http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 4 (3): 284-288, 2005
ISSN 1812-5638

Proving Poverty of Steganography System

[1]Ala'a Al-Hamammi and [2]Maisa'a Hamed Al-Hamadani
[1]Faculty of Information Technology, Al-Ahliyya Amman University,
[2]University of Technology, Amman, Jordan

Abstract: The application of possible attacks and their success is necessary to evaluate the security of any steganography system. There are many types of application packages attacks such as filters and software used to destroy the hidden data in cover image, when the attacker couldn't detect the existence of the secret data. For that the easy way for the attacker is to submit the suspected image to different types of attack. Some of these attacks could be smoothing filters, image conversion, re-sizing, mosaic and visual pixel detection. Hiding in edge points, direct hiding and hiding in reference images are three methods of steganography. The three methods are applied for single and double hiding as a proposed steganography system that submitted to these kinds of attacks to prove and evaluate the strength of the proposed system. Finally the proposed system is proven success against some types of attack, but not all.

Key words: Steganography, software attacks, filters attack, stego image

INTRODUCTION

One concern of privacy in every day life is that one can communicate confidentially[1]. Steganography is an ancient art, going back as far as the need for secret communications go, it's the art and the science of hiding data into innocent-looking cover-data[2,3].

For secure covert communication it is important that by injecting a secret message into a cover document no detectable changes are introduced. The main goal is to not raise suspicion and avoid introducing statistically detectable modifications into the stego-document. The embedded information is undetectable if:

1. The image with the embedded message is consistent with the model of the source from which the cover image is draw[4].
2. The original cover medium needs to be an unknown, because the comparison between cover medium and stego medium reveals changes. If the adversary can not obtain the actual cover medium then the embedded message can not deduced by observing differences between the original and the stego medium.

Two necessary conditions for secure steganography:

1. The secret key is unknown to the adversary.
2. The adversary does not know the actual medium.

In practice, these two conditions are easily met. It suffices to create a cover medium with a digital camera or by scanning holding picture, as long as the unmodified original is not made publicly available[5]. The undetectability is directly influenced by:

1. The size of the secret message, the longer the message, the larger the modification of the cover image and the higher the probability that the modifications can be statistically detected.
2. The format of the image, (GIF and JPEG) are recognized by all browsers and are widely used over the Internet, posting these files on one's web page will undoubtedly raise less suspicion.
3. The content of cover image, natural photographs with 24 bits per pixel provide the best environment for message hidden. The redundancy of the data helps to conceal the presence of secret message. It appears that secure schemes in palette images should not manipulate the palette but rather embed message bits in the image data[4].

STEGANALYSIS

Steganograhy encompasses methods of communication in such a manner that the existence of the message should be undetectable[6]. Steganalysis is relatively new science of discovering, decoding and/or rendering useless covert messages hidden in a carrier file.

Corresponding Author: Dr. Alaa Al-Hamammi, Professor, Faculty of Information Technology, Al-Ahliyya Amman University, Zip Code 1928, P.O. Box 276, Amman, Jordan

The general purpose of steganalysis is to collect sufficient statistical evidence about the presence of hidden message in imagery[7].

Breaking a steganography system normally consists of three parts: Detection, Extracting and Destruction.

- Detection is usually the first step. Just knowing that someone is using a covert communication channel into or out of the network.
- Extracting is the next step in steganalysis would be decoding the detected file to see what is hidden inside.
- Destruction is the last step and it actually the easiest[8].

If the attacker can not confirm his hypothesis that a secret message is embedded in a cover, then a system is theoretically secure[6].

Since one of the main reasons to use steganography is to conceal the fact that a message is being hidden. Decoding a hidden message will be a very tough problem with analogous to cryptanalysis.

To decode a covert message where the attacker does not know:

1. The encoding method.
2. The format of the hidden message.
3. How to access to original version of the carrier file[8] and the key is only known for both sender and receiver[1].

Decoding process will be very complex and resource intensive. If the hidden file encrypted before it is merged into the cover file then, even if the user decodes the hidden message, it is still hidden again by an encryption algorithm. It is good for the embedded to know things that his adversary does not think he knows[8], despite of these obstacles the steganalysis still in an attempt to detect the existence of hidden information[6].

There are two kinds of attack against a stegosystem. One is passive attack to detect the existence of a secret message embedded in stego-data. The other is active attack to modify the stego-data slightly in order to distract the embedded data[9].

STEGANOGRAPHY SYSTEMS

There are many steganography systems invented in a few years later, because hiding process (especially in image) gives wide applications, so the information can be hidden many different ways in the cover and it depends on human to choose the appropriate positions for hiding.

Single and double hiding is one of steganography systems, this system hide the secret text file in cover image by using single hiding or double hiding.

Single hiding is designed to hide information in one step, this step will hide the secret message in cover image by providing one of the three methods, which are Hiding in edge points, direct hiding, or hiding in reference images.

Double hiding is designed to hide information in two steps, the first step hide the secret message in digital image (cover 2) and the second step hide the produced stego-image in cover image (cover 1) by using two hiding methods which are Hiding in edge points and hiding with reference images.

Generally the techniques that used in the system are pixel domain and transform domain[10].

ATTACK ON SINGLE AND DOUBLE HIDING SYSTEM

Attack on the hidden information may take several forms: detection, extracting, distracting, in the first form the attacker will not detect whether the existing image file is a stego image or not. The proposed system achieves the main goal of steganography by avoiding draw of a suspicion stego image. Concealing the very existence of the secret information and the cover image is not available to the attacker because the stego image is not popular image. If the attacker have a suspicion to the transmitted image, then he will try to extract the secret information, but the following points must be known:

1. The type of steganography, if it is a classical steganography then the techniques used for concealing the information must be known. If it is a modern steganography then the key and the techniques of the steganography that used for embedding message must be found.
2. The manner of choosing the pixels that is used in the hiding process.
3. The number of the bits of the secret message that are used to hide them in the pixel.
4. The hidden information is hiding indirectly.

So the attacker will gain just a collection of random characters, then he will think it is encryption information and apply the decryption process to it and will gain another level of random characters. In case of double hiding the process will be very complex to extract the secret information. The hidden information in this type is a dummy image which is used to confuse the attacker. If the attacker reaches to this level of extracting process and thinks that he succeed in finding the secret information. To reach to this progress in extracting process is very complex process because there is many levels that attacker must pass. These levels are extracting, decryption and finally decompression. So the process is very complicated for the attacker (not for the receiver) to have the real hidden information.

If the attacker can not detect and extract the secret information, then the image will either pass to the receiver or the third form of the attack on hidden information which is (distraction) will be applied. The stego image will be submitted to different types of digital image filters or software attacks, such as Stir-mark, Mosaic, or other attacks. In single and double hiding system the attack stage consist of three types, they are smoothing filters, image conversion, mosaic, re-sizing and visual pixel detection.

Smoothing filters: In this type there are many low-pass filters used with stego image to destroy the hidden data such as mean, median and other types of smoothing filters. In this attack the reference method will force these filters without destroying its content because the hidden data will be in the borders of the cover image and the smoothing filters can't reach the pixels in the border the effect of this filter is shown in Fig. 1.

Image conversion: Image conversion is one type of attack on stego image. This attack will destroy the hidden data in the image, because it works on the pixel format of the image. When the pixel format of the stego image changed (make it smaller or bigger) the data of the image will be changed, so any hidden data will change too. Direct Hiding method will force this type, because actually there is no secret message hidden inside the cover image. This attack is shown in Fig. 2.

Re-sizing attack: This attack will reduce the size of the stego image. The reducing process will be done by decreases the height, width, or both of the image, the proposed system for both types will this type of attack as shown in Fig. 3.

Mosaic attack: The Mosaic attack consists of chopping an image up into a number of smaller sub images and then stuck these sub images together, so they appear identical to the original image[11]. After applying this software on the stego image of the proposed system, the hidden data was destroyed, so the system can not force this type of the attack. The application of this attack is shown in Fig. 4.

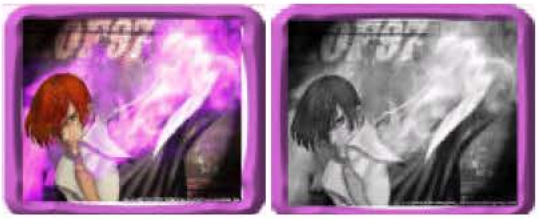

Image before process **Image after process**

Fig. 1: Smoothing filter attack (Mode filter)

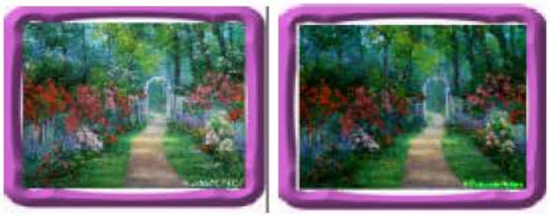

Image before process **Image after process**

Fig. 2: Image conversion attack

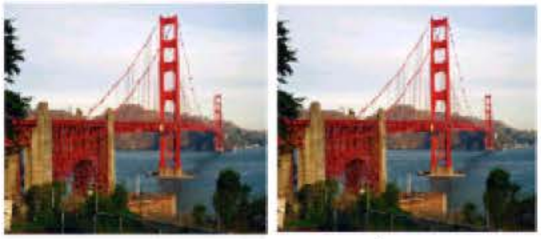

Image before process **Image after process**

Fig. 3: The result of re-sizing attack

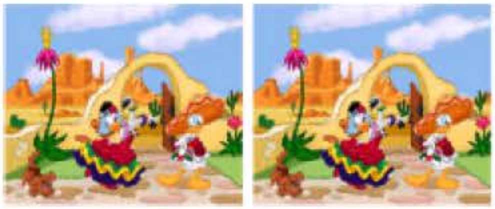

Image before process **Image after process**

Fig. 4: The mosaic attack

Visual pixel detection: The visual pixel detection works as a filter and it deals with BMP and GIF image file format only. Visual pixel detection filtering the pixels depends on its information and relation between other neighborhood pixels, this filter can remove from image pixels 1,2,3,4, or 5 bits then re-draw the image depends on these bits[1].

The effective of this filter on the proposed system will be discussed in the following points:

Table 1: The result of single and double hiding system with and without compression techniques

With compression techniques							
	Without encryption			With encryption			
Single hiding	Smooth filters	Visual pixel detection	Image conversion	Smooth filters	Visual pixel detection	Image conversion	Statistical tests
E.D. method	Yes	Yes	Yes	Yes	No	Yes	No detect
Reference	No	No	Yes	No	Yes	Yes	No detect
Direct	Yes	Yes	No	Yes	No	No	Detect
	Without encryption			With encryption			
Double hiding	Smooth filters	Visual pixel detection	Image conversion	Smooth filters	Visual pixel detection	Image conversion	Statistical tests
E.D. method	Yes	No	Yes	Yes	No	Yes	No detect
Reference	No	No	Yes	No	Yes	Yes	No detect
Without compression techniques							
	Without encryption			With encryption			
Single hiding	Smooth filters	Visual pixel detection	Image conversion	Smooth filters	Visual pixel detection	Image conversion	Statistical tests
E.D. method	Yes	Yes	Yes	Yes	Yes	Yes	No detect
Reference	No	Yes	Yes	No	Yes	Yes	No detect
Direct	Yes	Yes	No	Yes	Yes	Yes	Detect
	Without encryption			With encryption			
Double hiding	Smooth filters	Visual pixel detection	Image conversion	Smooth filters	Visual pixel detection	Image conversion	Statistical tests
E.D. method	Yes	Yes	Yes	Yes	Yes	Yes	No detect
Reference	No	Yes	Yes	No	Yes	Yes	No detect

Note: The "Yes" means that the techniques will effect by the attack tools, "No" means that the techniques will no effect by the attack

- Any stego image of JPEG file format will notsubmitted to this filter because, it does not deal with JPEG file format.
- For both types of the system the hiding in GIF-animation will not arouse any suspicion.
- In the proposed system the direct hiding and hiding in edge point will force this filter without any suspicion to the existence of the hidden data, but the hidden data in Hiding with Reference Image will be detected.

RESULTS

Table 1 allows fair comparison among all the suggested methods for both types of hiding in the proposed system, from expressing the application of the various kind of attacks and the effect on the suggested methods.

CONCLUSIONS

Followings are some points concluded from this research:

1. Single and double hiding proved it's resistance against some type of the attacks, but not all, because there is no existence for a secure system in the world.
2. Any type of attack depends on the size of the hidden data, as the size of the embedded data decrease, the immunity of the cover will be increased.
3. The type of hiding will not affect the submitted attacks.
4. Hiding with reference images is the only and the best method to be used against the smoothing filters.
5. Direct hiding truly didn't hide any secret data, this mean that it doesn't depend on the pixel format, so this method is candidate method to be used against image conversion.
6. From the experiments the attack operation in animated.
7. Stego file will force better than using still stego file.

REFERENCES

1. Franz, E. and A. Pfitzmann, 2000. Steganography Secure against Cover-Stego-Attacks. Information Hiding, Third International Workshop, Lecture Notes in Computer Science, Springer, 1768: 29-46.
2. Misamore, M., 2002. Steganography: using covert channel in the information Age. {http:// userpages.Umbc.edu/~mmisam1/papers/stego.htm}.
3. Provos, N. and P. Honeyman, 2001. Detecting Steganographic Content on the Internet. University of Michigan, USA.

4. Fridrich, J. and R. Du, 2000. Secure Steganographic Methods for Palette Images. Information Hiding. 3rd International Workshop, Lecture Notes in Computer Science, Springer, 1768: 47-60.
5. Provos, N., 2001. Probabilistic methods for improving information hiding. University of Michigan, USA.
6. Katzenbeisser, S. and F.A. Petitcolas, 2000. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House.
7. Fridrich, J., R. Du and M. Long, 2000. Steganalysis of LSB Encoding In Color Images. {http://citeseer.nj.nec.com/403441.html}.
8. Blacke, T.M., 2001. Steganalysis, PDF. {http://rr.sans.org/topappers/topapers_list.php}.
9. Shin, N., 2000. One-Time Hash Steganography. Information Hiding. 3rd International Workshop, Lecture Notes in Computer Science, Springer, 1768: 17-28.
10. Hameed Al-Hamadani, M., 2003. Concealment of information in digital image. Thesis submitted to the University of Technology, Amman, Jordan.
11. Petitcolas, F.A., R.J. Anderson and M.G. Kuhn, 1998. Attacks on Copyright Marking Systems. Information Hiding. 2nd International Workshop, Lecture Notes in Computer Science, Springer, 1525: 218-238.
12. Alaa Al-Hamami, M., 2002. Information Hiding Attack in image. Thesis submitted to the Informatic Institute for Postgraduate Students of the Iraqi Committee for Computers and Informatic.