IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 14, Issue 3 (Sep. - Oct. 2013), PP 37-41
www.iosrjournals.org

New and Unconventional Techniques in Pictorial Steganography and Steganalysis

Vikas Kothari[1], Dinesh Goyal[2]
Software Engineering Department / Suresh Gyan Vihar University, India
Computer Science Engineering Department/ Suresh Gyan Vihar University, India

Abstract: *Steganography involves transferring data through a given channel in such a way that the communication channel itself is hidden from all involved parties. It is a form of security through obscurity; this technique protects both messages and stations involved in communication. In the most modern form of digital steganography, electronic communication may include complex steganographic lines of code inside transport layer which accomplishes the aforementioned task of protecting data and anonymity of participating stations. Steganography is much confused with the term cryptography former is fundamentally different in the sense that the message is sent secretly without attracting any attention of third party intruders by protecting anonymity of involved channels, nodes and stations.*
Keywords: *Steganography, Security and Protection, Cryptography, Data Hiding, Data Encryption*

I. INTRODUCTION

Steganography is the art of invisible communication. It refers to hiding the existence of the communication channel itself. The general idea of hiding messages in common digital contents, interests a wider class of applications that go beyond steganography. The techniques involved in such applications are collectively referred to as information hiding [1]. By using information hiding techniques, it is possible to fuse the digital content within the image signal regardless of the file format and the status of the image (digital or analog). In this thesis we will refer to cover work or equivalently to cover image, or simply cover to indicate the images that do not yet contain a secret message, while we will refer to stego Work, or stego images, or stego object to indicate an image with an embedded secret message. Moreover, we will refer to the secret message as stego-message or hidden message.

Depending on the meaning and goal of the embedded metadata, several information hiding fields can be defined, even though in literature the term 'information hiding' is often used as a synonym for steganography.

From an Information Theory perspective, we can introduce steganography by adopting a slightly different point of view [2]. In [3] Shannon was the first that con- sidered secrecy systems from the viewpoint of information theory. Shannon identified three types of secret communications which he described as

1. '*concealment systems, including such methods as concealed ink, hiding a payload in an irrelevant text, or in a fake covering cryptogram, or other methods in which the existence of the message is hidden from the intruder*',
2. *Privacy system*
3. *Cryptographic system*

Today steganography is also seen as a way of ensuring freedom of speech in military dictatorship countries or connected to homeland security. Steganography has also been supposed to be used by terrorists to design terroristic attacks. Example about the terrorism are the technical jihad manual [5] that is part of a terrorist manual and the color of the Osama Bin Laden's beard in its clips: military investigators think that secret messages are associated each color of the beard to coordinate terrorist cells.

Another topical target of steganography is computer warfare. New worms and spywares stole a lot of information about users and then they have to find a way to carry out this data by preventing any suspicion of transmission existence by antivirus, firewall or data stream analysis. During the last few years image steganography research has raised an increasingly interest. A variety of techniques have been proposed especially for a given image file format like gif, jpeg or images represented in the pixel domain. In fact, the main idea behind steganography undetectability is: less embedding changes to the cover Work means a less detectable stego object. Even though this statement is not completely true (as it shown in [8]), it represents a good starting point to develop and to improve initial steganographic techniques proposed in the literature.

II. RELATED WORK

Yu-Chen Shu, Wen-Liang Hwang presented Conventional secret message passing methods embed a message in the cover-text, so the receiver must use stego-text to extract the message content. In contrast, this paper proposes a new paradigm in which the receiver does not necessarily require stego-text to retrieve the message content. Under the proposed approach, the sender can produce keys without modifying the cover-image, and the intended recipient can use the keys and an image that resembles like the cover-image to recover the message.

The feature has the potential to generate many new secret message passing applications that would probably be impossible under the current widely used paradigm. The performance criteria of the new paradigm are presented. We propose a subspace approach to implement the paradigm, demonstrate that the criteria can be satisfied, and consider some interesting.

Supriya Rai and Ruchi Dubey presented Steganography is one of the most powerful tools for information hiding. In this paper, we have modified least significant bit (LSB) substitution method for data hiding.

Conventional LSB technique uses the least significant bit of consecutive pixels for embedding the message which draws suspicion to transmission of a hidden message. If the suspicion is raised, then the goal of steganography is defeated. Still LSB technique is the most widely used as it is simple. In our implementation pixels to be substituted with information are selected randomly which makes it superior to the conventional approach. The robustness of the algorithm is further increased by using keyless steganography. This paper proposes a novel technique to hide information in a 24 bpp RGB image using modified LSB substitution method.

Amitava Nag , Saswati Ghosh presented Image steganography is a method of concealing information into a cover image to hide it. Least Significant-Bit (LSB) based approach is most popular steganographic techniques in spatial domain due to its simplicity and hiding capacity. This paper presents a novel technique for Image steganography based on LSB using X-box mapping where we have used several Xboxes having unique data. The embedding part is done by this Steganography algorithm where we use four unique X-boxes with sixteen different values (represented by 4- bits) and each value is mapped to the four LSBs of the cover image. This mapping provides sufficient security to the payload because without knowing the mapping rules no one can extract the secret data (payload).

S.Premkumar, A.E.Narayanan presented Core banking is a set of services provided by a group of networked bank branches. Bank customers may access their funds and perform other simple transactions from any of the member branch offices. The major issue in core banking is the authenticity of the customer. Due to unavoidable hacking of the databases on the internet, it is always quite difficult to trust the information on the internet. To solve this problem of authentication, we are proposing an algorithm based on image processing, improved steganography and visual cryptography. This paper proposes a technique of encode the password of a customer by improved Steganography, most of the steganographic techniques use either three or four adjacent pixels around a target pixel whereas the proposed technique is able to utilize at most all eight adjacent neighbours so that imperceptibility value grows bigger and then dividing it into shares. Total number of shares to be created is depending on the scheme chosen by the bank. When two shares are created, one is stored in the Bank database and the other is kept by the customer. The customer has to present the share during all of his transactions. This share is stacked with the first share to get the original image. Then decoding method is used to take the hidden password on acceptance or rejection of the output and authenticate the customer.

Zawawi, M.N., Mahmod, R., Udzir, N., Ahmad, F. and, Desa, J.M presented The word Steganography originated from a greek language which directly translated as covered writing. The idea of covered writing in steganography here is a practice of hiding or covering the real information with a disguise of a day to day widely accepted object. Traditionally in ancient times steganography is practiced by means such as, covering a roll of scriptures inside a fruit or food item, inserting symbols on body tattoos, hidden objects in paintings and even in clothing such as shoes. The main idea of steganography is to hide information within the physical aspect of any everyday object where the hidden information existence is less likely to be there. In the digital age, these objects are replaced by digital files. Since all media are available in this form, steganography techniques usually exploit it by hiding on the bit stream, headers and even on its compression scheme. The use of this method, however, is not without its enemy; on the other axis of steganography, there exists steganalysis which aims to detect steganography behavior and perhaps extract the information hidden within.

III. METHODOLOGY

The contribution of this thesis is threefold. As a first contribution we introduce a comparative methodology for the comparison of different steganalyzers. The second contribution of the thesis regards steganography, since we introduce a new embedding domain and a corresponding method, called MPSteg-color, which outperforms, in terms of undetectability, classical embedding methods. Next, we briefly describe each contribution.

Comparative methodology in steganography

As a second contribution we discuss a variety of issues associated with comparison of different steganalyzers and highlight some of these issues with a case study comparing four steganalysis algorithms designed to detect embedding. In particular, we discuss issues related to the creation of the training and testing sets. We emphasize that for steganalysis, it is very unlikely that the assumptions used to cre- ate the training set will match conditions used during deployment. Consequently, it is imperative that testing also investigates how performance degrades as the test set deviates from

the training data. The subsequent empirical evaluation of four algorithms on four different test sets revealed that algorithm performance is highly variable, and strongly dependent on the training and test imagery. Experimental results clearly demonstrate that the performance is strongly image-dependent, and that further work is needed to establish more comprehensive databases. It is also common to assume that the embedding rate is known during testing and training, but this is unlikely to be the case in practice. Once again, significant performance degradation is observed. Experimental results also suggest that the common practice of training at a low embedding rate in order to deal with a wide range of embedding rates during testing is not as effective as training with a mixture of embedding rates.

MPSteg-color

The third contribution regards steganography for color images. Specifically, we propose a new steganographic method that tries to use the fail-safe of steganalyzers to improve the undetectability of the stego-message. In fact, although steganalyzers do not know the hidden message, they rely on a statistical analysis to understand whether a given signal contains concealed data or not. However this analysis disrespect the semantic content of the cover signal. We argue that, from a steganographic point of view it is preferable to embed the secret message at higher semantic levels of the image, e.g. by modifying structural elements of the cover image like lines, edges or flatareas.

By the above consideration, we propose a new steganographic technique, called MPSteg-color, that hides the stego-message into some selected coefficients obtained through a high redundant basis decomposition of the color image. The decomposition is efficiently obtained by using a Matching Pursuit (MP) algorithm. In this way the hidden message is embedded at a higher semantic level and hence it is more difficult for a steganalyzer to detect it.

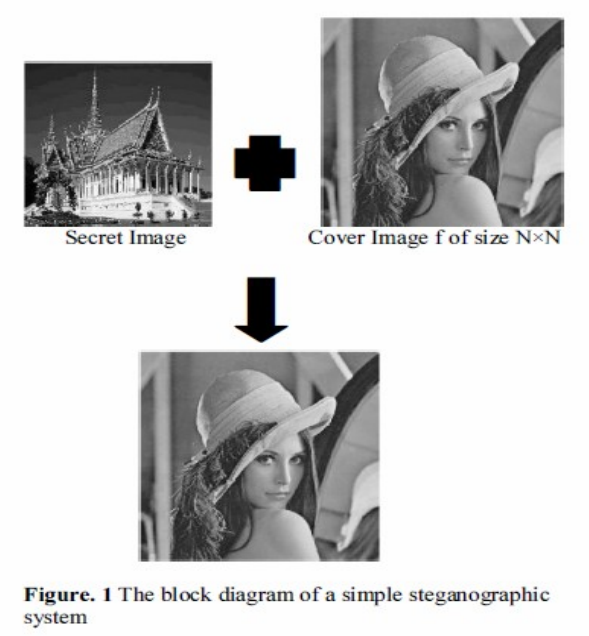


Figure. 1 The block diagram of a simple steganographic system

IV. INDENTATIONS AND EQUATIONS

The steganalysis problem is a binary classification problem is or isn't the test instance (image) a stego image? As such, there are four possible outcomes. These are:

1. True positives, i.e. test instances that are correctly labeled as stego Works;
2. True negatives, i.e. test instances that are correctly labeled as non-stego Works;
3. False negatives, i.e. test instances that are incorrectly labeled as non-stego Works;
4. False positives, i.e. test instances that are incorrectly labeled as stego Works.

If P and N denote the real number of positive and negative instances, and TP and FP denote the predicted number of true positives and false positives, respectively, then the true positive rate, t_p is defined as

$t_p = TPP$,

and the false positive rate, f_p as:

$f_p = FN \,.\, P$

Common performance metrics which can be derived from these include precision, recall, accuracy and F-measure:

Precision = TP/TP+FP

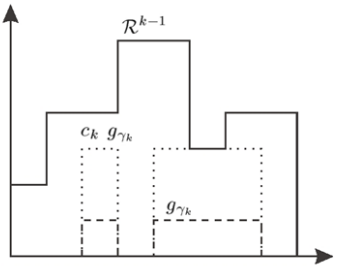
Recall = TP/P,

Accuracy = TP+TN

F-measure = 2/(1/precision)+(1/recall)

V. FIGURES AND TABLES

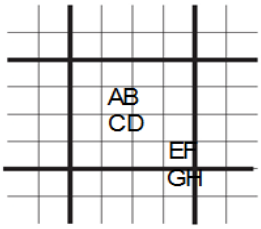
In order to avoid that quantization errors prevent the correct decoding of the hidden message, let us observe that the stego-messages will be embedded in the MP domain by modifying the coefficients c_k in equation (7.3), however, after embedding, the modified image must be brought back into the pixel domain. If we want to avoid the introduction of quantization errors it is necessary that the reconstructed image belongs to the *Image class*.



The Selection Rule

Targeted steganalyzers

The first targeted steganalyzer we used is built on the simple blocking artifacts detector (BD) described in [64]. This technique was originally developed for detect- ing JPEG block artifacts, however, we adapted it to detect the artifacts introduced by MPSteg-color and use them as a feature to detect the presence of a stego-message. The algorithm is very simple: we split the image into blocks whose size should be matched to that used by the MP algorithm. Regardless of the block partition strategy the steganalyzer assumes that blocks are located on a grid aligned with the top-left .



For each block the numbers $Z = |A + D - B - C|$ and $Z = |E + H - F - G|$ are computed.

$$Z = |A + D - B - C|$$

$$Z = |E + H - F - G|$$

where A, B, C, D, E, F, G and H are taken as shown in Figure 11.1 in the case of 4×4 blocks, the extension to larger blocks being trivial. Next the normalized histograms vectors $h(n)$ and $h(n)$ are computed respectively for Z and Z and the following feature is calculated:

$$255\, f_{BD} = \sum_{n=0} |h(n) - h(n)|.$$

The above procedure is repeated for the three color bands producing a three-dimensional feature vector that is given as input to the FLD classifier. The second steganalyzer we developed relies on the knowledge of the histogram of MP coefficients. For this to be possible, we assume that the steganalyzer knows the MP dictionary but it does not know the reference band that is used to calculate the decomposition path (hence a random band is used as a reference by the steganalyzer).

Due to the embedding asymmetry applied to coefficients having value equal to 1 - that are either left unchanged or incremented by one - a flat step appears in the leftmost part of the histogram, while this effect does not appear in the cover image.

By considering this effect, we propose to use the following feature:

$$f_{MP\,HA} = |h(2) - h(1) + h(3)|$$

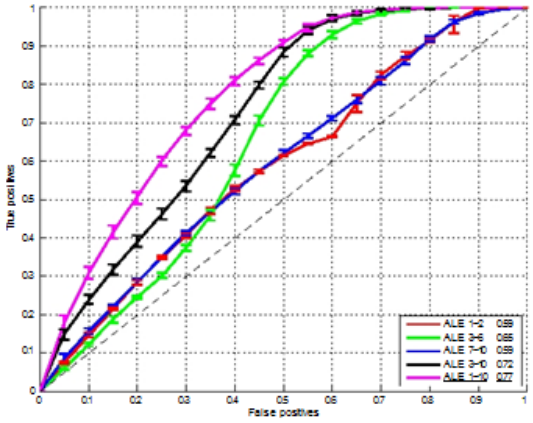
where h is the histogram function. In the sequel we will refer to this technique as MPHA.

VI. Result & Conclusion

Since similar results were observed for various embedding rates, we only report classification results for $\rho = 0.5$.

Given figure shows the improvements in classification resulting from elimination of border effects. The original algorithm of Zhang *et al.* is compared with a system based on feature 1 of Table 4.1 (ALE 1), and features 1 and 2 (ALE 1-2). The error bars on each plot indicate the minimum and maximum values observed during the 20 cross-validation runs. First of all, we note the unexpectedly poor performances of all three algorithms, i.e. the ROC curves are very close to the diagonal. This is due to the wide variety of images present in of composite database.

Despite the poor performance of all three algorithms, the two algorithms based on new ALE features (ALE 1 and ALE 1-2) exhibit a slight improvement in clas- sification performances. The system using the first two ALE features (ALE 1-2) achieves the highest performances based on area under the ROC curve (AUC), with a score of 0.59.



Analysis of the impact of ALE features selection on classification results.

REFERENCES

[1] M. Kharrazi, H. Sencar, and N. Memon, "Image Steganography: Concepts and Practice," *Lecture Note Series, Institute for Mathematical Sciences, National University of Singapore*, 2004.
[2] I. Cox, T. Kalker, G. Pakura, and M. Scheel, "Information transmission and steganography," *Lecture Notes in Computer Science*, vol. 3710, p. 15, 2005.
[3] C. Shannon, "Communication Theory of Secrecy Systems," *Bell System technical Journal*, vol. 28, pp. 656-715, 1954.
[4] G. J. Simmons, "The prisoners' problem and the subliminal channel," in *Advances in Cryptology: Proceedings of CRYPTO'83*. Plenum Pub Corp, 1984, pp. 51-67.
[5] R. Givner-Forbes, "Steganography: Information Technology in the Service of Jihad," *The international Centre for Political Violence and Terrorism Research*, March 2007. [Online]. Available: www.pvtr.org
[6] R. Anderson, "Stretching the limits of steganography," *Lecture Notes in Computer Science*, vol. 1174, pp. 39-48, 1996.
[7] Wikipedia The Free Encyclopedia. [Online]. Available: http://en.wikipedia.org/wiki/Printer_steganography
[8] G. Cancelli and M. Barni, "MPSteg-color: A new steganographic technique for color images," *Information Hiding: 9th International Workshop, Ih 2007, Saint Malo, France, June 11-13*, vol. 4567, pp. 1-15, 2007.
[9] A. Westfeld, "F5-a steganographic algorithm: High capacity despite better steganalysis," in *Information Hiding: 4th International Workshop, IH 2001, Pittsburgh, PA, USA, April 25-27, 2001: Proceedings*. Springer, 2001, p. 289.
[10] M. Goljan, J. Fridrich, and T. Holotyak, "New blind steganalysis and its implications," *Proceedings of SPIE*, vol. 6072, pp. 1-13, 2006.
[11] J. Fridrich, M. Goljan, P. Lisonek, and D. Soukal, "Writing on wet paper," *IEEE Transactions on Signal Processing*, vol. 53, no. 10 Part 2, pp. 3923-3935, 2005.
[12] J. Fridrich, M. Goljan, and D. Hogea, "Attacking the outguess," in *Proc. of the ACM Workshop on Multimedia and Security*, 2002.
[13] P. Sallee, "Model-based methods for steganography and steganalysis," *International Journal of Image and Graphics*, vol. 5, no. 1, pp. 167-189, 2005.
[14] J. Fridrich, T. Pevn` and J. Kodovsk` "Statistically undetectable jpeg steganography: y, y, dead ends challenges, and opportunities," in *Proceedings of the 9th workshop on Mul- timedia & security*. ACM New York, NY, USA, 2007, pp. 3-14.