Article Info

ABSTRACT

This paper reviews the method of classification of the types of images used in data concealment based on the perspective of the researcher’s efforts in the past decade. Therefore, all papers were analyzed and classified according to time periods. The main objective of the study is to infer the best types of images that researchers have discussed and used, several reasons will be shown in this study, which started from 2006 to 2017, through this paper the pros and the cons in the use of favourite types in the concealment of data through previous studies.

Keywords:

Compressions
Graphical format file
Image types
Steganography

1. INTRODUCTION

In steganography kin of message is not directly delivered to the recipient but converted through multimedia files of domain such as image, video, or audio. These multimedia files are then hidden with in another object know as cover text, the original message sent is separated from it [1], [2]. The use of steganography is widely utilized in various organization especially in communication between members of the military intelligence operatives or agents of companies. The reasons of using this are to hide secret message and for espionage purposes. If there is any doubt arises even when the security is accomplished the observer might know the concealed data behind the original message [3].

There are some terminologies is used in steganography which cover message, secret message, secret key, and embedding algorithm cover message serves as the carrier of the message in some domain. A secret message is the information that is needed to be hidden in suitable digital media, while secret key serves as a mean to embed the hidden message depends on the hiding algorithm. Finally, embedding algorithm is a method used to embed the secret information in the cover message [4]. In other words, the aim of steganography is to conceal a mysterious message in cover media in a way that others are unable to detect it. In fact, “steganography implies concealing are of information inside another”. Currently, steganography hides data into a medium using the following component [5]:

a) The cover media (image, audio, video, text, other) that will hide data.

b) The secret message (image, audio, video, text, other) But the most widely used is plain text. However, theoretically we can use all data coming from multimedia as secret messages.

c) The stego function (embedding algorithm) we can call f(s) and its inverse f(s)-1. if you need to restore the hidden data

d) An optional secret key or stego-key (K) or using password to hide and conceal the message [4], [5].
2. APPLICATION IN IMAGE STEGANOGRAPHY

In the area of information security, this has led to a renewed interest in steganography, image are one of the most widely used groups of steganography and have been extensively used for security of information. Currently investigators have examined the effects of property on steganography. Steganographic procedures insert a message inside a cover. The different highlights describe the quality and shortcomings alert strategies. Each feature is relatively important as it depends on a certain application [10]-[11] such as capacity. The idea of capacity in information covers up a total number of bits, and effectively recouped by stego system [10]-[11]. The second feature is robustness. Robustness alludes to the capacity of the embedded in-formation to stay in place if the stage-system undergoes transfor-matio. For example, non-liner and liner filtering’s, random noise addition, rotation, scaling, and loose compression [11], [12]. All this is shown in Figure 1:

![Figure 1. Application features in the image steganography](image)

If there is a picture with an implanted message that is steady from where the pictures are drawn and the embedded algorithm is undetectable. For instance, in utilizing the commotion segment of an advanced picture steganography strategy is needed in order to embed a secret message. This is done without rolling out measurable improvement to the noise in the carrier. The infacility to detect the hidden message is information by the measurement of the secret message and the configuration of the cover image content [11]. Meanwhile, invisibility (perceptual transparency) is an idea that depends on human visual or sound systems. The implanted data becomes subtle if a normal human being is an able to recognize between the bearers with concealed data, and the ones without the data [11], [12]. It is essential that there is no significant degradation or any loss of perceptual quality of the cover in the embedding process. Security is the final feature in the embedded algorithm is safe if these is no removal to the information even after it is being discovered by an attacker. After all it depends on the total information of the embedded algorithm and the secret key [10], [12].

3. RELATED REVIEW

The review is based on two parts which are image compression types and proportion file format used.

3.1. Image Compression Types

For the beginning it explore the causes of the selection of researchers in the two types of image compression in the use of data concealment. According to Figure 2 the lossy compression has the largest proportion compared to the lossless compression. This is because vary small file size and a lot of tools, plugins and software support the largest proportion. In addition, the reluctance of some researcher because of quality degrades with the highest proportion of compression that make it hard to return to it is original size after compressing process. Meanwhile, the lossless compression is low among some researchers who believe that it is actually not a loss of quality last rather a slight decrease in image file sizes.it may also be form their view that larger files than if you were to use lossy compression [1], [3], [5], [7], [8], [12], [13]-[50].
3.2. Graphical File Format Used

There are five major graphical file formats used which is shown in Figure 3. The largest proportion is represented by raster format followed by vector format, raw format and compound format of the smallest proportions is the metadata format.

Most researchers tend to study and use raster format as they believe that the graphics are highly suitable for non-linear art images such as digitalized photographs, scanned artwork or detailed graphics. This is because there are subjective chromatic gradations undefined lines, shapes, and complex composition present in raster format. However, the disadvantage of this format is the image might suffer from a malady called image degradation because raster image are pixel-based. As a result, the image might get blurry and imprecise when blown up, jagged, and rough like wise seen in photographic, image. In up-close, a person can see individual pixels comprise the image. For example, raster-based logo can be magnified to 1000 [15], [46]-[49]. When studying in depth the study of which types of raster images researchers prefer to study jpeg is the most popular as it has high controlled degree of compression is characterized by small file size. The format is compatible as if displays exactly how the images appear to be in any browsers, text and graphic programmers, on all computers, tablets and mobile devices. It is indeed applicable to be used in full-color realistic image with many color and contrast transitions as the picture quality is high with small degree of compression. All the above reasons made this genre a favorite for researchers to study and choose in their research [5], [16], [26]-[41], [50].

4. CONCLUSION

The most obvious finding to emerge from this study is by studying the research related to the concealment of data during the last decade and finding out the reasons for selecting a type of image and requiring other types to represent all kinds of images which can hide the data the generalizability of these results is subject to certain limitations as shown in Figure 4 and Figure 5.
For instance, the size of the data to be hidden depends on the size image used and the speed of the medium of the carrier is also one of the most important factors that we must consider to easy transfer which will reduce the amount of data transferred. There is also another factor easy to deal with the type of image transferred from in the applications which we have avoided. For example, dealing with raw type that is large but not all programs and applications can deal with it. Other factors also do not destroy the hidden data in species as if cannot maintain the information transferred after the dismantling of steganography of images to retrieve the hidden data.

ACKNOWLEDGEMENT

The authors wish to thank the Ministry of Higher Education Malaysia in funding this study under the Fundamental Research Grant Scheme (FRGS), S/O code 13576, and Research and Innovation Management Centre, Universiti Utara Malaysia, Kedah for the administration of this study.

REFERENCES

[38] Bhattacharyya, S., A survey of steganography and steganalysis technique in image, text, audio and video as cover carrier. Journal of global research in computer science, 2011. 2(4).


