International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 6, Issue 2, March - April 2017 ISSN 2278-6856

Optimal Specifications for a Secure Image Steganography Method

AbdulgaderAlmutairi

College of Sciences and Arts in ArRass,
Qassim University, Kingdom of Saudi Arabia

Abstract:*Nowadays, computer-based communications are important and crucial to the modern life, as they help people to share information, communicate with each other and exchange electronic documents among them. In fact, the ascendant's increase in the uses of the internet and multimedia has raised the interests in image steganography in order to secure and protect them. So far, several researches have been carried out in this area in order to identify and determine the most convenient optimal specifications for a secure image steganography method. In spite of that, the optimal specifications for a secure image steganography method have not been recognized yet. This paper comes out to state and classify these missing specifications. Therefore, a comprehensive survey on a variety of different methods, algorithms and schemes in image steganography was conducted in order to figure out and identify the optimal specifications for a secure image steganography method. Afterwards,the specifications for a secure image steganography method were shaped up according to this survey.*

Keywords: Component, Image Steganograph, Data Hiding, Cryptography in Image Steanography and Embedding and Extracting a Secret Message.

1. Introduction

Steganography is the science and an art of hiding a secret message in various files types such as text files, digital images files, digital audio files and digital video files. It is composed of two Greek words namely Stegano and Graphy. The word Stegano actually means covered whereas the word Graphy means writing. Therefore, steganography means covered writing[1, 2].Steganography is different fromcryptography ascryptography scrambles a message so it cannot be understood whereas steganography hides the message so it cannot be seen. Steganography is a form of security technique through obscurity, the science and art of hiding the existence of a message between the sender and the intended recipient [1, 3, 4, 5].

The goal of steganography is to hide (convey) the message under cover files, concealing the very existence of information exchange. Indeed, among a variety of files types, an image steganography is the preferred, since the altered image with slight variations in its colours will be indistinguishable from the original image by human eye [2].

In General, Steganography is classified into four types as follows [1]:

- *Text steganography*:In text steganography, information is concealed in text files. It includes anything from altering the formatting ofcurrent text, changing the word within the text, creating random sequences or using context-free grammars to produce readable texts.
- *Video steganography*: The gathering of images and sounds are known as video files.Hence, the majority of the existing techniques on images and audio can be applied to video files. Due to the fact that video is a moving stream of images and sounds, a huge amount of data can be concealed inside the video.
- *Audio steganography*: A secret message is embedded by using digital sound and this can be done by slightly changing the binary sequence of a sound file. This process is known as audio steganography.
- *Image steganography*: It is known as the process of hiding a secret image behind the cover image in such a way that the presence of the secret image is locked and the cover image seems to be the same [6-18].

Normally, Steganography requires three main components namely carrier object, secret data and steganography algorithm as shown in figure 1 and 2. Steganography can be used for many useful applications like secure transmission of top-secret data between international and national governments, online banking security, military and intelligent agencies security and safe circulation of secret documents among defence organizations[1, 19].

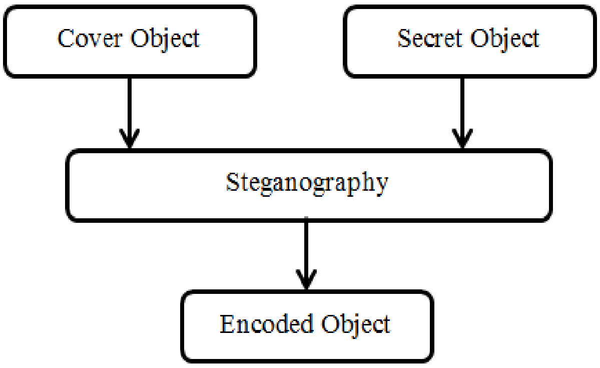

Fig. 1 Secret Object Encode Process

Broadly, image steganography has concerns onthe following aspects: capacity, security and performance[20]. This research concentrates on the security aspect.In addition to this, the research focuses on image steganography.Despite the fact that there are many different carrier file formats that can be used in steganography, the images are the most popular due to their frequency on the internet [2].

2. CATEGORIES OF STEGANOGRAPHIC TECHNIQUES

Steganography techniques categorized into two broad domains are as follows[1, 20-22]:

a. Spatial Domain Techniques

In spatial domain techniques, the pixels of carrier object like image and video objects are directly changed in order to hide secret data inside it. The following techniques belong to spatial domain[1][20-22]:

i. Least Significant Bit (LSB)

Least Significant Bit (LSB) is defined as a basic strategy toimplementsteganography.Like all steganographicapproaches, data is embedded into the cover such that a casual observer cannot detect it. The technique works by changing the information to a given pixel, with the information from the data in the image. Normally, an LSB algorithm replaces the most of the right bits of cover files bytes. In case a bit of the cover imageC(i,j) is equal to the bit of secret massage (SM) to be embedded, C(i,j) remains unchanged, otherwise C(i, j)is set to bit of secret message (SM) [1][23]. For example, the letter 'A' is an ASCII code of 65 in decimal, which is 01000001 in binary and bits of the image pixels before hiding(embedding) a secret message are as follows:

Pixel 1: 1111100**0** 1100100**1** 0000001**1**

Pixel 2: 1111100**0** 1100100**1** 0000001**1**

Pixel 3: 1111100**0** 1100100**1** 00000011

Least Significant Bit (LSB) algorithm hides (embeds) bits of letter 'A', which are **01000001** into image pixels in order to produce:

Pixel 1: 1111100**0** 1100100**1** 0000001**0**

Pixel 2: 1111100**0** 1100100**0** 0000001**0**

Pixel 3: 1111100**0** 1100100**1** 00000011

ii. Gray-Level Modification (GLM)

Gray Level Modification (GLM) is identified as a technique in which the gray level values of the image pixels are altered in accordance with a mathematical function, to represent binary data. Each pixel has a distinct gray level value, which can have even or an odd value. This even or odd value of the grey level is suitablychanged to represent binary data [24].

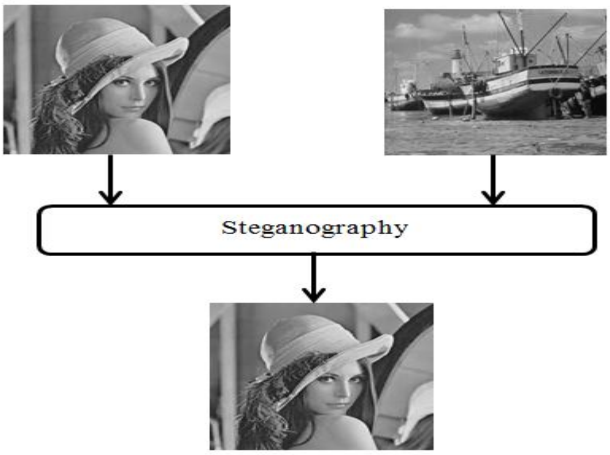

Fig. 2 Secret Object Encode Process with Lana image

iii. Pixel Value Differencing (PVD)

In Pixel-value differencing (PVD) scheme the difference value is used between two consecutive pixels in a block in order to define how many secret bits should be embedded. It provides high imperceptibility to the stego image by selecting two consecutive pixels and designs a quantization range table to determine the payload by the difference value between the consecutive pixels. Additionally, it offers the advantage of conveying a large number of payloads, while still maintaining the consistency of an image characteristic after data embedding [25].

b. Transform Domain Techniques

In transform domain techniques, the carrier object is first transformed from spatial domain to transform domain and then its frequencies are used to hide the secret data. After embedding the secret data, the object is again transformed into spatial domain. These techniques have lower payload but are robust against statistical attacks[1][20-22]:

i. Discrete Wavelet Transform Technique (DWTT)

The discrete wavelet transform (DWT) is an implementation of the wavelet transform that uses a discrete set of the wavelet scales and translations thereby obeying some defined rules [26].

ii. Discrete Fourier Transform Technique (DFTT)

The DFTT is the most important discrete transform that is used to perform Fourier analysis in many practical applications. In image processing, the samples can be the values of pixels along a row or column of a raster image [27].

iii. Discrete Cosine Transform Technique (DCTT)

A discrete cosine transform technique (DCT) expresses a finite sequence of data points in terms of a sum of cosine functions oscillating at different frequencies. DCTs are important to numerous applications in science and engineering forlossy compression of audio (e.g. MP3) and images (e.g. JPEG), where small high-frequency components can be discarded. The use of cosine rather than sine functions is critical for compression, asit turns out that fewer cosine functions are needed to approximate a typical signal [1][28].

3. Classifying existing image steganography methods in aspects of security

Based on reviewing of researches in [2][29-31], they can be classified into one or more of the following six features i.e. multilayer approach, method performance, method robustness, encrypting a secret message, unlimited image's size and image's formats.

In fact, only a method in the research [2] supported a multilayer approach feature, while other methods in researches [29-31] did not support it. Meanwhile, methods in researches [29-31] achieved a high method's performance feature, since their methods are based on LSB algorithm, which is reasonably fast in embedding and extracting a secret message.

However,a method in research [2] achieved a low method's performance feature because PWT algorithm requires a lot of mathematical calculations. At the same time, a research in [2] provided moderate method's robustness feature because it encrypted a secret message with AES algorithm and processed data hiding with PWT algorithm. Indeed, this method is suffering some obstacles like a secure distribution of AES key and requires a lot of mathematical calculations, which negatively affects the performance.

Other researches in [29-31] provided low method's robustness feature, since their methods were based on LSB algorithm that is easy to extract and recover the hided secret message. Also, they did not provide an encryption to the secret message. Besides that, methods in researches [2, 31] are able to process unlimited image sizes, while methods in researches [29-30] processed only limited image sizes. In addition, methods in researches [2, 29-30] supported all image formats, while method in research [31] supports only BMP & PNGimage formats. Finally, a research in [2] provided a secret message encryption feature using AES algorithm but it did not provide a secure distribution of AES key. Other researches in [29-31] did not provide a secret message encryption feature at all.

4. Optimal specifications for a Secure Image-Steganography Method in aspect of Security

Based on the survey unveiled in TABLE I above, this research that shaped up the optimal specifications for a secure image steganography method in aspect of security is as follows [36]:

- The method should consider a multilayer approach in its design in order to provide a robust secure data embedding (hiding) and extracting. Normally, the method consists of two consecutive layers i.e. one for a secret message encryption and decryption, while the second for embedding and extracting a secret message [19-22].
- The method should provide a quick reasonable performance during processing and manipulating image steganography, as an acceptable time frame of image steganography is required by the end users [19-22].
- The method should provide a secure embedding and extracting processes to a secret message in image steganography. The secure embedding and extracting processes should involve encrypting and decrypting a secret message with extremely strong cryptographic algorithm and secure distribution of cryptographic algorithm's key. As well, it should involve unbreakable embedding process for unauthorized parties [2-5, 19, 32-35].
- It should also include a secure design for embedding and extracting a secret message and a proposed method should be designed based on strong techniques such as randomized embedding, extracting techniques and statistical based techniques [1, 19-22].
- The method should be able to process unlimited image sizes due to spreading different image sizes on the internet [19-22].
- The method should support all image formats because limit support of image formats restricts spreading of the proposed method [6-22].
- The method should provide an encryption and decryption layer. In this layer, only recommended cryptographic algorithms like AES, RSA, Elliptic Curve, SHA256, SHA512 and SHA3 should be used. In addition, merely secure algorithms and techniques for distributing cryptographic algorithms' keys like public key distributions should be used [3-5, 32-35].

5. CONCLUSION

In this paper, firstlya comprehensive survey on a variety of different methods, algorithms and schemes in image steganography is conducted. As the survey shows, none of the previous researcheswere successful in providing completefeatures in image steganography method, algorithm or scheme due to absence of optimal specifications. Hence, this paper intended to classify and state these optimal specifications. Finally, the optimal specifications for a secure image steganography method are shaped up and described as well.

TABLE I. A COMPREHENSIVE SURVEY ON EXISTING IMAGE STEGANOGRAPHY METHODS IN ASPECT OF SECURITY

No.	Research	Multilayer Approach	Method Performance	Method Robustness	Unlimited Image Size	Image Formats	Encryption	
							Secret Message	Key
1	A Modified Image Steganography Method based on LSB Techniques [29].	No	High (LSB1&LSB2)	Low	No	All	No	No
2	MLSB Technique based on 3D Image Steganography Using AES Algorithm [2].	Yes	Low (DWT)	Moderate	Yes	All	Yes (AES Algorithm)	No
3	A Proposed Algorithm for Steganography in Digital Image based on Least Significant Bit (LSB) [30].	No	High (LSB1&LSB2)	Low	No	All	No	No
4	A Comprehensive Image Steganography Tool using LSB Scheme [31].	No	High (LSB1&LSB2)	Low	Yes	BMP & PNG	No	No

REFERENCES

[1] S. Kurane, H. Harke, and S. Kulkarni, "TEXT AND AUDIO DATA HIDING USING LSB AND DCT A REVIEW APPROACH," Natl. Conf. "Internet Things Towar. a Smart Futur. "Recent Trends Electron. Commun., 2016.

[2] E. Nandhini, M. Nivetha, S. Nirmala, and R. Poornima, "MLSB Technique Based 3D Image Steganography Using AES Algorithm," J. Recent Res. Eng. Technol. ISSN, vol. 3, no. 1, p. 2936, 2016.

[3] A. Hasan, "Computer Security," 2010. [Online]. Available: http://www.contrib.andrew.cmu.edu/~aishah/Sec.html.

[4] J. Talbot and D. Welsh, "Complexity and Cryptography," pp. 1–9, 2006.

[5] Sarciszewski, "Guide to Cryptography," 2015.

[6] E. R. Harold, "What is an Image," 2006.

[7] B. N. Chary and B. Sreenivas, "Processing of satellite image using digital image processing," 2011.

[8] S. shica and D. K. Gupta, "Various Raster and Vector Image File Formats," Ijarcce, vol. 4, no. 3, pp. 268–271, 2015.

[9] P. Hansen, "PNG 8, 24, 32," 2011. [Online]. Available: http://www.patrickhansen.com/blog/2011/02/04/png-8-24-32-what/.

[10] W. N. Ibrahem, "Types of Digital Images," pp. 1–13, 2014.

[11] Manifold, "Image Types," 2011. [Online]. Available: http://www.georeference.org/doc/image_types.htm.

[12] Willamette, "Image File Formats," 2012. [Online]. Available: http://www.willamette.edu/~gorr/classes/GeneralGraphics/imageFormats/. [Accessed: 20-Jun-2010].

[13] H. K. Kelda and P. Kaur, "A Review: Colour Models in Image Processing," Int. J. Comput. Technol. Appl., vol. 5, no. 2, pp. 319–322, 2014.

[14] P. M. Nishad and R. Manicka Chezian, "Various Colour Spaces and Colour Space Conversion," J. Glob. Res. Comput. Sci., vol. 4, no. 1, pp. 44–48, 2013.

[15] M. Kharinov, "Information quantity in a pixel of digital image," arXiv1401.7517 [cs, math], no. 2, pp. 1–11, 2014.

[16] M. Studio, F. Digital, and M. Workshops, "digital image," pp. 3–7, 2012.

[17] M. J. Dahan, N. Chen, A. Shamir, and D. Cohen-Or, "Combining colour and depth for enhanced image segmentation and retargeting," Vis. Comput., vol. 28, no. 12, pp. 1181–1193, 2012.

[18] T. Zuber, "CHANNELS AND BIT DEPTH," 2010. [Online]. Available: http://www.zuberphotographics.com/content/digital/bit-depth.htm

[19] K. Muhammad, "A Secure Cyclic Steganographic Technique for Colour Images using Randomization," Tech. Journal, Univ. Eng. Technol. Taxila, 2014.

[20] M. H. and M. Hussain, “A Survey of Image Steganography Techniques,” Int. J. Adv. Sci. Technol., vol. 54, pp. 113–124, 2013.

[21] N. Hamid and R. B. Ahmad, “Image Steganography Techniques: An Overview,” no. 6, pp. 168–187, 2012.

[22] J. Kour and D. Verma, “Steganography Techniques – A Review Paper,” Int. J. Emerg. Res. Manag. &Technology, vol. 9359, no. 35, pp. 2278–9359, 2014.

[23] A. MILLER, “LEAST SIGNIFICANT BIT EMBEDDINGS: IMPLEMENTATION AND DETECTION,” 2012. [Online]. Available: http://www.aaronmiller.in/thesis/.

[24] E. C. Vidyasagar M. Potdar, “Grey Level Modification Steganography for Secret Communication,” 2004. [Online]. Available: https://www.researchgate.net/publication/4137627_Grey_level_modification_steganography_for_secret_communication.

[25] H.-W. T. and H.-S. Leng, “A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number,” 2013. [Online]. Available: http://www.hindawi.com/journals/jam/2013/189706/.

[26] C. A. Petr Klapetek, David Nečas, “Wavelet Transform,” 2016. [Online]. Available: http://gwyddion.net/documentation/user-guide-en/wavelet-transform.html.

[27] R. Wang, “Discrete-time Fourier transform,” Introd. to Orthogonal Transform., no. 1, pp. 146–219, 2013.

[28] Anitha, “Transform & Discrete Wavelet Transform,” vol. 2, no. 8, pp. 1–6, 2011.

[29] M. M. Emam, A. A. Aly, and F. A. Omara, “A Modified Image Steganography Method based on LSB Technique,” Int. J. Comput. Appl., vol. 125, no. 5, p. 9758887, 2015.

[30] A. E. Mustafa, A. M. F. Elgamal, M. E. Elalmi, and A. Bd, “A Proposed Algorithm For Steganography In Digital Image Based on Least Significant Bit,” Res. J. Specif. Educ., no. 21, 2011.

[31] Sahar A. El_Rahman, “A Comprehensive Image Steganography Tool using LSB Scheme,” I.J. Image, Graph. Signal Process., 2015.

[32] S. Karthik and A. Muruganandam, “Data Encryption and Decryption by Using Triple DES and Performance Analysis of Crypto System,” vol. 2, no. 11, 2014.

[33] P. Mahajan and A. Sachdeva, “A Study of Encryption Algorithms AES, DES and RSA for Security,” vol. 13, no. 15, 2013.

[34] R. Biswas, S. Bandyopadhyay, and A. Banerjee, “A FAST IMPLEMENTATION OF THE RSA ALGORITHM USING,” pp. 1–15, 2014.

[35] P. Gupta and S. Kumar, “A Comparative Analysis of SHA and MD5 Algorithm A Comparative Analysis of SHA and MD5 Algorithm,” no. July, 2014.

[36] Mohammed A. Saleh and Azizah Abdul Manaf. Optimal Specifications for a Protective Framework against HTTP-based DoS and DDoS Attacks. International Symposium on Biometrics and Security Technologies (ISBAST 2014), May 2014 (IEEE).