ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 1, pp: (27-35), Month: January-March 2014, Available at: www.researchpublish.com

Strengthening the Security of Information using Steganography

Gutta Sadhana

Abstract: **We propose a new method for strengthening the security of information through a combination of signal processing, cryptography and steganography. Cryptography provides the security by concealing the contents and steganography provides security by concealing existence of information being communicated. Signal processing adds additional security by compressing and transforming the information. The proposed method, viz. Steganography Based Information Protection Method (SBIPM), consists of scanning, coding, encryption, reshaping, cover processing and embedding steps. Scanning, coding, encryption steps make the information unintelligible so that one cannot extract plain message. Embedding make the message invisible so that one cannot detect it. Reshaping spreads the message so that embedded message can be detected from distorted steganos by authorized receivers. Cover processing makes detection of embedded message more difficult since the distortion is either due to noise addition or due to message embedding. Simulation and steganlysis results show the method provides high security and the information is safe from various attacks.**

I. INTRODUCTION

Now a days, various modes of communication like LAN, WAN and INTERNET are widely used for communicating information from one place to another around the globe. Such communication networks are open which any one can access easily. They are regularly monitored and an intercepted. In steganography, a message is embedded in a cover media in an invisible manner so that one could not suspect about its existence.

In this paper we present a substitution based information protection method where we combine cryptographic, steganography and signal processing concepts together for achieving security. The method is known as **Steganography Based Information Protection method.** In this method we substitute the information bit in randomly selected pixels at random places within LSB region.

STEGANOGRAPHY

The word steganography comes from the Greek *Steganos*, which mean covered or secret and *–graphy* mean writing or drawing. Therefore, steganography means, literally, covered writing. Steganography is the art and science of hiding information such that its presence cannot be detected and a communication is happening. A secret information is encoding in a manner such that the very existence of the information is concealed. Paired with existing communication methods, steganography can be used to carry out hidden exchanges.

The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. It is not to keep others from knowing the hidden information, but it is to keep others from thinking that the information even exists. If a steganography method causes someone to suspect the carrier medium, then the method has fail Until recently, information hiding techniques received very much less attention from the research community and from industry than cryptography. This situation is, however, changing rapidly and the first academic conference on this topic was organized in 1996. There has been a rapid growth of interest in steganography for two main reasons

(i) The publishing and broadcasting industries have become interested in techniques for hiding encrypted copyright marks and serial numbers in digital films, audio recordings, books and multimedia products.
(ii) Moves by various governments to restrict the availability of encryption services have motivated people to study methods by which private messages can be embedded in seemingly innocuous cover messages.

The basic model of steganography consists of *Carrier*, *Message* and *Password*. Carrier is also known as *cover-object*, which the message is embedded and serves to hide the presence of the message.

Basically, the model for steganography is shown on Figure 1. Message is the data that the sender wishes to remain it confidential. It can be plain text, cipher text, other image, or anything that can be embedded in a bit stream such as a copyright mark, a covert communication, or a serial number. Password is known as *stego-key*, which ensures that only recipient who knows the corresponding decoding key will be able to extract the message from a *cover-object.*

Recovering message from a *stego-object* requires the *cover-object* itself and a corresponding decoding key if a *stego-key* was used during the encoding process. The original image may or may not be required in most applications to extract the message.

There are several suitable carriers below to be the *cover-object*:

(i) Network Protocols such as TCP, IP and UDP

(ii) Audio that using digital audio formats such as wav, midi, avi, mpeg, mpi and voc

(iii) File and Disk that can hides and append files by using the slack space

(iv) Text such as null characters, just alike morse code including html and java

(v) Images file such as bmp, gif and jpg, where they can be both color and gray- scale.

In general, the information hiding process extracts redundant bits from *cover-object*. The process consists of two steps.

(i) Identification of redundant bits in a *cover-object*. Redundant bits are those bits that can be modified without corrupting the quality or destroying the integrity of the *cover-object*.
(ii) The embedding process then selects the subset of the redundant bits to be replaced with data from a secret message. The *stego-object* is created by replacing the selected redundant bits with message bits

STEGANOGRAPHY VS. CRYPTOGRAPHY

Basically, the purpose of cryptography and steganography is to provide secret communication. However, steganography is not the same as cryptography. Cryptography hides the contents of a secret message from a malicious people, whereas steganography even conceals the existence of the message. Steganography must not be confused with cryptography, where we transform the message so as to make it meaning obscure to a malicious people who intercept it. Therefore, the definition of breaking the system is different. In cryptography, the system is broken when the attacker can read the secret message. Breaking a steganographic system need the attacker to detect that steganography has been used and he is able to read the embedded message.

In cryptography, the structure of a message is scrambled to make it meaningless and unintelligible unless the decryption key is available. It makes no attempt to disguise or hide the encoded message. Basically, cryptography offers the ability of transmitting information between persons in a way that prevents a third party from reading it. Cryptography can also provide authentication for verifying the identity of someone or something.

In contrast, steganography does not alter the structure of the secret message, but hides it inside a *cover-image* so it cannot be seen. A message in ciphertext, for instance, might arouse suspicion on the part of the recipient while an "invisible" message created with steganographic methods will not. In other word, steganography prevents an unintended recipient from suspecting that the data exists. In addition, the security of classical steganography system relies on secrecy of the data encoding system. Once the encoding system is known, the steganography system is defeated.

It is possible to combine the techniques by encrypting message using cryptography and then hiding the encrypted message using steganography. The resulting *stego-image* can be transmitted without revealing that secret information is being exchanged. Furthermore, even if an attacker were to defeat the steganographic technique and detect the message from the *stego-object*, he would still require the cryptographic decoding key to decipher the encrypted message [1]. Table 1 shows that both technologies have counter advantages and disadvantages [19].

TABLE 1 - Advantages and disadvantages comparison

Steganography	Cryptography
• Unknown message passing	Known message passing
• Little known technology	Common technology
• Technology still being developed for certain formats	Most algorithms known to government departments
• Once detected message is known	Strong algorithms are currently resistant to brute force attack, large expensive computing power required for cracking technology.

STEGANOGRAPHY APPLICATIONS

There are many applications for digital steganography of image, including copyright protection, feature tagging, and secret communication. Copyright notice or watermark can embedded inside an image to identify it as intellectual property. If someone attempts to use this image without permission, we can prove by extracting the watermark.

In feature tagging, captions, annotations, time stamps, and other descriptive elements can be embedded inside an image. Copying the *stego–image* also copies of the embedded features and only parties who possess the decoding *stego-key* will be able to extract and view the features. On the other hand, secret communication does not advertise a covert communication by using steganography. Therefore, it can avoid scrutiny of the sender, message and recipient. This is effective only if the hidden communication is not detected by the others people.

II. STEGANOGRAPHIC TECHNIQUES

Over the past few years, numerous steganography techniques that embed hidden messages in multimedia objects have been proposed. There have been many techniques for hiding information or messages in images in such a manner that the alterations made to the image are perceptually indiscernible. Common approaches are include:

(i) Least significant bit insertion (LSB)
(ii) Masking and filtering
(iii) Transform techniques

Least significant bits (LSB) insertion is a simple approach to embedding information in image file. The simplest steganographic techniques embed the bits of the message directly into least significant bit plane of the *cover-image* in a

deterministic sequence. Modulating the least significant bit does not result in human- perceptible difference because the amplitude of the change is small.

Masking and filtering techniques, usually restricted to 24 bits and gray scale images, hide information by marking an image, in a manner similar to paper watermarks. The techniques performs analysis of the image, thus embed the information in significant areas so that the hidden message is more integral to the cover image than just hiding it in the noise level.

Transform techniques embed the message by modulating coefficients in a transform domain, such as the *Discrete Cosine Transform* (DCT) used in JPEG compression, *Discrete Fourier Transform*, or *Wavelet Transform*. These methods hide messages in significant areas of the *cover-image*, which make them more robust to attack. Transformations can be applied over the entire image, to block throughout the image, or other variants.

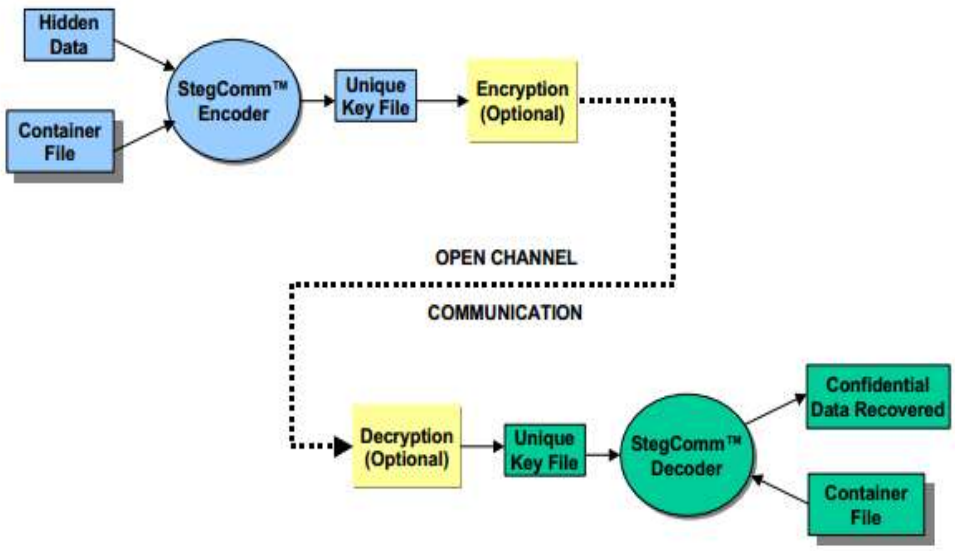
STEGANOGRAPHY TECHNIQUE

Steganography is the art and science of communicating in a way which hides the existence of the secret message communication. It aims to hide information /covered writing. Information to be protected is hidden in another data known as cover or carrier. Data containing hidden message are called as Steganos or Stegos. Steganos look like cover data and it is difficult to differentiate between them. Steganography based communication over easily accessible platforms to prevent leakage of information.

STEGANOGRAPHY METHODS

According to modification in covers, the methods can be categorized as:

- Substitution
- Transform domain
- Spread spectrum
- Statistical
- Distortion
- Cover generation



ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 1, pp: (27-35), Month: January-March 2014, Available at: www.researchpublish.com

Figure 1: This illustrates the operations of Steganography Communication **(StegComm)** through data flow diagram

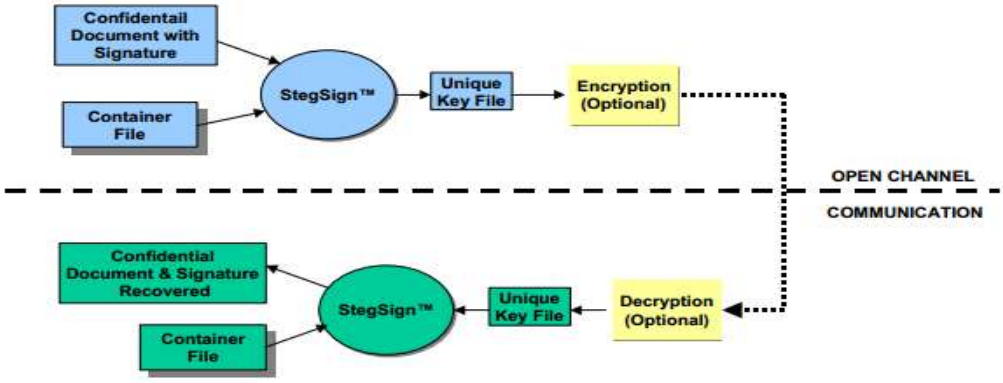


Figure 2: This illustrates the Steganography Signal **(StegSign)** through data flow diagram.

SUBSTITUTION METHOD

It is commonly used simple method in which we can put information bits in LSB sequentially at fixed place, randomly at fixed place or randomly at random places in cover pixels. The message to be protected passes through scanning, coding, encryption process to form an embedded message. In this method, there is a provision of increasing the robustness by spreading message bits randomly. This is done to detect the embedded message from distorted steganos

Many attacks on such steganographic systems are suggested. Some attacks that can be applied are given below:

1. Stego-Only Attack
2. Message-Stego Attack
3. Cover-Stego Attack
4. Message-Cover-Stego Attack

III. PROPOSED METHOD

The framework of proposed **Steganography Based Information Protection method** is shown in Fig 1. Its description is presented in the following steps**.**

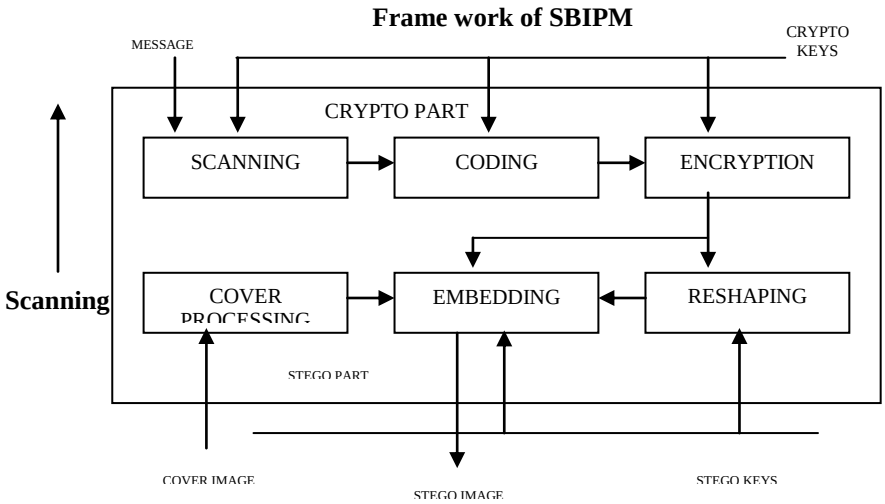


Figure 3: Frame work of SBIPM

The messages are mostly connected with the neighborhood elements, i.e. pixels in an image are varying smoothly and letter in the text are related to those on the right and the left. Scanning process minimizes these relations by suitably created random arrangement of message elements. We consider a randomization scheme in which a scan function, defined on different scan patterns, controls the randomization. A function defined for getting a scan path for randomizing the block is known as key for this process.

CODING

It contains some redundant space due to smooth variation in images and language characteristics in text. The distribution of message elements shows that it can be represented with lesser number of bits. In error free coding, the most frequent elements are represented by shorter codes and least frequent letters by longer codes. These codes change the statistical properties of the message. Huffman codes are error free and can be used for increasing the security. We use Huffman codes for text coding and Modified Huffman codes for binary images or Fax data. These codes are used for achieving additional security.

ENCRYPTION

This process conceals the message by transforming it into unintelligible form. Mostly, shift register based schemes are being used in present – day cryptography due to their simplicity and ease of hardware implementation. In shift register based schemes, the message bits are added under modulo two with binary random sequences. Linear feedback shift registers, feedback polynomials, state filter function and combining function are known as key parameters of this process.

RESHAPING

In applications, the method is required to be made robust so that embedded message can be deducted easily, even when stego images are slightly modified. In digital communications, information is transmitted bit-by-bit, i.e. as binary signaling. Larger the pulse size of the symbol higher is the probability of detection. Improvements of performance is due to the fact that for fewer symbols to hide we use more locations per symbol. Each symbol is represented by a pattern of binary bits.

COVER PROCESSING

Mostly LSB are highly variable in cover images and some minor changes in this region do not effect its quality and visual appearance. The highly variable region can be used for hiding secret information in invisible manner. Depth of hiding of cover image used for information hiding can be measured by an entropy measure. To make steganography secure against known cover image attack, it is necessary to make cover image suitable for information hiding so that it is not vulnerable to known cover – stego attack. The parameters used for generating random binary sequence and depth of hiding chosen ones are considered as key parameters.

EMBEDDING PROCESS

Process proposed is based on substitution method where message bits, after above processing steps, are embedded in cover image in randomly selected pixels at random places in LSB region within decided depth. Cover image to be used for embedding is processed first by modifying LSB of pixels. Embedding of information does not affect the quality and visual appearance of stego images. Embedding is based on the theory of shift registers.

This embedding method provides greater flexibility of hiding information and makes detection of embedded message more difficult. Even if we know that there exits an embedded message, its extraction is very difficult without knowing the key used. An attack who has no knowledge of key parameters cannot extract the embedded message.

Method of restoring clear message is reverse of the above steps, i.e., to detect, decrypt, decode and reconstruct the message. If reshaping is used then it is required to deshaped prior to decryption

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 1, pp: (27-35), Month: January-March 2014, Available at: www.researchpublish.com

IV. SIMULATION AND STEGANALYSIS RESULTS

We will consider text-in-image embedding to demonstrate the simulation results, but the method can be used for other messages like binary images too, which was already analysized and given in IETE Technical Review.

VISUAL PRECEPTION

For any steganography based secure system, the perception of steganos should be as cover image itself so that one cannot differentiate them and detect the existence of embedded message. From fig 3, the cover image, processed cover image and stego images look similar and one is not able to distinguish them visually.

DIFFERENCE ANALYSIS

The "difference-images "obtained by taking the difference between cover, processed cover and stego images are not visible. For making the difference visible in "difference-images "for visual interpretation, we first increase differences by multiplication of weight factor and then revert the values to get the strengthened "difference-images ".

The strengthened difference-images obtained are shown in fig 4. From analysis of these "difference-images ", on could not say that the changes are either due to cover processing or message embedding and hence we can say that the method is safe from known cover-stego attack.

DISTORTION ANALYSIS

Distortion analysis of stego images is carried out by studying distortion / similarity messages statistically. There are many methods for measuring distortion that can be used for distortion analysis. Distortion between two different images is measured by considering Mean Square Error (MSE), Mean Absolute Error (MAE) or Histogram Similarity (HS).

DEPTH VS DISTORTION ANALYSIS

Distortion occurred in different steganos is required by varying the depth of hiding for embedding information in cover image. The relation between depth of hiding used and distortion occurred in the stego images. That depth of hiding within some LSB region is most suitable for message embedding as the distortion is very small in this region. As the depth of hiding increases beyond preferable region, the distortion becomes noticeable and unsuitable for message hiding.

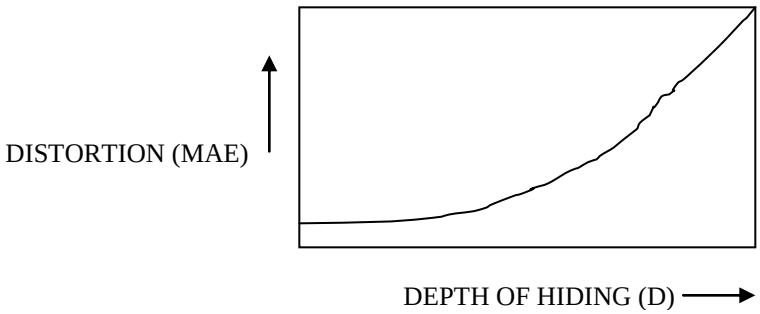


Figure 4: Depth Vs Distortion Analysis

SECURITY

A method, SBIPM, for providing the security of our important information has been proposed in this paper which is based on the techniques of signal processing, cryptography, and steganography. The security of information has been strengthened by applying scanning, coding, and encryption, cover processing and embedding techniques in the method. Reshaping step of the method provides robustness for detecting message correctly in such situation when stego image is

distorted. The method developed is safe from various attacks. Simulation and steganalysis results shown in this paper shows that one will not be able to distinguish between cover and stego images.

V. CONCLUSION

Thus we conclude that the strength of security achieved is very high and unauthorized receiver will not be able to get back the original message using exhaustive without the knowledge of key parameters.

Digital Steganography is interesting field and growing rapidly for information hiding in the area of information security. It has a vital role in defence as well as civil applications. In future we will have more of secure systems based on this technology.

REFERENCES

[1] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, "Multimedia data-embedding and watermarking technologies," *Proc. IEEE*, vol. 86, no. 6, pp. 1064–1087, Jun. 1998.

[2] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding—a survey," *Proc. IEEE*, vol. 87, no. 6, pp. 1062–1078, Jul. 1999.

[3] M. Barni and F. Bartolini, *Watermark Systems Engineering*. New York: Marcel Dekker, 2004.

[4] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*. San Francisco, CA: Morgan-Kaufmann, 2002.

[5] J. Eggers and B. Girod, *Informed Watermarking*. Boston, MA: Kluwer, 2002.

[6] N. F. Johnson, Z. Duric, and S. Jajodia, *Information Hiding. Steganography and Watermarking—Attacks and Countermea-sures*. Boston, MA: Kluwer, 2001.

[7] S. Katzenbeisser and F. A. Petitcolas, Eds., *Information Hiding Techniques for Steganography and Digital Watermarking*. Nor-wood, MA: Artech House, 2000.

[8] J. A. Bloom, I. J. Cox, T. Kalker, J.-P. M. G. Linnartz, M. L. Miller, and C. B. S. Traw, "Copy protection for digital video,"

[9] *Proc. IEEE (Special Issue on Identification and Protection of Mul-timedia Information)*, vol. 87, no. 7, pp. 1267–1276, Jul. 1999.

[10] C. Herley, "Why watermarking is nonsense," *IEEE Signal Process. Mag.*, vol. 19, no. 5, pp. 10–11, Sep. 2002.

[11] P. Moulin, "Comments on 'Why watermarking is nonsense'," *IEEE Signal Process. Mag.*, vol. 20, no. 6, pp. 57–59, Nov. 2003.

[12] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *IEEE Trans. Inf. Theory*, vol. 44, no. 5, pp. 1897–1905, 1998.

[13] F. Bartolini, A. Tefas, M. Barni, and I. Pitas, "Image authentica-tion techniques for surveillance applications," *Proc. IEEE*, vol. 89, no. 10, pp. 1403–1418, Oct. 2001.

[14] E. Martinian and G. W. Wornell, "Authentication with distortion constraints," in *Proc. IEEE Int. Conf. Image Processing* 2002, pp. II.17–II.20.

[15] D. Kundur and D. Hatzinakos, "Digital watermarking for telltale tamper proofing and authentication," *Proc. IEEE*, vol. 87, no. 7, pp. 1167–1180, Jul. 1999.

[16] J. Kelley, "Terror groups hide behind web encryption," *USA Today* Feb. 5, 2001 [Online]. Available: http://www.usatoday.com/life/ cyber/tech/2001-02-05-binladen.htm

[17] B. Chen and C.-E. W. Sundberg, "Digital audio broadcasting in the FM band by means of contiguous band insertion and precan-celling techniques," *IEEE Trans. Commun.*, vol. 48, no. 10, pp. 1634–1637, Oct. 2000.

[18] A. Baros, F. Franco, D. Delannay, and B. Macq, "Rate-distor-tion analysis of steganography for conveying stereovision disparity maps," *Proc. SPIE*, vol. 5306, pp. 268–273, Jan. 2004.

[19] Y. Steinberg and N. Merhav, "Identification in the presence of side information with application to watermarking," *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1410–1422, May 2001.

[20] M. Holliman, N. Memon, and M. Yeung, "On the need for image dependent keys in watermarking," presented at the 2nd Workshop Multimedia, Newark, NJ, 1999.

[21] G. Depovere and T. Kalker, "Secret key watermarking with changing keys," in *Proc. Int. Conf. Image Proc.* 2000, pp. I.10–I.13.