows the comparison before and after the image media file types of PDF, PDF, SVG and WEBP being shredded using Image Shredded Tool.

Table 2

PDF	
 Image Shredder Tool IMAGE DISPLAY TATi UNIVERSITY COLLEGE Browse Image Start Shredding Project by: Ahmad Daniel b Mohamad Hatta Supervisor: Pn Wan Ainul Alyani Co-supervisor: Dr Akhyari bin Nasir	 Image test - Copy.pdf File | C:/Users/User/Desktop/fyp%20aina%20joo/imagetester/PDF/image%20test%20-%20Copy.pdf We can't open this file Something went wrong.
SVG	
 Image Shredder Tool IMAGE DISPLAY TATi UNIVERSITY COLLEGE Browse Image Start Shredding Project by: Ahmad Daniel b Mohamad Hatta Supervisor: Pn Wan Ainul Alyani Co-supervisor: Dr Akhyari bin Nasir	 Image test - Copy.svg File | C:/Users/User/Desktop/fyp%20aina%20joo/imagetester/SVG/image%20test%20-%20Copy.svg This page contains the following errors: error on line 1 at column 1: Document is empty Below is a rendering of the page up to the first error.
WEBP	
 Image Shredder Tool IMAGE DISPLAY TATi UNIVERSITY COLLEGE Browse Image Start Shredding Project by: Ahmad Daniel b Mohamad Hatta Supervisor: Pn Wan Ainul Alyani Co-supervisor: Dr Akhyari bin Nasir	 Image test - Copy.webp File | C:/Users/User/Desktop/fyp%20aina%20joo/imagetester/WEBP/image%20test%20-%20Copy.webp

4.0 CONCLUSION

After Image Shredder Tool are tested using several image files types, the result meets the project objective. Based on the result, all image file types that has been chosen can be shredded using Image Shredder Tool. There are five file types five types BMP, GIF, JPEG, PNG and TIFF which are perceptible and able to be shredded using Image Shredder Tool.

However, there are also files that unable to be viewed but able to be shredded; PDF, SVG and WEBP. PDF file is unable to be viewed for the reason that it is a document file type and not an image file type. However, it is managed to be shredded, similar to SVG and WebP files respectively. These three files can be used as an image file but they are not exactly an image file.

Table 3: Summary of result

No.	Image File Type	Perceptible before shredded	Shredded
1	BMP	Yes	Yes
2	GIF	Yes	Yes
3	JPEG	Yes	Yes
4	PNG	Yes	Yes
5	TIFF	Yes	Yes
6	PDF	No	Yes
7	SVG	No	Yes
8	WEBP	No	Yes

ACKNOWLEDGEMENT

The authors gratefully acknowledge Faculty Computer, Media and Technology Management, UC TATI.

REFERENCES

B., M., Holi, G., & Murthy, S. (2016). An Overview of Image Security Techiques. *International Journal of Computer Applications*.

Diego Galar, U. K. (2017). *eMaintenance: Essential Electronic Tools for Efficiency*. Academic Press.

Allen, E., & Triantaphillidou, S. (2012). *The manual of photography and digital imaging*. CRC Press.

Boutell, T. (1997). PNG (Portable network graphics) specification version 1.0.

Golding, M. (2008). *Real world Adobe illustrator CS4*. Peachpit Press.

Miano, J. (1999). *Compressed image file formats: JPEG, png, gif, XBM, BMP*. Addison-Wesley Professional.

Morkel, T., Eloff, J. H., & Olivier, M. S. (2006). Using image steganography for Decryptor distribution. *On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops*, 322-330.

Ramesh, & Dr. A. Shanmugam. (2011). Comparison and analysis of discrete cosine transform based joint photographic experts group image compression using robust watermarking algorithm. *American Journal of Applied Sciences*, *8*(1), 63-70.

Tim Fisher. (2010, August 21). *DoD 5220.22-M: Everything you need to know*. Lifewire. https://www.lifewire.com/dod-5220-22-m-2625856

Tim Fisher. (n.d.). *What is the write zero data sanitization method?* Lifewire. https://www.lifewire.com/what-is-the-write-zero-method-2626052

Tim Fisher. (n.d.). *Is the Gutmann method a good way to erase data?* Lifewire. https://www.lifewire.com/gutmann-method-2625891