Human Visual Based Perception for Steganography

Abstract
News articles in 2014 stated that 1.8 billion images are uploaded daily to the Internet, and this number is expected to increase annually. However, some of these uploaded images may contain hidden information that can potentially be malicious (e.g. an image that contains hidden information regarding terrorism recruitment) or may cause serious damage (e.g. an employee wishing to hide sensitive company details in an image file and exporting the image to 3rd parties). This research studied the most effective methods in manipulating images to hide information (Data Loss).

Significant work has been done on computational algorithmic detection. Yet the desired output from this work was to find the point at which a human can no longer visually establish the difference between an original image and a manipulated image. This research examined the extent of use for file formats, bit depth alterations, least significant bits and message and audio concealment. Findings of this study indicated that audio insertion and picture insertion into cover image files are the strongest in deceiving the human eye. These results have been categorised for the enhancement of the research field for human visual perception for image based steganography.

Keywords
Steganography, Data Loss Prevention, Human Perception, Image Manipulation
1 Introduction

Data Loss Prevention is very topical due to the ever increasing number of cyber-attacks and data leakage incidents. Data Loss Prevention (better known as DLP) refers to the methods that identify, monitor, and protect data at rest, in motion, and in use, through extensive content analysis [1]. It is estimated that 90% of large organisations are targeted on an annual basis for data breaches and lose, on average, between £1.46 - £3.14 million [2]. McAfee report 43% of all data loss is due to internal actors where an employee or someone with access to the computer systems maliciously exports sensitive data to external entities [3]. One of the ways in which this is conducted is by hiding information in media files to avoid detection.

However, the practice of concealing secret information is no recent discovery. This practice dates back over 2000 years and has been used in personal, political and especially military messages at times of war [4]. As early as 486 BC, the Greeks received warning of Xerxes’ plans of attack from messages secreted beneath the wax of a clay tablet by dotting successive letters with secret ink [5]. Hundreds of years later, Mary Queen of Scots would utilise substitution ciphers to secretly communicate with her supporters while being held prisoner by Queen Elizabeth of England.

The word ‘Steganography’ was derived by the two Greek words ‘Steganós’ (covered), and ‘Graptos’ (writing) which constitute a literal translation of ‘cover writing’ [6]. While classical cryptography (encryption) is about concealing the content of a message by ‘scrambling’ it where 3rd parties know communication has taken place [7], steganography is about concealing the very existence of the message altogether [5]. Luo et al defines Steganography as a technique for hiding information [8]. This definition, although vague, has been extended to define steganography as the art and science of communication, where the very existence of that communication is hidden [9]. To illustrate a representation of steganography in today’s technological environment, it is an information security tool that stores secret information in a media file where only the sender and receiver can discover the private data [10]. Steganography is predominantly prevented by DLP, yet what techniques exist in DLP to prohibit its operations?

1.1 Data Loss Prevention Techniques

The best practices for Data Loss Prevention against steganographic practices are divided into two areas of research: data-at-rest and data-in-motion. Both areas cover the current ‘industry standard’ for data loss prevention.

1.1.1 Data-At-Rest

Data-at-rest refers to the data stored at an endpoint (such as a computer or mobile device) [11], where steganography predominantly involves the manipulation of static multimedia files by the user [12]. When a system is infiltrated, these users can either be internal (authorised user) or external
(unauthorised user) and leak sensitive/confidential data. A common way in which this data is leaked is to embed the sensitive data into cover images (the image a user sees upon opening a file) or other forms of multimedia. Preventative measures, for data-at-rest steganography, often include the use of endpoint encryption or authentication such as by passwords, to prevent unauthorised parties, and restrict access to a subset of authorised users, or with potential steganographic tools that can be used to hide data within images [13]. Furthermore, the system could include physical media control to prevent the copying of sensitive data to unauthorised media to further prevent steganography and enhance DLP. This would leave the malicious user little choice but to transfer the sensitive data over the systems network to an external source, which then concerns the research area of data-in-motion security.

1.1.2 Data-In-Motion
This relates to any information that is transferred between endpoints over a network [11]. Data-in-motion steganography can often involve modifications to network protocols and deliberate deception to conceal the transfer of sensitive information [12]. This can be prevented by the use of network monitoring with packet sniffers, such as Wireshark and firewalls, to log and monitor network traffic and detect and investigate unauthorised sensitive data transfers [13]. In addition, secure email, secure API’s and encrypted physical media ensure that data exchanges are only made with authorised 3rd parties, any unauthorised attempts would be flagged and reported.

1.2 Why Human Perception?
Data Loss Prevention, especially in industry today, relies heavily on the success of automated steganography detection algorithms that operate during the ‘data in motion’ phase combined with the strength of physical security in ‘data-at-rest’. However, most steganographic techniques, for content based file formats, randomly place a hidden message in a cover image which is visually obvious to the human eye, but very difficult for even the most sophisticated algorithms to detect [14]. This leads to the question of why there is a significant lack of research in human visual detection of steganography. A DLP algorithm may detect an image, yet can a human visually detect inconsistencies in an image where algorithms cannot? If yes, then to what extent? This work conducted tests on this very subject.

1.3 Aims and Objectives
The aims and objectives of this research were as follows:

1. To manipulate images using the following steganographic/conversion techniques: File Format; Bit Depth; LSB Images; LSB Text and Audio Input.
2. To produce a table characterising the human deceptive value/effectiveness of steganographic methods.

3. To establish the visible point of the ‘strongest steganographic image’ where an image can be modified until it can be spotted by the human eye.

To ensure valid comparative data, the experiment was conducted on a single machine to ensure there were no changes in resolution, brightness and screen quality for each participant.

1.4 Research Scope
This research produced 17 converted/manipulated images and compared them to the originals to evaluate the extent of human perception of steganographic images. The research built on research from previous academics that touched on the human perception aspects of steganography [15], while utilising the steganographic techniques to convert and manipulate the images necessary for the study [7] [16] [17]. Although the research incorporated some psychological aspects of research which can be used within the field of psychology, this research was purely aimed at, and operated within, the confines of the Computer Science security field. The research limited its scope to those above the age of 18 and included both computer science and non-computer science participants of all age ranges and sexes.

1.5 Paper Structure

2 Following this ‘Introduction’ section, the ‘Literature Review’, will discuss both computational aspects as well as visual research, in order to gain a comprehensive understanding of work already done in steganography. The ‘Methodology’ will then convey the techniques and processes used to manipulate images and complete the conditions of the experiment and the objectives of the work. This is followed by the ‘Results’ section, where the outcome of the experiment is conveyed alongside a relevant critical ‘Discussion’ regarding the impact of the results on the field of study. The paper is then terminated with relevant ‘References


3 Literature Review

This section critically analyses and reviews the multitude of work done for computational steganographic algorithms and the minimal work done for human visual based perception against images subjected to steganographic techniques.
3.1 Computational Steganography

Computational steganography, gained traction back in the early 1990’s with the introduction of how algorithms could be utilised for steganography, giving birth to the Least Significant Bit (LSB) algorithm [16]. This introduced linguistic steganography where within this LSB algorithm, natural language could be secretly embedded into a cover image. Linguistic steganography has been the centre of debate regarding potential communication between terror activists, such as the attacks on the World Trade Centre in 2001 [18][19]. There are approximately 28 billion images hosted over 2 billion sites, making manual human checking for all steganographic images impossible [19]. This is why analysis algorithms are a necessity, in correlation with human visual detection, for Data Loss Prevention. Analysis can find patterns, such as keyword lists and hashing and report a concern for determination by human subjects [20].

3.2 Steganography Techniques

In recent decades, steganography has seen significant computational developments, in comparison to its previous use throughout history [7] [8] [21]. Yet why is steganography needed? Table 1 below compares the effectiveness of information hiding techniques for different motivational factors such as: confidentiality (ensuring communication remains between trusted parties only); integrity (no message tampering); and irremovability (named as ‘unremovability’ in [22], an inability to reverse engineer or decrypt steganography methods to reveal hidden information) [22].

<table>
<thead>
<tr>
<th>Technique</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Unremovability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Digital Signatures</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Steganography</td>
<td>Yes / No</td>
<td>Yes / No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

*Table 1 - Comparing Message Hiding Techniques [22]*

Table 1 above highlights the value that steganography has for information hiding, confidentiality, integrity and irremovability, in comparison to alternatives such as encryption and digital signatures. Furthermore, steganography, when executed correctly, incorporates many techniques to conceal content without revealing its existence.

3.2.1 Least Significant Bit (LSB)

One technique to hide information is the Least Significant Bit algorithm, better known as LSB. This is a commonly utilised steganographic technique to embed information in a cover file. LSB can be used in the cover files of many forms of multi-media but it is used most frequently used for images. LSB manipulates specific bits of an image by changing the least significant values to avoid detection. An example of LSB’s functionality for manipulating the three primary colour values, red, green and blue (RGB) of an image can be seen below [7]:
The letter A is represented in binary by:

01000001

An example image is represented in binary as:

(00100111 11101001 11001000)
(00100011 11001000 11101001)
(11001000 00100111 11101001)

If the letter A were to be inserted into an image using LSB1:

(00100110 11101001 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

This represents LSB1 as it only manipulates the 1st bit. LSB 2 would be represented as such:

If the letter A were to be inserted into an image using LSB2:

(00100101 11101000 11001000)
(00100011 11001000 11101001)
(11001000 00100111 11101001)

The lower the LSB exchange, the harder it is to detect manipulation within the image however, this adversely means that a smaller amount of information can be stored due to the limited number of least significant bits that can be manipulated. The higher the LSB exchange, the easier it is to detect manipulation in the image, yet a larger amount of data can be stored within the image due to the larger volume of bits.

3.3 Human Based Visual Perception

Steganography relies on the assumption that a human is not aware of the existence of any hidden data. This is one of the predominant reasons why steganography is argued to be just as, if not more, effective than cryptography. It is much easier to hide the existence of hidden data than to make its existence known e.g. where an attacker/investigator knows exactly what to look for i.e. a decryption key [23]. As the human eyes are insufficient when detecting minimal changes in colour or positioning [24], steganography can be tailored specifically to exploit this inadequacy to the benefit of a malicious user, yet little research has been published in this field.

Limited research has touched on how humans see images that have been subjected to steganography [15]. Morkel et al discussed how humans perceive different file formats that have been subjected to the LSB algorithm, including JPEG, BMP and GIF. They declared JPEG and BMP to be the most effective in hiding information, yet other work states that PNG and BMP are more effective in
concealing information [23][25]. Morkel et al.’s study is only limited to file format perception and does not include the way in which humans perceive images that have been subjected to key steganographic techniques including: bit depth; LSB images; LSB text and audio insertion etc. Moreover, this study dates back to 2005 and is arguably outdated. Their findings exclude the research of the PNG file format altogether. This current study aims to update these findings and to add PNG to the research field for comparison by looking at how humans perceive different file formats of the same image.

3.4 Defining Scope
With steganographic techniques, such as the LSB algorithm, data can be successfully concealed in images. Although steganography detection algorithms are automated to detect hidden information in images, the most important area of steganography (and its core principles) is its ability to be imperceptible to the human eye [15]. The predominant amount of steganography detection research focuses purely on computational algorithms [26] [27] [28] [29] as opposed to the human visual detection elements. This presents an opportunity to explore new areas of research into human visual perception of steganography. This paper will therefore focus on this area with the aim to further develop this field by analysing how humans can visually detect various steganographic techniques.

4 Methodology
This section details the process of deriving an artefact along with the relevant technologies used for this work. Both successes and setbacks are documented along with relevant screenshots and steps so these processes can be replicated.

4.1 Design
The original image file formats to be used were JPEG, BMP and PNG. However, the BMP file format had to be changed to GIF as the Qualtrics survey software used for this study would not accept images of a BMP file format. The user interface was also important for participant interaction and to successfully engage a participant. Two images would be placed side by side for parallel cognitive processing [30] and will henceforth be defined as an ‘image set’.

Firstly, image formats were investigated and then in an experiment, two images with different formats or with one as an original image and the other as a cover image would be compared by volunteer participants.
4.2 Image Conversions
Original images (taken mainly from steganography based papers) were manipulated to generate output images that could be used in the study. All images conversions were used from the resource list which included dual Hanns-G monitors and an XPC Shuttle tower on a Windows 10 operating system.

4.2.1 File Format Conversions
The first of the image conversions included a simple manipulation technique of importing an image into Microsoft Paint and converting the file format through the ‘save as’ function. The image sourced was ‘Lena’, which has been used in many previous steganography related papers and is a landmark steganographic image [12][31][32].

Initial attempts to convert the file format proved ineffective as changing the file format by manually re-naming the file extension in a directory did not convert the image. This was found by checking the files within a hex editor and discovering that the first four bytes, the signature of the file type, remained the same [33]. Analysis of the file size, where different file formats of the same image have different file sizes, demonstrated that the file size had remained the same.

The successful process of converting the file format with MS Paint can be seen in 1 below.

![Figure 1 - Process of Converting the Lena File Format](image)

The Lena image was sourced online as a GIF [35] and converted to the PNG and JPEG file formats with MS Paint. These converted images were then verified with the use of an online hex editor to ensure a successful conversion had taken place (see Figure 2 below).
4.2.2 Bit Depth Conversions

The second image conversions were made to manipulate the original images (predominantly 24 bits by default) to a lower bit rate. The bit depth represents the amount of bits per pixel. The greater the bit rate, the higher the quality of the image due to the greater number of colours [7]. However, previous research claims that an 8 bit colour image is just as good as a full colour, 24 bit image [36].

To test this, the image selected for this was the Mona Lisa, argued to be the world’s most famous painting [37]. This can be beneficial to the study as a recognisable image is often easier to detect if there has been any manipulation, therefore truly testing the strength of the steganography technique.

The Mona Lisa was downloaded in a standard format of 24 bits online [38]. This 24 bit image represents $2^{24}$ colours resulting in a possible 16,777,216 colour variations by default [39]. The process of conversion can be seen below in Figure 3.
The three conversions for the 8 bit, 4 bit and 1 bit versions of The Mona Lisa were initially attempted with GIMP 2.8, predominantly due to its ability to manually edit the maximum amount of colours the image could use. The image imported was a 24 bit image but GIMP only allowed a bit conversion down to an 8 bit image (maximum of 256 colours) and no higher, meaning a 12 or 16 bit image would not be possible for this section of the work [40]. Although the 8, 4 and 1 bit images could be created with GIMP, MS Paint is more widely established as an image conversion technique. Microsoft Paint was therefore used as a suitable alternative (as can be seen working with The Mona Lisa in Figure 3 above) to cover the full range of bit conversions of 8, 4 and 1 [41].

The Portable Network Graphics (PNG) was also used as a file format. As PNG is a lossless file format, this stores a better quality/closer matching copy of the image, whereas the Joint Photographic Experts Group (JPEG) is a lossy file format and focuses on smaller file sizes over image quality [7]. As image quality is one of the most important factors of the study, to ensure the most accurate research outcome based on human perception, a lossless file format (in this case, PNG) is used for various sections of the artefact, except for JPEGs when used briefly for file format conversions.

4.2.3 LSB Image Input Conversions

The third image conversions involved the use of the LSB algorithm, which was utilised to hide the Lena image into the baboon image. This was done with the online tool, Incoherency, created by James Stanley [42]. Both Lena and The Baboon images selected for this section have been used in many previous steganography related papers [12][31][32]. The Baboon image was uploaded first as the cover image, followed by the Lena as the secret image. The amount of LSB places could be selected with a sliding bar as can be seen in Figure 4 below.
The output images utilised LSB1, LSB3, LSB5 and LSB7. Furthermore, the images uploaded and used for this section were also the PNG file format used for its lossless compression technique. As these images were completed, the next set of linguistic conversions were made.

4.2.4 LSB Textual Input Conversions
After extensive research into textual steganographic tools, there was only one reliable option online, yet this only enabled the use of LSB1 due to a 250,000 character maximum [43] as can be seen in Figure 5 below.

However, software named ‘SteganUI’ from Yunjia Wang, a University of St-Andrews postgraduate student, was under development and provided the unique functionality to select various LSB values to hide text within an image [44]. This software was an offline and unpublished eclipse package that allowed a range of LSB numbers from 1 to 8. The output file could also be converted to an alternate file format including JPEG and PNG, yet PNG was selected for the purpose of this study [45].

Random strings were generated to populate the text to be hidden within the images. Manually this would take too long so a random string generator was used [46]. Utilising the LSB 8 manipulated image as an example, 50,000 words containing 20 characters each were generated, totalling 1,000,000 characters to hide within a Union Jack Image. This particular image was chosen due to its hard lines (the solid straight lines within an image), where any ‘squints’ or ‘disfigurements’ in the hard lines of the image would be easily detected by a participant of the experiment.

This text was then copied to a .txt file and saved for later use for SteganUI. The original ‘Union_Jack.png’ image was imported into the text hiding software. The previous text file, containing the 1 million characters, could now be imported into the Qualtrics software to be concealed within the
Union Jack PNG image. The necessary output file format could be selected, along with the bit exchange in this case 8 bits, as shown below in Figure 6.

Processing this image, especially across an 8 bit exchange, took on average of between 8-10 hours to fully process due to the large volume of characters. Once this process successfully completed, the image is shown within the IDE and outputted to the software’s destination folder (see Figure 7 below).

The output files were then imported to Qualtrics along with all other selected instances of LSB 1, LSB 4, LSB 6 and LSB 8. If all LSB’s were used (from 1-8) it would have cluttered the survey with too many images of the Union Jack, as well as prove difficult for a user to notice any significant change between LSB increments of 1.
4.2.5 Audio Input Conversions

Audio files were then placed into image sets for the study. The Audio file entitled, ‘bell-ringing-01.mp3’ was an mp3 file with a 16 second duration, and a 672KB file size (0.672MB), sourced online, legally, for free [47]. The mp3 file format was chosen due to its status as the most popular file format for digital audio compression [48]. The bell audio file was placed into a GIF image file because of its lossless compression and chosen as PNG could not be used with this method. The image used was the 1893 version of ‘The Scream’ painting by Edvard Munch, obtained online as a JPEG [49] as shown in Figure 8, then converted to a GIF file format through MS Paint making the size of this GIF file 7.28MB without audio insertion.

The audio file is placed within the image file, ‘The_Scream_Original.GIF’ to create a new file altogether, ‘Scream_Bell.GIF’ [50]. The manipulated output image file generated from this process is 7.94MB, compared to the file size of the original input GIF image file of 7.28MB, conveying that the audio file is successfully concealed within The Scream image.

There were, however, limitations to this technique as the audio file bits are added to the image file instead of replacing the bits already there. This causes the file size to increase dramatically. This was evident on the first attempt of this section of work when using Beethoven’s 9th symphony 1st movement, “Allegro ma non troppo, un poco maestoso (D minor)”. This caused the file size of the original Scream GIF image file to increase from 7.28MB to 42.9MB and conflicted with the 16MB file size limitation offered by Qualtrics. The bell was chosen as a suitable alternative due to its significantly smaller file size.

A second cover image of ‘The Scream’, for the next image set, was generated using a larger audio file, “Richard Wagner – Ride of the Valkaryies” with a size of 4.57MB at a length of 5 minutes, than the ringing bell used previously at 0.672MB for 16 seconds. The Wagner audio file was obtained from the video streaming platform, YouTube [51], and converted with a ‘YouTube to MP3 converter’ [52].

The Windows command prompt was utilised once again and produced a slightly larger output file size of 11.8MB, which would be compatible with Qualtrics 16MB file size limit.

Simple cross multiplication to find the missing proportion can indicate the maximum audio time limit that can be used to ‘hide’ audio in The Scream input image using this technique, without exceeding the Qualtrics file size limit. This is calculated as: \[16MB = \frac{11.8MB}{N} = 6.8 \text{ mins} = 6m\ 47s.\]
Even if an audio file was sourced at the exact limit of 6 minutes and 47 seconds, there is a low probability of a user seeing much visual difference in an extra 4.2MB that has been ‘copied’ and not ‘blended’ together to make the output image. This is discussed at length later in Section xx.xx.

4.3 Image Uploads
All the images (both original and manipulated) required to be uploaded to the Qualtrics survey software. Each image was given a resolution breadth of 317 by default. This provided enough space to include the original and the manipulated images side by side for easier viewing for the participants of the study. See Figure 9 below for an example with ‘The Mona Lisa’.

The height varied depending on the natural height of an image e.g. ‘The Last Supper’ requires less height than ‘The Mona Lisa’. The height, however, was irrelevant compared to the width just as long as the original and the manipulated were displayed side by side. After all the original and manipulated images were uploaded to the platform and formatted along with all relevant information, the environment of the experiment could be designed.

5 Experiment
The participant of the study is asked to sit down and conduct the experiment from an Apple MacBook Pro 15 Inch with a retina display. The MacBook had been chosen predominantly due to its portability, enabling more participants, especially living out-with a lab environment, to conduct the study with the ease of bringing the experiment to them [53].

This model of MacBook Pro also has an Ambient Light Sensing (ALS) system that automatically adjusts the brightness of the display in proportion to the light available in the laptops location [54]. This feature will be turned off to ensure each participant involved in the study is presented the artefact with the exact same screen brightness. No evidence was found to indicate whether the charging of a MacBook provides a greater brightness than without, therefore for portability, no charger will be used while the participant is involved with the study.
The following screen features are applied to the MacBook Pro:

- Brightness = 100%
- Ambient Light Sensing = Off
- Resolution = Default (2880 x 1880) and 220 Pixels Per Inch
- Display Profile = ‘Display’

Informal alpha testing estimated the full study, including reading of the ethics and debriefing forms, to take somewhere between 10-12 minutes. The participant is audio recorded during the experiment to hear their thought process and decision making spoken out loud for the benefit of the study. Furthermore, vocalising thought processes during the experimentation has been proven to be beneficial for research purposes to engage the participant more with the study [55].

For any one question, the user is shown an image set, two images side by side sequentially, where one image is the original and the other image is manipulated (either minor or majorly) yet the user is not told which is which. The participants are asked to judge the visual ‘similarity’ between the original and the manipulated images.

5.1 Key Information

Below is the itinerary to the study:

1. The participant is asked to read a hard copy of the participant information form to confirm they understand what will be required of them = 2 Minutes
   a. The participant accesses the artefact with a Mozilla Firefox browser (MacBook default browser)
   b. Before starting, the participant is asked to provide verbal confirmation that they have read the participant information sheet and agree to being verbally recorded during the process.
2. The participant is then asked to open the Qualtrics survey = 10 Seconds
3. The participant then reads the full ethics form = 2 Minutes
a. Computationally agrees to all experiment conditions
b. Asked once again if they give consent to being digitally recorded.

4. Survey starts and asked to, “Please Take 10 Seconds Minimum to Analyse Each Question Carefully” = 3 Minutes and 30 Seconds
   a. Asked to answer 17 Questions with 2 images per question (1 image set)
      i. 34 Images to analyse in total
      ii. Gives answers based on the statement:
          1. “These Images Look Similar”
   b. Participant is asked if they have seen the image set before
   c. In the last few image sets for ‘The Last Supper’ painting, participants are asked, “Are you sure you cannot see anything hidden in either of the images?” by a supervisor, if they do not visually detect the “Can You See This Message?” hidden within the front facing tablecloth of the painting.

5. Participant then submits their answers and reads debriefing form = 2 Minutes

The study does not include anyone below the age of 18 for ethical purposes and a supervisor is present for the duration of the experiment with each participant while being audio recorded.

5.2 Scoring
Scores were allocated to each answer a participant gave for each image set. Scoring, on a descending scale from a maximum of 5 to a minimum of 1, was assigned to each question in the Qualtrics artefact in accordance with the use of a Likert scale. This scale was selected due to its popularity in attitude based experiments, its simplicity and versatility [56]. The scoring was assigned based on the similarity between two images, the closer the visual similarity, the higher the score (closer to 5) the manipulated image would receive. The wording of the statement was selected carefully to evaluate how respondent’s definition of “These images look similar” influenced their decision process. The manipulated images with the highest scores are the most visually effective in concealing information. With this quantitative data, the point at which a human can no longer visually establish the difference between an original image and a manipulated image can be sourced (see page 34 under ‘The ‘Strongest’ Steganography Image’). This would give indications toward the extent of steganographic value for file formats, bit alterations, LSB and message and audio concealment techniques.

Furthermore, the result of this study, based on scoring, will output the best combination of all these techniques for different kinds of visual deception.
The example in Figure 11 above conveys how this project’s scoring was applied to the Qualtrics artefact. This shows two Union Jack images (left of the blue line in Figure 11 above) where one is the original, and the other is the manipulated image with 200 characters hidden within LSB 1. As both these images are visually identical, the manipulated image is therefore given a score of 5, whereas the other two visually unidentical images (right of the blue line in Figure 11 above) conveys an original Union Jack, while the other image contains 1 million characters hidden in LSB 8, are given a score of 1 on the Likert scale. This example would indicate that LSB 1 in the first set of Union Jacks is a stronger use of steganography than LSB 8. The participants’ scores for each image set are collected and calculated to find the mean score. The higher the mean score, the stronger the value of the steganographic/image conversion technique in deceiving the human eye.

6 Results
The central aim of this project was to manipulate images using steganographic techniques, categorise the results from strongest to weakest and to suggest the most efficient ways to hide different types of data in images with the ‘strongest steganographic image’. This section will detail these results from each of the image sets and produce the findings to effectively satisfy the remaining incomplete objectives of this project.

6.1 Key Information - Participants
There were a total of 50 respondents over a 7 day experimentation period. Each participant gave their full consent to the study and to being audio recorded during the experimentation process. Experiment length and average is rounded to the nearest value accordingly, with no decimal place, as can be seen below in Table 2.
6.2 Overall Image Comparison Results
This section displays the overall results across the 50 participants involved in the experimentation process. Further data visualisations for each of the image sets can be seen in 'Appendices'.

Each section will have the dual images as thumbnails to remind the reader what images were being used for the tests. Relevant clips from audio recordings are presented using quotations to gain a deeper understanding into why participants selected the answer that they did. Lastly, each figure will contain a mean Gauge chart (at the top right hand side of each figure) to convey the similarity between the images. With the exception of file formats, each image set that has a higher mean score (closer to 5 and green) will be seen as a stronger steganographic technique. A lower mean score (closer to 1 and red) will be regarded as a weaker steganography technique with blue signalling a more central Likert scale score.

6.2.1 File Formats
Overall, in contrast to initial predictions, many of the participants saw a varied difference between the file formatted images, predominantly referring to how, “The shape of her face is different” (Lena) and the “Sharper image quality” between the file formatted images.

6.2.1.1 JPEG Vs GIF
Several participants believed that Lena’s face on the JPEG image was “thinner” and “sharper” than the GIF image. Furthermore, the “lighting” on her “right shoulder” was “different” with the JPEG (at a “higher brightness”) than the GIF (at a “lower brightness”) (Figure 12).
The mean, shown in Figure 12 above, indicates that a JPEG and GIF file format of the same image do not share either a strong or weak similarity with a score of 3.62.

6.2.1.2 JPEG Vs PNG
Participants claimed the content of this Lena image set was “identical” but the JPEG image still looked “sharper” than the GIF image, one participant defining the PNG as “blurry”.

An average value score of 3.34 was produced by the 50 participants indicating only an average similarity between JPEG and PNG.
6.2.1.3 GIF Vs PNG
By the third image set of file formats, many participants “could not distinguish the difference” between the Lena GIF and PNG images.

![Figure 14 - Results of GIF Vs PNG (Lena)](image)

This resulted in a strong mean score of 4.10 out of the 50 respondents of the study, labelling the similarity between these two file formats as very strong.

6.2.2 Bit Depth
Participants expressed previous knowledge of this painting and could spot changes quite easily due to their previous recognition and familiarity of ‘The Mona Lisa’. However, the human eye sees red, green and blue in different brightness levels and as this painting possesses a darker green background with no high contrast colours [57], some participants claimed that brightness and colour changes were harder to see in this painting.

6.2.2.1 24 Bit Vs 4 Bit
Participants described the image set as “very different” visually, yet most participants still acknowledged that the manipulated image was the Mona Lisa. Participants also noticed “a severe change in colour” with the 4 bit image (which only contains a maximum of 16 available colours).
The lack of colours resulted in a significant amount of ‘strongly disagrees’, giving a low score for this manipulated image.

### 6.2.2.2 8 Bit Vs 24 Bit

Participants claimed that there was “no significant difference” between the 8 and 24 bit images, backing up claims made by other research done in this area that there is little visual difference between an 8 and 24 bit image [36]. However, a small portion of participants noticed that the sky in the background was “darker” in the 8 bit image and “lighter” in the 24 bit image.

The participants that noticed the colour changes assigned a lower score to the 8 bit image while those who did not assigned a higher score, resulting in a 3.36 mean score value.
6.2.2.3 1 Bit Vs 24 Bit
These images were “very different” and often received a strongly disagree selection, especially as the 1 bit was a greyscale image with only black and white available as colours.

![Figure 2 - Results of 1 Bit Vs 24 Bit (Mona Lisa)](image)

This caused respondents to assign a low score to the similarity rating, resulting in a mean score of only 1.48.

From the above the strongest steganographic technique was the 8bit Mona Lisa.

6.2.3 LSB Images
Although popularly used in image steganography, the baboon image was predominantly unrecognised by participants. Generally, participants were attracted to the baboon’s eyes and the colour of the nose and cheeks when attempting to detect changes. One participant even focused predominantly on the yellow and orange in the fur to see if the contrast/brightness changed.

6.2.3.1 LSB 3 Vs Original
These images were described as “very similar” where it was “very hard to distinguish the difference”.

![Image of LSB 3 Vs Original](image)
As a result, the LSB 3 manipulated image received a very high score from respondents with no ‘strongly disagree’ answers given by any participant.

6.2.3.2 Original Vs LSB 5

Participants established the manipulated image was “still a baboon” but not identical to the original image. Furthermore, the manipulated image was said to be “slightly darker”.

This provided an overall mean score of 2.98, neither a significantly strong or weak steganographic technique.
6.2.3.3 Original Vs LSB 7
This image set was described as “not similar at all” due to the LSB 7 image where a “woman was clearly inside” the image. However, many respondents did acknowledge that the manipulated image was “still the baboon image”.

![Figure 20 - Original Vs LSB 7 (Baboon)](image)

This produced a low score of 1.38 due to the large amount of respondents that noticed Lena in the Baboon cover image.

6.2.3.4 Original Vs LSB 1
Participants often spotted no difference here at all as LSB 1 manipulates very little in an image.

![Figure 21 - Results of Original Vs LSB 1 (Baboon)](image)

This caused respondents to score the LSB 1 image highly with a total mean score of 4.34.
From the above work, the strongest steganographic technique was considered to be LSB3 on the Baboon image.

6.2.4 LSB Textual Insertion

The Union Jack was unanimously known by every participant of the study where many participants recognised the “colour changes” across the Union Jack image sets that were made with the LSB algorithm. Many participants took extra time with this section and began to doubt their perception, as some of the image sets were so alike it became difficult to establish the difference between the two images. Participants often changed their answers with even two participants asking if there were some fault with the screen of the MacBook Pro.

6.2.4.1 Original Vs 200,000 Characters LSB 1

This image set looks “identical” and “very similar” to the original for most participants.

An average mean score of 4.12 conveys that 200,000 characters at LSB 1 is a very strong steganographic technique.

6.2.4.2 200 Characters LSB 1 Vs Original

The second set of Union Jacks often confused participants due to their almost identical similarity to the first image set. This caused people to adjust their answers based on suspicions rather than their eyes.
However, this did still score reasonably well even though there is not enough manipulation with LSB 1 to notice any significant difference visually. The doubt of human perception, especially with these images is an intriguing research area that is discussed in Section xx.xx under, ‘LSB Textual Insertion – The Union Jack’.

6.2.4.3 Original Vs 1 Million Characters LSB 8
The manipulated image here was described as “completely different”. 
With LSB 8 manipulation, around 40% of the image is completely disfigured with pixilation causing a score of 1.50.

6.2.4.4 800,000 Characters LSB 4 Vs Original

Some participants stated the colour was “off on one side” and one of the union jacks in the image set was “slightly darker in one half” of the image.

![Image of bar chart showing results](image)

Figure 25 - Results of 800,000 Characters LSB 4 Vs Original

The darker side was not significant enough for the larger number of respondents to provide a lower score and was therefore given an overall score of 3.02.

6.2.4.5 Original Vs 1 Million Characters LSB 6

Participants who noticed the darker half of one of the Union Jacks in the previous image set almost automatically noticed the same fault with the image but this time it was “even darker than before”.

![Image of bar chart showing results](image)
As this half was “significantly darker”, this caused respondents to select a far lower score than the previous image set.

From this section of the research, the strongest steganographic technique was 200,000 characters under LSB1 with the Union Jack image.

6.2.5 Audio Insertion
The Scream painting was only known to a small amount of participants. The painting itself contains many dim colours with low contrast of pixels, making any alterations, like ‘The Mona Lisa’ difficult to see.

6.2.5.1 Original Vs Original w/ Bell (672KB)
The manipulated image seemed “brighter” but still “very similar”. Many participants claimed the two images were still “exactly the same”.

![figure26](image-url)
The similarity of The Scream images caused many respondents to give either a ‘strongly agree’ or ‘agree’ selection with absolutely no ‘strongly disagree’ from any of the respondents.

6.2.5.2 Original w/ Ride of the Valkyries (4.57MB) Vs Original
Participants still consider this image set to be “identical”. The mean score is still very high, indicating this method is very strong for visual deception.

The strongest steganographic technique/conversion for this area was the original Scream image embedded with the Bell sound file (672KB)

6.3 Experiment Duration Timings
The average time spent on the study was 5 minutes exactly. Many of the respondents started the experiment at a slower rate while their attention span was very high. The average time spent on each question then peaked toward the middle (Union Jack images) then sped up towards the end of the
study (toward The Last Supper images). The faster time spent on each question toward the end could have been due to ‘experiment experience’ where the participant is accustomed to what is required of them during the experimentation process, enhancing their ability to make cognitive decisions quicker.

7 Discussion
This section provides a critical analysis of the results and processes produced by this experiment. This includes aspects of: the experimentation process; the order in which the image sets were placed; unexpected results; and decisions made by participants that may have been based on doubt rather than perception.

7.1 Critical Analysis of Results & Potential Future Work
This section will detail how each aspect tested contributes to the research filed of steganography and suggest future work where necessary.

7.1.1 File Format – Lena
Due to the way in which this question was presented, the ‘strongest’ file format cannot be derived. The comparison of the file formats was included only to see if the human eye noticed a difference between file formats. Previous studies have indicated that there is a difference on a computational level [7] [23][58] with only one other study indicating that there is a difference on a visual level [15]. This work has produced results strongly indicating various visual differences in brightness, image sharpness and shapes of objects within the image.

7.1.2 Bit Depth – Mona Lisa
The results show that of the images tested, the 8 bit depth image of Mona Lisa was the closest, visually, to where human perception could not see a difference compared to the original. However, the 8 bit depth image, although visually similar to the original, did not have an exceptionally high mean score, indicating that it is not strong enough to be used in place of a 24 bit image. It would be fair to argue that a 12 or 16 bit image would be close enough to deceive the human eye into thinking a 12 or 16 bit depth image was the original 24 bit standard. This can be tested in future work.

7.1.3 LSB Images – Baboon
The LSB 3 image had the highest score based on participants’ results, even higher than LSB 1 by a margin of 0.22 on the mean score. The LSB 3 image may have placed higher due to the ordering in which the image sets were placed in the Qualtrics artefact. Participants may assume that the first few image sets of each steganographic/conversion technique are “warm up sets” before the real image manipulation commences in the later image sets. Regardless, participants did have the opportunity to return to previous questions and change their answer accordingly, therefore LSB 3 is the strongest for hiding images based on the results of this study.
7.1.4  **LSB Textual Insertion – The Union Jack**
The first two image sets of Union Jacks were the only real anomaly when the results were produced. This was when the LSB technique that concealed 200,000 characters of text was superior in hiding information compared to only 200 characters of textual information with the exact same LSB1 placement. A strong argument could be made that the number of bits used in LSB (e.g. LSB1, LSB2 etc.) is more important in concealing information than the amount of text that is input into the image. Further analysis could point toward the doubts participants were having halfway through the experiment. As the Union Jack image sets were visually very similar to each other, participants were vocal and requested the opportunity to return to a previous answer and change it. Although this was allowed during the experiment, the participant was verbally informed at the beginning of the study to “… not let previous answers influence their current decisions”. This verbal statement did, however, seem to be disregarded due to many participants questioning and doubting their own decision making.

7.1.5  **Audio Insertion – The Scream**
The Audio insertion technique was, based on the results and mean scores, the highest scoring steganographic technique tested for the entire project. The advantage of this technique is its invisibility to the human eye if any modifications have been made to an image. The disadvantage is the high probability in which a data loss prevention algorithm would detect this kind of audio insertion technique based on the very foundations of steganalysis where an image will be flagged if it contains such a large file size [59].

Furthermore, although the identities of participants cannot be disclosed in accordance with ethics, it is interesting to note that a mother and her son (both above the age of 18) taking the experiment independently, both identified a ‘change in direction’ of the bridge within The Scream image and were the only two to do so. This could perhaps indicate that perceptions of images are somewhat hereditary. This is an intriguing field for future research.

The audio input conversions also restricted the extent of the project as the Qualtrics survey software could not take any files above 16MB. Future work could include a study that analyses if humans perceive any visual changes to an image that conceal larger audio files by utilising an alternative platform to Qualtrics. In addition, the technique of copying files into other files does not efficiently conceal ‘hidden information’. Both of the individual files (the audio and the image) are simply ‘added on top of one another’ instead of ‘blended together’. Future work should seek more efficient methods when hiding audio files in cover image files.

7.1.6  **The ‘Strongest’ Steganography Image**
The following combination of steganographic techniques included into one image would prove to be the most efficient in hiding data from the human eye, all while maintaining a low file size to go
undetected by steganalysis algorithms. All recommendations will be based on the results of this experiment.

The ‘Strongest’ steganographic image would be:

- **File Format:** PNG (due to lossless compression)
  - GIF has not been selected as participants often claimed JPEG and PNG were “sharper” than GIF. JPEG has not been selected due to its lossy compression.
- **12 Bit Depth**
  - This project has shown that an 8 bit depth value is close but not visually identical to a 24 bit image. Moving from 256 colours to 4096 colours ($2^8 = 256, 2^{12} = 4096$) should replicate the 24 bit image enough to successfully go unnoticed by human perception.
- **LSB 3 (for image hiding)**
  - This is dependent on the cover image and the image to be hidden, yet this has proven to be the strongest of the image sets.
- **LSB 1 (for textual insertion)**
  - A maximum of 200,000 characters of text can be secreted successfully within an image with little visual difference to the image.
  - Note: more characters cannot be added without moving up to LSB 2.
- **Less than 1MB file (for Audio insertion)**
  - If the file size is too large, steganalysis algorithms will pick up on this
  - Ideally keep the vocal message short to avoid detection. If the audio message is too large, the audio file should be divided and placed within several cover images independently.

Below is a table that categorises, in order of strongest to weakest, all the steganographic techniques tested in this study. Again, this excludes file formats due to the inability to categorise them in order:

<table>
<thead>
<tr>
<th>Image Sets</th>
<th>Strongest Technique</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LSB 3 Image</strong></td>
<td>4.56</td>
</tr>
<tr>
<td><strong>Original w/ Bell (672KB)</strong></td>
<td>4.52</td>
</tr>
<tr>
<td><strong>LSB 1 Image</strong></td>
<td>4.34</td>
</tr>
<tr>
<td><strong>Original w/ Ride of the Valkyries (4.57MB)</strong></td>
<td>4.24</td>
</tr>
<tr>
<td><strong>LSB 1 Text 200,000 Characters</strong></td>
<td>4.12</td>
</tr>
<tr>
<td><strong>LSB 1 Text 200 Characters</strong></td>
<td>3.76</td>
</tr>
<tr>
<td><strong>8 Bit Depth</strong></td>
<td>3.36</td>
</tr>
<tr>
<td><strong>LSB 4 800,000 Characters</strong></td>
<td>3.02</td>
</tr>
<tr>
<td><strong>LSB 5 Image</strong></td>
<td>2.98</td>
</tr>
<tr>
<td><strong>LSB 8 1 Million Characters</strong></td>
<td>1.88</td>
</tr>
<tr>
<td><strong>LSB 6 1 Million Characters</strong></td>
<td>1.88</td>
</tr>
<tr>
<td><strong>4 Bit Depth</strong></td>
<td>1.55</td>
</tr>
<tr>
<td>Technique</td>
<td>Strongest</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Audio Insertion</td>
<td>4.38</td>
</tr>
<tr>
<td>LSB Images</td>
<td>3.31</td>
</tr>
<tr>
<td>LSB Textual Insertion</td>
<td>2.93</td>
</tr>
<tr>
<td>Bit Depth</td>
<td>2.13</td>
</tr>
</tbody>
</table>

Table 3 - Each Image Set Ranked from Strongest to Weakest

Each aspect used (i.e. File Formats, Bit Depth, LSB Images etc.) each have their image set score collected and averaged to find the mean score, providing a strength score for the overall technique for image based steganography:

8 Conclusions

This thesis has focused on human visual perception based steganography. This area of research elicits true insight into computer security and how sophisticated images can become when manipulated for secretive purposes. Although experience can be gained from where to look and how these techniques work, human based visual inspection of images does not scale as algorithms do. With 28 billion images circulating the internet, there will always be new images chosen for steganography based purposes. This work has produced key results that indicate the lowest level of quality and file size, while concealing the largest amount of data, for the most efficient steganographic image, undetectable to the human eye. By knowing what the most effective ways are to conceal information, steps can be taken in future work to enhance Data Loss Prevention to restrict and prevent their use, especially in matters of national, financial and industrial security.
9 References


10 Appendices

10.1 Artefact/Experiment Screenshots

10.1.1 Questionnaire Information

I ...

- Have a Computer Science Background
- Do Not Have a Computer Science Background
- Would Prefer Not To Answer

My age is ...

0 10 20 30 40 50 60 70 80 90 100

Slide This Bar

I wear Glasses

- Yes
- Sometimes
- No
10.1.2 Online Image Questionnaire

Questions - Please Take 10 Seconds Minimum to Analyse Each Question Carefully

<table>
<thead>
<tr>
<th>Strongly agree</th>
<th>Agree</th>
<th>Neutral</th>
<th>Disagree</th>
<th>Strongly disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td>These Images Look Similar</td>
<td><img src="image1.png" alt="Image" /></td>
<td><img src="image2.png" alt="Image" /></td>
<td><img src="image3.png" alt="Image" /></td>
<td><img src="image4.png" alt="Image" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Strongly Agree</th>
<th>Agree</th>
<th>Neutral</th>
<th>Disagree</th>
<th>Strongly Disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td>These Images Look Similar</td>
<td><img src="image5.png" alt="Image" /></td>
<td><img src="image6.png" alt="Image" /></td>
<td><img src="image7.png" alt="Image" /></td>
<td><img src="image8.png" alt="Image" /></td>
</tr>
<tr>
<td>Strongly Agree</td>
<td>Agree</td>
<td>Neutral</td>
<td>Disagree</td>
<td>Strongly Disagree</td>
</tr>
<tr>
<td>----------------</td>
<td>-------</td>
<td>---------</td>
<td>----------</td>
<td>------------------</td>
</tr>
<tr>
<td><strong>These Images Look Similar</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Strongly Agree</th>
<th>Agree</th>
<th>Neutral</th>
<th>Disagree</th>
<th>Strongly Disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>These Images Look Similar</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### These Images Look Similar

<table>
<thead>
<tr>
<th>Strongly Agree</th>
<th>Agree</th>
<th>Neutral</th>
<th>Disagree</th>
<th>Strongly Disagree</th>
</tr>
</thead>
</table>

### These Images Look Similar

<table>
<thead>
<tr>
<th>Strongly Agree</th>
<th>Agree</th>
<th>Neutral</th>
<th>Disagree</th>
<th>Strongly Disagree</th>
</tr>
</thead>
</table>
These Images Look Similar

<table>
<thead>
<tr>
<th>Strongly Agree</th>
<th>Agree</th>
<th>Neutral</th>
<th>Disagree</th>
<th>Strongly Disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

These Images Look Similar

<table>
<thead>
<tr>
<th>Strongly Agree</th>
<th>Agree</th>
<th>Neutral</th>
<th>Disagree</th>
<th>Strongly Disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

These Images Look Similar

<table>
<thead>
<tr>
<th>Strongly Agree</th>
<th>Agree</th>
<th>Neutral</th>
<th>Disagree</th>
<th>Strongly Disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Strongly Agree</td>
<td>Agree</td>
<td>Neutral</td>
<td>Disagree</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------</td>
<td>-------</td>
<td>---------</td>
<td>----------</td>
</tr>
<tr>
<td>These Images Look Similar</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>These Images Look Similar</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>These Images Look Similar</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

These images are of the Union Jack flag and 'The Scream' painting by Edvard Munch.
Put all the results onto a webpage or refer to thesis for results? Otherwise just too long for a publisher