Analytical Review on Graphical Formats Used in Image Steganographic Compression

Roshidi Din, Osman Ghazali, Alaa Jabbar Qasim
School of Computing, College of Arts and Sciences, Universiti Utara Malaysia, 06010 Sintok, Kedah, Malaysia

Article Info

Article history:

Received May 26, 2018
Revised Jul 27, 2018
Accepted Aug 10, 2018

Keywords:

Compressions
Graphical format file
Image types
Steganography

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.

Corresponding Author:

Roshidi Din,
School of Computing, College of Arts and Sciences,
Universiti Utara Malaysia,
06010 Sintok, Kedah, Malaysia.
Email: roshidi@uum.edu.my

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 messagein 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 have 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:

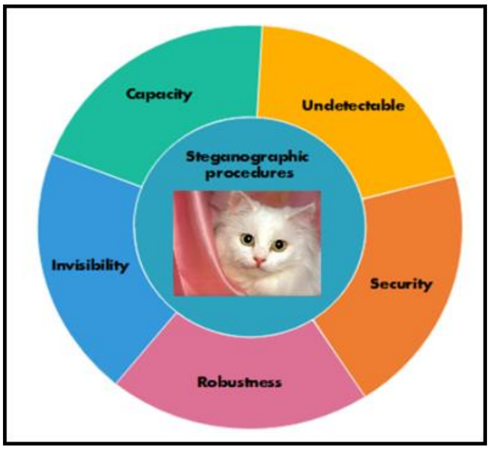

Figure 1. Application features in the image steganography

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].

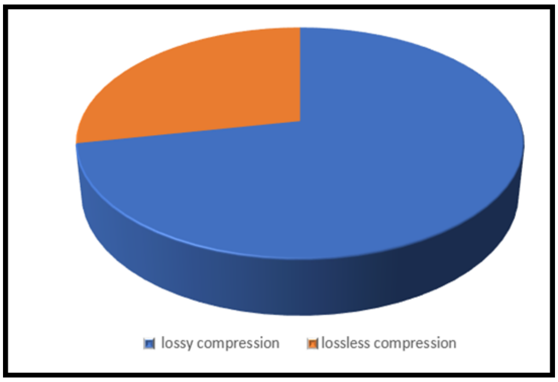

Figure 2. Image compression types that used in last decade

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 rester format followed by vector format, raw format and compound format of the smallest proportions is the metadata format.

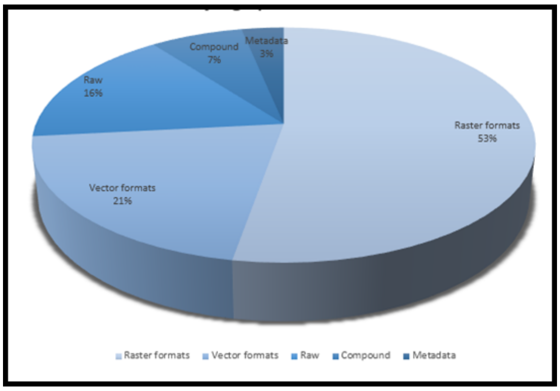

Figure 3. Percentage research of graphical file formats used

Most researchers tend to study and use raster format as they believe that the graphics are highly suitable for non-liner 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.

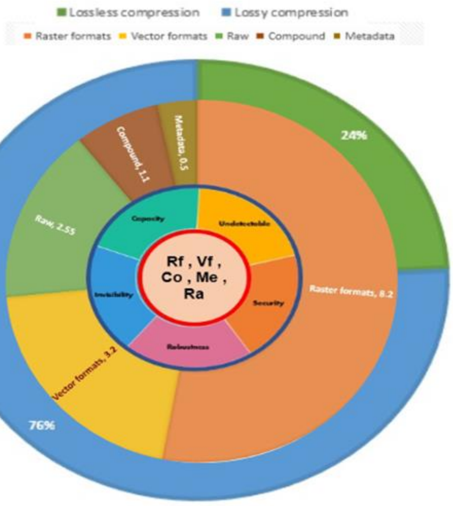

Figure 4. A summary of graphical file format used

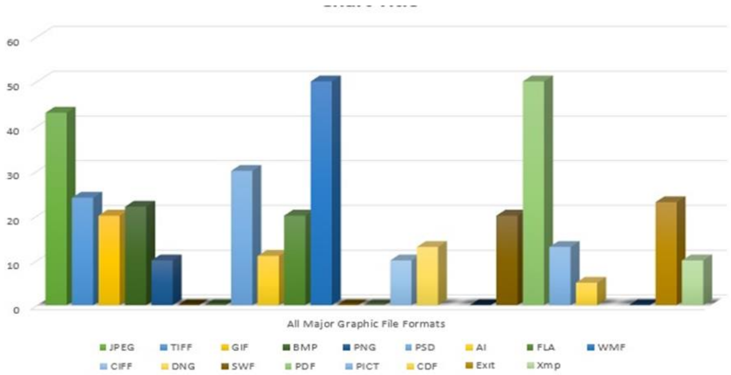

Figure 5. A chart bar of graphical file format used

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

[1] Bandyopadhyay, S.K., Bhattacharyya, D., Ganguly, Mukherjee, S. and Das, P. A tutorial review on steganography. International conference on contemporary computing. 2008, 1-10.
[2] Banik, B.G. and S.K. Bandyopadhyay, Review on Steganography in Digital Media.
[3] Das, S., Das, S., Bandyopahy, B. and Sanyal, S. Steganography and Steganalysis: different approaches. arXiv preprint arXiv:1111.3758, 2011.
[4] Fang, W.-P., A Data Hiding Method which the Secret Image Exist After Cropping Style Image Resizing.

[5] Fridrich, J. and J. Kodovsky, Rich models for steganalysis of digital images. IEEE Transactions on Information Forensics and Security, 2012. 7(3): p. 868-882.

[6] Kadum, S.A. and T.H. Abaidah, Enhancement an Algorithm to Hide a Text into a Digital Image as a Steganography Technique.

[7] Din, R., Samsudin, A., Muda, T.Z.T., Omar, M.N. Fitness value based evolution algorithm approach for text steganalysis model. International Journal of Mathematical Models and Methods in Applied Sciences, 2013.

[8] Din, R., Muda, T.Z.T., Lertkrai, P. and Omar. M.N. Text steganalysis using evolution algorithm approach. 2012. 11th WSEAS International Conference on Information Security and Privacy (ISP'12), 2012, 1-6.

[9] Johnson, N. and S. Jajodia. Steganalysis of images created using current steganography software. Information Hiding. 1998. Springer.

[10] Johnson, N.F. and S. Jajodia, Exploring steganography: Seeing the unseen. Computer, 1998. 31(2).

[11] Petitcolas, F.A., Anderson, R.J. and M.G. Kuhn, Information hiding-a survey. Proceedings of the IEEE, 1999. 87(7): p. 1062-1078.

[12] Dunbar, B., A detailed look at Steganographic Techniques and their use in an Open-Systems Environment. Sans Institute, 2002. 1.

[13] Bhavsar, J.H. and Khan, I. Techniques of Steganography and Steganalysis. Information Technology and System.2012. 1-4.

[14] Shrivastava, G., A. Pandey, and K. Sharma. Steganography and its technique: Technical overview. Proceedings of the Third International Conference on Trends in Information, Telecommunication and Computing. 2013. Springer.

[15] Jalab, H., A. Zaidan, and B. Zaidan, Frame selected approach for hiding data within MPEG video using bit plane complexity segmentation, 2009.

[16] Frączek, W., W. Mazurczyk, and K. Szczypiorski, Hiding information in a stream control transmission protocol. Computer Communications, 2012. 35(2): p. 159-169.

[17] Stallings, W. and M.P. Tahiliani, Cryptography and network security: principles and practice. Vol. 6. 2014: Pearson London.

[18] Swain, G., Digital image steganography using nine-pixel differencing and modified LSB substitution. Indian Journal of Science and Technology, 2014. 7(9): p. 1444-1450.

[19] Abraham, A. and M. Paprzycki. Significance of steganography on data security. in Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on. 2004. IEEE.

[20] Qiao, T., et al., Steganalysis of JSteg algorithm using hypothesis testing theory. EURASIP Journal on Information Security, 2015. 2015(1): p. 1.

[21] Memon, Q.A., Embedding Authentication and DistortionConcealment in Images–A Noisy Channel Perspective. Proceeding of the Electrical Engineering Computer Science and Informatics, 2014. 1(1): p. 385-390.

[22] Kuo, W.-C. and S.-Y. Chang, Hybrid GEMD Data Hiding. Journal of Information Hiding and Multimedia Signal Processing, 2014. 5(3): p. 420-430.

[23] Islam, S., M.R. Modi, and P. Gupta, Edge-based image steganography. EURASIP Journal on Information Security, 2014. 2014(1): p. 1.

[24] Zhang, Y., et al., Research on embedding capacity and efficiency of information hiding based on digital images. International Journal of Intelligence Science, 2013. 3(02): p. 77.

[25] Holub, V. and J. Fridrich. Digital image steganography using universal distortion. in Proceedings of the first ACM workshop on Information hiding and multimedia security. 2013. ACM.

[26] Zeki, A.M., A.A. Ibrahim, and A.A. Manaf, Steganographic software: analysis and implementation. International Journal of Computers and Communications, 2012. 6(1): p. 35-42.

[27] Tayel, M., H. Shawky, and A.E.-D.S. Hafez. A new chaos steganography algorithm for hiding multimedia data. in Advanced Communication Technology (ICACT), 2012 14th International Conference on. 2012. IEEE.

[28] Ritchey, P.C. and V.J. Rego. Hiding Secret Messages In Huffman Trees. in Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2012 Eighth International Conference on. 2012. IEEE.

[29] Ren, S., T. Zhang, and D. Mu, Study of Reversible Information Hiding Scheme Based on GHM and ASA. Applied Mathematics Information Sciences, 2012. 2: p. 253-260.

[30] Kayarkar, H. and S. Sanyal, A survey on various data hiding techniques and their comparative analysis. arXiv preprint arXiv:1206.1957, 2012.

[31] Hamid, N., et al., A Comparison between using SIFT and SURF for characteristic region based image steganography. International Journal of Computer Science Issues, 2012. 9(33-3): p. 110-116.

[32] Choudhary, K., Image steganography and global terrorism. International Journal of Scientific & Engineering Research, 2012. 3(4): p. 12.

[33] Yang, B., et al., Steganography in Ms Excel document using text-rotation technique. Information Technology Journal, 2011. 10(4): p. 889-893.

[34] Raval, M., et al., Image Tampering Detection Using Compressive Sensing Based Watermarking Scheme. Proceedings of MVIP 2011, 2011.

[35] Li, B., et al., A survey on image steganography and steganalysis. Journal of Information Hiding and Multimedia Signal Processing, 2011. 2(2): p. 142-172.

[36] Kumar, K.S., et al., Performance comparison of robust steganography based on multiple transformation techniques. Int. J. Comp. Tech. Appl, 2011. 2(4): p. 1035-1047.

[37] Ibrahim, R. and T.S. Kuan, Steganography algorithm to hide secret message inside an image. arXiv preprint arXiv:1112.2809, 2011.

[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).

[39] Zaidan, B., et al., On the differences between hiding information and cryptography techniques: An overview. Journal of Applied Sciences, 2010. 10: p. 1650-1655.

[40] Shreelekshmi, R. and M. Wilscy, Preprocessing Cover Images for More Secure LSB Steganography. International Journal of Computer Theory and Engineering, 2010. 2(4): p. 546.

[41] Lin, C.-C. and P.-F. Shiu, High capacity data hiding scheme for DCT-based images. Journal of Information Hiding and Multimedia Signal Processing, 2010. 1(3): p. 220-240.

[42] Khare, A., M. Kunari, and P. Khare, Efficient algorithm for digital image steganography. Journal of Information Science, Knowledge and Research in Computer Science and Application, 2010: p. 1-5.

[43] Hmood, A.K., et al., On the accuracy of hiding information metrics: Counterfeit protection for education and important certificates. International Journal of Physical Sciences, 2010. 5(7): p. 1054-1062.

[44] Hmood, A.K., et al., On the Capacity and security of steganography approaches: An overview. Journal of Applied Sciences, 2010. 10: p. 1825-1833.

[45] Filler, T. and J. Fridrich. Steganography using Gibbs random fields. in Proceedings of the 12th ACM workshop on Multimedia and security. 2010. ACM.

[46] Elnajjar, M., et al., Optimization Digital Image Watermarking Technique for Patent Protection. arXiv preprint arXiv:1002.4049, 2010.

[47] Chin-Wei, B. and M. Rajeswari, Multiobjective Optimization Approaches in Image Segmentation–The Directions and Challenges. Int. J. Advance. Soft Comput. Appl, 2010. 2(1).

[48] Al-Azawi, A. and M.A. Fadhil, Arabic text steganography using kashida extensions with huffman code. J. Applied Sci, 2010. 10: p. 436-439.

[49] Amirtharajan, R. and J.B.B. Rayappan, Steganography-time to time: A review. Res. J. Inform. Technol, 2013. 5: p. 53-66.

[50] Naji, A., et al., Novel approach for secure cover file of hidden data in the unused area within exe file using computation between cryptography and steganography. International Journal of Computer Science and Network Security. 2009. 9(5): p. 294-300.