International Journal of Computer Applications Technology and Research
Volume 3– Issue 9, 589 - 591, 2014, ISSN: 2319–8656

Steganography using Interpolation and LSB with Cryptography on Video Images-A Review

Jagdeep Kaur
Computer Science Department
UIET, Kurukshetra University
Kurukshetra, India

Abstract: Stegnography is the most common term used in the IT industry, which specifically means, "covered writing" and is derived from the Greek language. Stegnography is defined as the art and science of invisible communication i.e. it hides the existence of the communication between the sender and the receiver. In distinction to Cryptography, where the opponent is permitted to detect, interrupt and alter messages without being able to breach definite security grounds guaranteed by the cryptosystem, the prime objective of Stegnography is to conceal messages inside other risk-free messages in a manner that does not agree to any enemy to even sense that there is any second message present. Nowadays, it is an emerging area which is used for secured data transmission over any public medium such as internet. In this research a novel approach of image stegnography based on LSB (Least Significant Bit) insertion and cryptography method for the lossless jpeg images has been projected. This paper is comprising an application which ranks images in a users library on the basis of their appropriateness as cover objects for some facts. Here, the data is matched to an image, so there is a less possibility of an invader being able to employ steganalysis to recuperate the data. Furthermore, the application first encrypts the data by means of cryptography and message bits that are to be hidden are embedded into the image using Least Significant Bits insertion technique. Moreover, interpolation is used to increase the density

Keywords: Cryptography, Stegnography, LSB

1. INTRODUCTION

As living in the society, human beings have repeatedly sought innovative and well-organized ways to communicate. The most primitive methods included smoke signals, cave drawings and drums. With the advancements of civilization introduced written language, telegraph, radio/television, and most newly electronic mail. Nowadays, almost each and every communication is carried out electronically; new requirements, issues and opportunities are born. At times when we communicate, we prefer that only the intended recipient have the ability to decipher the contents of the communication in order to keep the message covert. One of the common solution to resolve this problem is the use of encryption. Whilst encryption masks the significance of a communication, instances do exist where it would be preferred that the entire communication process is not obvious to any observer, even the fact that communication is taking place is kept secret. In this case, the communication taking place is hidden. Steganography can be used to conceal or cover the existence of communication. A major negative aspect to encryption is that the existence of data is not hidden. Data that has been encrypted, although unreadable, still exists as data. If given an adequate amount of time, someone could eventually decrypt that data. A solution to this dilemma is steganography.

2. DIFFERENT KINDS OF STEGNOGRAPHY

Approximately all digital file formats can be used for stegnography; but the formats that are more appropriate are those with a high level of redundancy. The term redundancy can be defined as the bits of an object that provide accurateness far greater than needed for the object’s use and display. Also, the redundant bits of an object are those bits that can be changed without the alteration being detected easily. Image and audio files particularly meet the terms with this prerequisite, while research has also uncovered other file formats that can be used for information hiding.

Figure 1 shows the four main categories of file formats that can be used for steganography.

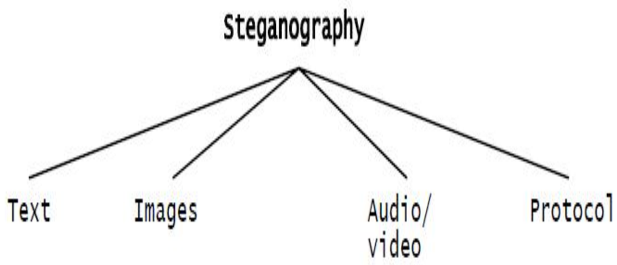

Figure 1 Types of Steganography.

Image steganography is about exploiting the inadequate powers of the human visual system (HVS). Within reason, any cipher text, plain text, images, or anything else that can be embedded in a bit stream can be concealed in an image.

Moreover, image steganography has come quite far in current years with the expansion of fast, influential graphical computers.

Digital image is the most important and common type of carrier used for steganography. A digital image is composed of finite number of elements each of which has a particular location and value (gray scale). The processing of these digital images by means of a digital Computer is referred as digital image processing. The images are used for steganography in the following ways.

The message or the data either in encrypted form or in the unique form is embedded as the covert message to be sent into a graphic file. This method results in the production of what is called a stego-image. An additional secret data may be required in the hiding process e.g. a stegokey. Furthermore, the stego-image is then transmitted to the receiver. After that, the recipient extracts the message from the carrier image. The message can only be extracted if both the sender and the recipient has a shared secret between them.

This could be the algorithm for extraction or a special parameter such as a key. A stego-analyst or attacker may try to intercept the stego-image. The computer based stenography allows changes to be made to what are known as digital carriers such as sounds or images. The changes represent the hidden message, but result is successful if their is no discernible change to the carrier. The information has nothing to do with the carrier sound or image. Information might be about the carrier such as the author or a digital watermark or fingerprint.

Stegnography applications that hide data in images generally use a variation of least significant bit (LSB) embedding . In LSB embedding, the data is hidden in the least significant bit of each byte in the image. The size of each pixel depends on the format of the image and normally ranges from 1 byte to 3 bytes. Each unique numerical pixel value corresponds to a color; thus, an 8-bit pixel is capable of displaying 256 different colors .Given two identical images, if the least significant bits of the pixels in one image are changed, then the two images still look identical to the human eye. This is because the human eye is not sensitive enough to notice the difference in color between pixels that are different by 1 unit. Thus, stegnography applications use LSB embedding because attackers do not notice anything odd or suspicious about an image if any of the pixel's least significant bits are customized.

3. CRYPTOGRAPHY

Cryptography[8] is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. In this paper we will focus only on confidentiality, i.e., the service used to keep the content of information from all but those authorized to have it.

Cryptography protects the information by transforming it into an incomprehensible format. It is useful to achieve private transmission over a public network. Also, the original text, or *plaintext*, is transformed into a coded alike called *ciphertext* via any encryption algorithm. Only those who hold a secret key can decipher (*decrypt*) the ciphertext into plaintext. Cryptography systems can be broadly classified into symmetric-key systems that use a single key (i.e., a *password*) that both the sender and the receiver have for their piece of work and a public-key systems that use two keys, a public key known to everyone and a private key that is unique and only the recipient of messages uses it. In the rest of this paper, we will discuss only symmetric-key systems.

Cryptography and stegnography are close cousins in the spy craft family: the former scrambles a message so it cannot be understood and the latter hides the message so it cannot be seen. A cipher message, for illustration, might arouse suspicion on the part of the recipient whilst an invisible message created with stegnographic methods will not.

In fact, stegnography can be useful when the use of cryptography is forbidden; where cryptography and strong encryption are barred, steganography can get around such policies to pass message covertly. However, stegnography and cryptography differ in the way in which they are evaluated; stegnography fails when the "enemy" is able to access the content of the cipher message, while cryptography fails when the "enemy" detects that there is a secret message present in the stegnographic medium .

The disciplines that study techniques for deciphering cipher messages and detecting hide messages are called *cryptanalysis* and *steganalysis*. The former denotes the set of methods for obtaining the meaning of encrypted information, while the latter is the art of discovering covert messages

4. DIFFERENCE BETWEEN CRYPTOGRAPHY AND STEGNOGRAPHY

In cryptography, the system is broken when the attacker can read the secret message. Breaking a stegnographic system has two stages:

1. The attacker can detect that stegnography has been used.

2. Additionally, he is able to read the embedded message.

In our definition a stegnographic system is insecure already if the detection of stegnography is possible (first stage).

5. CONCLUSIONS

The Steganography has its place in the security. On its own, it won't serve much but when used as a layer of cryptography, it would lead to a greater security.

Although only some of the main image steganographic techniques were discussed in this paper, one can see that there exists a large selection of approaches to hiding information in images. All the major image file formats have different methods of hiding messages, with different strong and weak points respectively. Where one technique lacks in payload capacity, the other lacks in robustness.

Steganography, particularly pooled with cryptography is a commanding tool which enables people to converse without possible eavesdroppers even knowing there is a form of communication in the first place. The proposed method provides acceptable image quality with very little deformation in the image. The main benefit of this System is to provide high security for key information exchanging. It is also useful in communications for codes self error correction. It can embed remedial audio or image data in case corruption occurs due to poor connection or transmission

6. REFERENCES

[1]Awrangjeb M (2003) An overview of reversible data hiding. ICCIT 75–79

[2]Celik MU, Sharman G, Tekalp AM & Saber E (2002) Reversible data hiding, Proceedings of IEEE 2002

International Conference on Image Processing 2, 157–160

[3]Chan CK, Cheng LM (2004) Hiding data in images by simple LSB substitution. Pattern Recognition 37:469–474

[4] Chang CC, Lin MH, Hu YC (2002) A fast and secure image hiding scheme based on LSB substitution. Int Pattern Recog 16(4):399–416

[5]GoljanM, Fredrich F & Du R (2001) Distortion-free data embedding, Proceedings of 4th Information Hiding Workshop, 27–41

[6] Huang LC, Tseng LY, Hwang MS (2013) A reversible data hiding method by histogram shifting in high quality medical images. J Syst Software 86:716–727

[7]Johnson NF & Jajodia S (1998) Exploring steganography: seeing the unseen. Comput Pract 26–34

[8]Jung KH, Yoo KY (2009) Data hiding method using image interpolation. Comput Standards Interfaces 31:465–470

[9] Artz, D., “Digital Steganography: Hiding Data within Data”, *IEEE Internet Computing Journal*, June 2001

[10] Hameed A. Younis, Dr. Turki Y. Abdalla, Dr. Abdulkareem Y. Abdalla , “ A Modified Technique For Image Encryption “,online access

[11] Simmons, G. J. The prisoners’ problem and the subliminal channel. In Advances in Cryptology: Proceedings of Crypto 83, pages 51–67. Plenum Press.

[12]Westfeld, A. (2001). F5-a steganographic algorithm: High capacity despite better steganalysis. In Proc. 4th Int’l Workshop Information Hiding, pages 289–302.2001