Steganography Techniques

Prapti Sharma, Shweta Goyal.

Graphic Era University.Dehradun-248001.

Abstract

Steganography is an vital region of study in current years relating a number of applications. It is the discipline of hiding information into the envelop picture viz., text, video, and image without making any major alteration to the cover image. In this paper, we examine various steganography techniques and implements. We declare a set of criteria to analyze and assess the strengths and weaknesses of the existing techniques.

1. Introduction

Similar to cryptography, steganography provides a way of communicating covert messages. While cryptography scrambles a message so that it cannot be tacit, steganography hides the very subsistence of the message by hiding it within a mover case of some kind An eavesdropper can catch cryptographic message , but can not still know a steganographic message exists. Encryption and steganography attain the alike aim by different way. Encryption encodes the facts so that an unintended receiver cannot resolve its planned significance. Steganography, in contrast attempt to stop an inadvertent recipient from suspecting that the facts is there[4]. Combining encryption with steganography allows for a improved personal communication. The aim of steganography is to shun drawing suspicion to the spread of the covert communication. On other hand steganalysis is a means of detecting probable covert message using against steganography.It relies on the truth that hiding information in digital medium alters the carriers and introduces bizarre signatures or some form of degradation that could be oppressed. Thus, it is vital that a steganography system to determine that the unseen messages are not noticeable.

A steganography system is generally tranquil of inclusion and removal of subsystems .The inclusion structure takes a host file, a arranged message file, and an elective type to insert the message into the host for creating a wrap host. This is referred to as the embedding procedure. The wrap host is then stored or transmitted. The extraction system operates in reverse It takes a secret host and an optional type as input and extracts the message. Some steganography systems have several forms of built in encryption and will routinely encrypt and decrypt. the message as piece of the course. Using the steganography, communicating messages can be unseen in different medium including text, audio, and image records. Such files are called carriers.

In the residual of the paper, we talk about different types of steganography techniques and tools and scan them against a set of criteria. We intend a fresh technique, which has been implemented and validated.

II.STEGANOGRAPHY TECHNIQUES

A. TEXT STEGANOGRAPHY

This involves something from altering the format of an existing text, altering words inside a text or generate readable texts. It is not clear if a safe and strong steganography is probable with text messages. For instance, a reformat of the text may obliterate the information encoded in the text. In addition, text messages may be able to be stored in dissimilar formats such as HTML, Postscripts, or PDF; the alter from one format to another may be destructive to the implanted messages. Text hiding techniques comprise: The Line-Shift coding, Word shift coding, Feature coding, Syntactic technique and cover generation technique[4,9,10].

B. AUDIO STEGANOGRAPHY

Similar to text files, sound records may be customized in such a way that they contain concealed information [8]. Such techniques embed information in sound files by the properties of the Human Auditory System (HAS). Examples of audio steganography techniques comprise least significant bit, phase coding and echo Hiding.

C. STEGANOGRAPHY IN NETWORKS

Information can be concealed in one of the OSI layers. For instance, the network cover hides information by IP headers used for routing information. The vacant IP header bits (e.g. the DF and MF bits) or the two idle bits (the least

D. IMAGE STEGANOGRAPHY

Compared to other type of steganography,Image steganography has fascinated wide study as well as popular usability in latest years. This is due to the reality that huge amounts of facts can be buried with no noticeable impact to the carriers and perhaps because of the fame of electronic images that have turn into usually accessible. With this in intellect, we explain steganography techniques and tools that use image records in more facts. We present a set of criteria to appraise them. appropriate to limited gap, we comprise a subset of the tools that we have considered and compared..

A premature job on the image steganography is Least Significant Bit technique (LSB) [3, 8, 10]. This technique is simple in together with the embedding and de-embedding (extracting messages) processes, but undergo several disadvantages. Fridrich et al. [14] point out that recent advances in steganalysis have shown that LSB does not guarantee detectability, evidenced by the fact that they can be successfully attacked using statistical [15], or even visual attacks [13]. additionally, it is very vulnerable. for instance, re-saving in a BMP image can obliterate the concealed information [3]. additionalyl, this technique is not appropriate for JPEG and GIF format.

A variety of Palette-based image techniques have been investigated [5,6,7,8,9]. Messages may be embedded in the palette indices [9]. The palette might seem doubtful (thus detectable) as pointed out in [12]. Efforts by Machado [7] are intended to decrease deformation by embedding message in the LSB of the palette colors channel. Due to the replica colors, the palette might be detected with no trouble as observed by Fridrich [16].A development effort, Fridrich [5] planned a new technique using parity of palette color. Westfeld [6] presents F5 in which an development effort, Fridrich [5] planned a new technique using parity of palette color. Westfeld [6] presents F5 in which the DCT (Discrete Cosine Transform) coefficient's total values of a JPEG image is decremented in its place of overwriting the LSBs in an attempt to protect against the planned statistical and deformation attacks. additionally, message bits are dispersed over the whole envelop image, to protect against the ocular attack. It has been pointed out that the F5 algorithm destroys stego- image histogram [16] and that it can be broken [20], thus detected. Provos [17] included error modification technique in Outguess. It uses a 2-pass algorithm, where bits are embedded in the first go by and changes are finished to DCT coefficients in the second one to equal the histogram of DCT coefficients of the stego-image with that of the cover image. A main disadvantage of using DCT coefficient's techniques is to facilitate the stego-images that can only be stored in the JPEG format. Many of the live steganographic tools were developed upon these techniques. Such tools include S-Tools, Hide & Seek, and Hide4PGP [7, 12,16,18].

An extra stylish technique is planned in [2,11] where all envelop bits can be accessed in the embedding procedure. It is referred to as pseudorandom variation technique. In this technique, the covert message bits can be dispersed randomly over the entire cover. In the Encoding procedure, the outputs of a random numeral producer are used as index embedded communication bits are. In this method the confidentiality may be superior as it is not certain that following message bits are embedded in the same order. since it is the case with LSB, part of facts that are arbitrarily stored in LSB may be misplaced. In addition, it may create a extremely loud image.

III. ASSESSMENT CRITERIA OF TECHNIQUES AND TOOLS

In an attempt to suggest a more safe technique, we examined the image steganography techniques and tools beside a situate of criteria. We measured more than 15 tools. Due to limited space, we point out a number of of them here. The assessment criteria are given below and the comparisons are briefed in Tables 1 and Table 2.

1) Intensity of Visibility(noticeable or hardly noticeable): Steganography techniques must embed information in such a manner that rooted data depart no traces or symbols of steganography use. The visibility is directly inclined by the size of the covert message, the design and the content of the carrier image. It is indicated by the acronym PER in the comparison tables. In the tables, V is visible and I is not.

2) Detectability (DET): This is a critical criterion. The achievement of a technique may be viewed by the difficulty concerned ing detecting the concealed information in the mover. It ranges from High (H) to Low (L).

3) Strength (STR): The embedded information must endure any reprocessing process for the envelop which may go through and still conserve its reliability.

4) Competence (COMP): This concerns the amount of information that can be accepted in a cover image. There is a trade-off between the capacity (message size) and robustness. For example the LSB techniques have the capability to hide larger amount of information in aenvelop image but a small reprocessing to the resulted image will obliterate information completely.

5) Domain Type (DOM): DOM is either Spatial(S) or Transform (T). The techniques that use alter domain hide information in important areas of the envelop images and may be more composite for attackers.

6) File Format Dependency (DEP): Some techniques are dependent on exact format of a mover type while others allow for additional freedom.

CRIT TECH	DOM	DEP	DET	NOTICE	STR	COMP
LBS	S	Y	H	V	L	H
PP	S	Y	H	V	M	H
PW	S	Y	M	I	L	H
PO	S	Y	H	V	L	L
PI	S	Y	H	V	L	L
MD	T	Y	L	I	M	L
ML	T	Y	M	I	M	M

TABLE 1 :Evaluation of the Stega-techniques.

The techniques that have been examined beside the above criteria are: Least Significant Bit (LSB), Pseudorandom permutations(PP), Patchwork technique(PW), Palette-based using the palette order(PO), Palette-based using the image (PI), Modulating the relative size of two DCT coefficients(MD), Manipulating the LSB's of the DCT coefficients(ML). Table 1 summarizes the comparison. In Table 2, FTYP indicates file type, CAR is for carrier, and E for encryption. It compares few tools.

CRIT TOOL	Technique used	Notice	FTYP	CAR	E
EZSTEGO	Palette/LSB	I	TXT	GIF	N
Gif-it-up	LSB	I	ANY	GIF	Y
Gifshuffle	Palette	I	M/TXT	GIF	Y
Pretty God envelope	Append data to end of file	I	ANY	ANY	N
S-Tools	LSB	I	ANY	BMP	Y
F5	DCT coefficient	I	ANY	JPEG	Y

IV. THE PROPOSED TECHNIQUE:

The Invisibility and undetectability criteria are vital requirements of booming steganographic schemes. That is, a proposed technique must not demean the image reliability by introducing a precise pattern in the created stego-image, thereby, disallowing differences between the stego-image and the cover image in all probable visual or numerical attacks Our proposed technique emphasizes undetectability. It allows for the change of the plans strength of (24 bit) colored image to embed covert message in a exact distance between them. It is based on altering the distance of two random selected pixel channels in a exact range that signify hidden data. It is intended to be vigorous against deformation. It takes into account other significant criteria such as safety and ability allowing for the growth of a booming steganographic system. The security is accounted for by adapting a vigorous encryption algorithm. A high capacity is achieved by compressing encrypted message, and with many carriers to fit secret message.

The two major phase of technique are: The embedding and the de-embedding. In the embedding procedure, sequences of distance differences and binary values that are generate in the preprocessing are utilized. Each distance between two random pixel channels will implant one message bit by adjusting the distance to the nearby value in the distance difference sequence whose binary value is the same to the message bit. In the de- embedding phase, the stego-key is used to create the same distance differences and binary sequences as those used in the embedding procedure. For each arbitrary selected pixel channels the closest distance between them is computed to find the hidden message from the parallel binary value.

Encoding:

1)Study image files.
2) Reduce covert file.
3) Encrypt covert file.
4) Analyse competence of covert file.
5) If the cover competence is not enough goto step 1.
6) else repeat
   I. Create binary sequence based on the key
   II. Create arbitrary distances series based on the key
   III. Obtain arbitrary pixel.
   IV. Obtain 2 arbitrary channels for this pixel
   V. Calculate distance between those channels
   VI. Match the distance between minimum error and have the same message bit.

Until the Covert file is terminated.

V. CONCLUSIONS

Decoding: Similar to coding but in reverse.
A tool implementing this method has been developed and tested by bearing in mind numerous image carriers that hide long messages. The line of the tool is a wizard-based allowing the user to go effortlessly through the process. There are two interfaces in the scheme one for the embedding phase and the other for the withdrawal
.

We have discussed numerous steganography techniques with an emphasis on image steganography. We file a set of criteria to look into the strengths and weaknesses of the presented techniques. We discussed the needs of more robust steganography techniques that obtain reward of the presented strengths and avoids the limitations. We also discussed and
compared a range of steganography tools. We have developed a new steganography technique and implemented a tool exemplifying its process. We have tested the tool using various images as carriers.

REFERENCES

[1] W. Bender, D. Gruhl, N. Morimoto, and A. Lu. Techniques for data hiding. In IBM Systems Journal, Vol. 35, Nos. 3-4, pages 313-336, February 1996.

[2] Aura, T., "Practical Invisibility in digital communication, in information hiding" First international workshop, proceedings, vol. 1174 of lecture notes in computer science , Springer, 1996, pp. 265-278.

[3] Johnson, N.F. and S. Jajodia. "Exploring Steganography: Seeing the Unseen." IEEE Computer Mag., February 1998.

[4] Westfeld, A., and G. Wolf, Steganography in a Video conferencing system, in proceedings of the second international workshop on information hiding, vol. 1525 of lecture notes in computer science, Springer, 1998. pp. 32-47.

[5] Pan ,H.K., Y.Y., Chen, and Y.C., Tseng, “A Secure Data Hiding Scheme for Two-Color Images”, Proc. Fifth IEEE Symp. Computers and Comm., IEEE Press, Piscataway, N.J., 2000.

[6] Westfeld, A.” F5-A Steganographic Algorithm: High Capacity Despite Better Steganalysis”, 4th International Workshop on Information Hiding ,2001.

[7] Curran, K. and K. Bailey, “ An evaluation of image-based steganography methods” International Journal of Digital Evidence ,Vol . 2 , issue 2, 2003.

[8] Kessler, G. “An Overview of Steganography for the Computer Forensics Examiner “, Computer & Digital Forensics Program, Champlain College, Burlington, Vermont, February 2004

[9] Rabah, K“ Steganography : The Art of Hiding Data” Information Technology Journal ,Vol 3 No.3, 2004 , pp. 245-269.

[10] Bennett, K. “Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text“ Technical Report, Center for Education and Research in Information Assurance and Security (CERIAS), 2004.

[11] J.M. Rodrigues, J.R. Rios and W Puech." SSB-4 System of Steganography using Bit 4". Proc. 5th International Workshop on Image Analysis for Multimedia Interactive Services, (WIAMIS'04), Lisboa, Portugal, April 2004.

[12] R. Chandramouli, M. Kharrazi, N. Memon, “Image Steganography and Steganalysis: Concepts and Practice “ , International Workshop on Digital Watermarking, Seoul, October 2004.

[13] Westfield, A., and A. Pfitzmann. “Attacks on Steganographic Systems - Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools - and Some Lessons Learned,” Lecture Notes in Computer Science, 1 768 : 61-75 (2000).

[14] Fridrich ,J, M. Goljan, and R. Du, “Detecting LSB steganography in color and grayscale images,” IEEE Multimedia Special Issue on Security, pp. 2 2^{2}8, October- November 2001.

[15] Avcibas, I. , N. Memon, and B. sankur, “Steganalysis using image quality metrics.” Security and Watermarking of Multimedia Contents, San Jose, Ca. , Feruary 2001.

[16] Fridrich, J., M. Goljan, , H. Dorin ,"Steganalysis of JPEG Images Breaking the F5 Algorithm". Information Hiding 2002, pp. 310-323.

[17] OutGuess Web Site ."Steganography Detection with Stegdetect ."URL: http://www.outguess.org/detection.php.Last accessed: 2004.

[18]] Fridrich, J., Goljan, M., and Hogea, D. " Attacking the OutGuess". In: Proceedings of the ACM Workshop on Multimedia and Security 2002, Juan-les-Pins, France, December 2002.

[19] Hatim A. Aboalsamh, Sami A. Dokheekh, Hassan I. Mathkour, Ghazy M. Assassa. “Breaking the F5 Algorithm: An Improved Approach”, Egyptian Computer Science Journal Vol.29 No 1. January 2007, pp 1-9