International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS)
ISSN (Online) 2349-6967 *Volume 2 , Issue 1(Jan-Feb 2015), PP1-5*

Information Hiding in Digital Images Using Image as a Key with together Steganography and Cryptography

Sangamesh Gama
Dept of Computer Science and Engg. B.K.I.T Bhalki

Abstract: In this paper, we present a new steganographic paradigm for digital images in grayscale formats. Mainly it concentrates on two methods i.e. Message hiding using LSB embedding and stochastic modulation. In LSB Embedding we concentrate on Least significant bit modulation in which we apply cryptography into the message image and then the cover image's LSB has been modulated with the message bits and hence achieving the steganography. In the Stochastic Modulation message bits are embedded in the cover image by adding a weak noise signal with a specified but arbitrary probabilistic distribution. This embedding mechanism provides the user with the flexibility to mask the embedding distortion as noise generated by a particular image acquisition device. This type of embedding will lead to more secure schemes because now the attacker must distinguish statistical anomalies that might be created by the embedding process from those introduced during the image acquisition itself. Unlike previously proposed schemes, this new approach, that we call stochastic modulation, achieves oblivious data transfer without using noise extraction algorithms or error correction. This leads to higher capacity (up to 0.8 bits per pixel) and a convenient and simple implementation with low embedding and extraction complexity. But most importantly, because the embedding noise can have arbitrary properties that approximate a given device noise, the new method offers better security than existing methods. The security of data hiding by adding noise to the cover image depending on the key value has been addressed in this project. From this the attacks do not work well for images and may produce a significant rate of false positives thus misguiding the stego analyst and ensure the highest level of security.

I. INTRODUCTION

1.1. Steganography

Steganography is the art of hiding information in ways that prevent the detection of hidden messages. The word Steganography comes from the Greek words *s*teganos (secret) and graphy (writing). It includes a vast array of secret communications methods that conceal the existence of message. These methods include invisible inks, microdots, character arrangement, digital signatures, covert channels, and spread spectrum communications.

Steganography and cryptography are cousins in the spy craft family. Cryptography scrambles a message so it cannot be understood. Steganography hides the message so it cannot be seen. A message in cipher text, for instance, might arouse suspicion on the part of the recipient while an "invisible" message created with steganographic methods will not. Steganography by itself does not ensure secrecy, but neither does simple encryption. If these methods are combined, however, stronger encryption methods result. If a message is encrypted and then embedded in an image, video, or voice, it becomes even more secure. If an encrypted message is intercepted, the interceptor knows the text is an encrypted message. But with steganography, the interceptor may not know that a hidden message even exists. To make a steganographic communication even more secure the message can be compressed and encrypted before being hidden in the carrier. Cryptography and steganography can be used together. If compressed the message will take up far less space in the carrier and will minimize the information to be sent. The random looking message which would result from encryption and compression would also be easier to hide than a message with a high degree of regularity. Therefore encryption and compression are recommended in conjunction with steganography.

1.2 Block Diagram

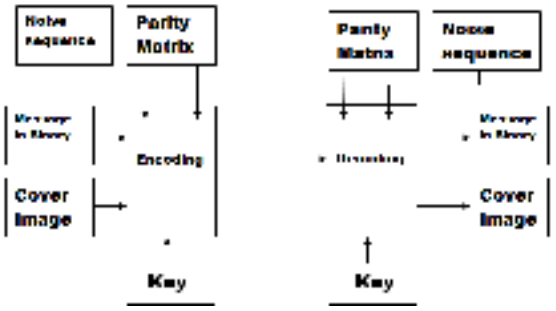


Figure1.1: The Stochastic Modulation Technique

The block diagram gives an overview of the stochastic modulation technique. As indicated, the message file is converted into a string of 1's and 1's. A key is used to generate the normally distributed Gaussian noise sequence, here image is used as a key for encryption process. The parity matrix is also generated and finally, using the parity matrix and the noise sequence, the message is embedded into the cover image.At the receiver, the same key is required to generate the same noise sequence and the parity matrix. Once these are ready, the message is readily extracted from the stego image. The extracted message string may then be reorganized to form the original message file. As seen, the key forms the heart of the security for the whole system in the absence of the key, any attacker will not be able to recover the message. Also, since the noise added resembles the noise generated by the image capturing devices, it cannot be detected by statistical methods.

1.3 File compression

Two kinds of compression are lossless and lossy. Both methods save storage space but have different results, interfering with the hidden information, when the information is uncompressed. Lossless compression lets us reconstruct the original message exactly; therefore, it is preferred when the original information must remain intact (as with steganographic images). Lossless compression is typical of images saved as GIF (Graphic Interchange Format) and 8bit BMP (a Microsoft Windows and OS/2 bitmap file). Lossy compression, on the other hand, saves space but may not maintain the original image's integrity. This method typifies images saved as JPEG (Joint Photographic Experts Group). Due to the lossy compression algorithm, which we discuss later, the JPEG formats provide close approximations to high quality digital photographs but not an exact duplicate. hence the term "lossy" compression.Hence in this chapter we summarized the purpose of steganography and some general concepts of steganography, in the next chapter we study the specific requirement and techniques for LSB and stochastic embedding modulation.

II. GAUSSIAN NOISE IN STEGANOGRAPHY

In the figure 2.1, we give the general definitions to some of the terms that we shall often use in the forthcoming discussion of stochastic modulation.

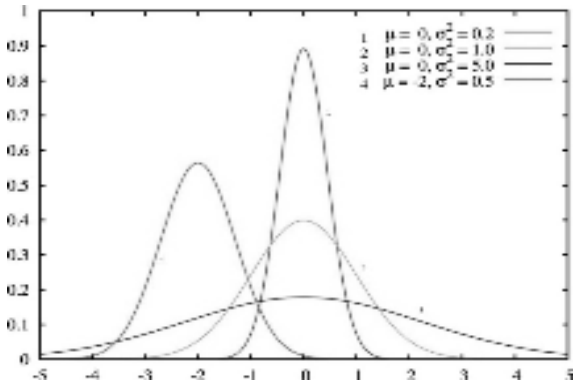


Figure 2.1: Normal distribution curve

2.1. Gaussian noise: Gaussian noise is also called as white noise. It is one of the most common noises that occurs in a communication system. The Gaussian noise is a spread spectrum noise and tends to affect all the frequency components of the communication channel equally. In our discussion, we assume that the image capturing devices generate this type of noise and our modulation technique shall be based on this principle.

2.2. Normal distribution: This is a kind of probability distribution function. The distribution is characterized by two parameters namely the mean and variance. The Characteristic probability distribution curve for the normal distribution is a bell shaped curve as shown in the figure Fig 2.1.

2.3.Noise sequence: The noise sequence is a sequence of random numbers which can take positive and negative values. The noise sequence will follow a normal distribution.

2.4.Parity function: The parity function will be used to generate a parity matrix. The parity matrix is a matrix containing values 1 and 0. It is used both during the embedding and the retrieving of the message, and acts as the heart of the stochastic modulation system.

2.5.Capacity: Capacity refers to the maximum length message that can be embedded into a given cover image. It is measured in terms of bits per pixel (bpp). The capacity is determined by the variance of the noise sequence.The Least Significant Bit embedding (LSB) with sequential or random message spread has been successfully attacked even for very short messages. In essence, the LSB embedding is so easily detectable because it introduces distortion that never naturally occurs to images and creates an imbalance between appropriately defined statistical quantities. A better approach is to replace the operation of flipping the LSBs by randomly adding 1 or –1 to pixels (+–1 embedding) and extracting the message bits from LSBs as in the classical LSB embedding. This is the embedding algorithm of Hide and it has also been accepted (in a slightly different version) for steganography in the JPEG format. It turns out that this simple modification of the LSB embedding paradigm is, in fact, much more difficult to detect.The +1,–1 embedding is a special case of our stochastic modulation when the noise η added to the cover image has the following probability distribution P: $P(\eta = -1) = p/2$, $P(\eta = 1) = p/2$, $P(\eta = 0) = 1-p$ (assuming the message is a random bit stream and $100p$ % of pixels were used for embedding). Notice that in +–1 embedding, the message bits are still encoded and extracted as LSBs of pixels. In this paper, we show how to extend this embedding archetype to a noise with an arbitrary probabilistic distribution P defined on n arbitrary set of integers. The algorithm that achieves this is called stochastic modulation.The embedding party (Alice) can use stochastic modulation, for example, in the following way. Alice will carry out experiments on her source of cover images and estimate the properties of the noise present in them. If Alice's acquisition device is a digital camera, the noise depends on the exposition time, the amount and type of ambient light at the scene, usage of a flash, the specific CCD sensor and camera circuitry, interpolation algorithms in camera's hardware, etc. The sensor and hardware noise are known to be well modeled by a Gaussian noise. Because there is in general a great

variation in the amount of noise in the images due to the multitude of contributing effects mentioned above, one could slightly increase the amount of noise without introducing any easily detectable statistical artifacts. This idea is at the base of our stochastic modulation.We make use of the following property of random signals for our purpose. If $\{s_i\}$ is a normally distributed Gaussian sequence $N(0, \sigma)$ and if z_i is a random variable uniformly distributed in $\{-1, 1\}$, then $\{z_i s_i\}$ is also $N(0, \sigma)$. In other words, a Gaussian sequence with randomized signs stays Gaussian. This statement is true for any random variable with a distribution symmetrical about zero.

Suppose the message m_i consists of a random sequence of 1's and –1's (m_i has zero mean). Consider a naïve steganographic scheme in which we add the signal $\{m_i s_i\}$ to the image. Unfortunately, in order to recover the message, the original image or at least its approximation (e.g., using low pass filtering) is necessary. Errors in estimating the original image necessitate employment of error correction schemes, which in turn may dramatically decrease the steganographic capacity. Below, we show a simple idea how a class of parameterized parity functions can be used to make this scheme oblivious.

We define a parity function P on pixel values, $P(x, s)$ $\{-1,1\}$, for x belongs to$\{0, \ldots, 255\}$ and $s > 0$, where s is an integer parameter, and $P(x, s) = 0$ for $s = 0$. This function applied to the stego image pixel values will produce message bits. The parity function is required to satisfy the following "ant symmetric" property for all x

$$P(x+s, s) = -P(x-s, s) \text{ for } s \neq 0.$$

For example, for $s = 1$, we can define $P(x, 1)$, $x = 0, 1, 2, \ldots$ as $P(x, 1) = 1, 1, -1, -1, 1, 1, -1, -1, \ldots$.In general, for $s > 0$, the first segment of $2s$ parities can be arbitrary, but every next segment of $2s$ values must be the negative copy of the previous segment. Thus, it is enough to define P on the set $[1, 2s]$. A good choice for the parity function is $P(x, s) = (-1)^{x+s}$, x belongs to $[1, 2s]$.

This parity function ensures that P changes its sign as often as possible. We will find this property useful when $x+s$ or $x-s$ should get outside of their dynamic range during embedding. Notice that besides the pixel value x, the parity function depends on the second parameter s. This is important because otherwise we could not find a function $P(x)$ satisfying $P(x+s) = -P(x-s)$ for all pixel values x and all positive integers s.

Code for to Use the Image as a Key

Generate a Gaussian distributed noise sequence of twice the length of the message

```
var = 1;
myki = input('Enter the path of key image: ');
key = imread(myki);
figure
imshow(key);
title('Original key file');
key1=sum(key);
key1=sum(key1');
key1=sum(key1);
key2=uint64(key1/10000);
key2=double(key2);
randn('seed',key2);
```

```
S = round(random('norm',0,var,1,sz));
length = size(find(S));
if L > length
   disp('Error!! Message too big... try with a bigger cover image');
   break
```

III. RESULTS

Examples for Steganography using stochastic Embedding

Here we present some of the example images which were tested on the codes written using the algorithms given in the upcoming chapter.

Example 1

Figure3.1: Cover image.bmp (300x200)

Cover image selected to test stochastic modulation

Figure3.2: Message image. jpg(69x66)

Secret image selected to test stochastic modulation

Figure3.3:image used as key for encryption

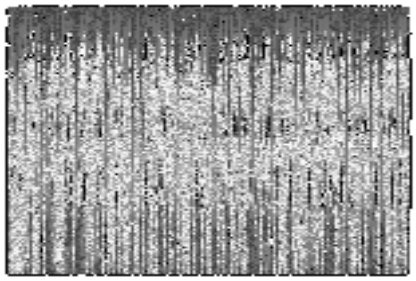
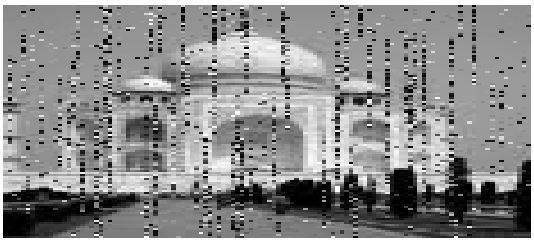


Figure 3.4: encrypted image.jpg

Encrypted image in stochastic modulation

Stego image generated using stochastic modulation of message image.jpg into cover image.jpg



Extracted message file from the stego image.

IV. CONCLUSION

This chapter summarizes the conclusions derived through the study under taken and the results presented in the project thesis.In this project titled "Information Hiding in Digital Images using Stochastic modulation", we have presented two techniques of steganography (i.e. Message hiding) using LSB embedding and stochastic modulation. Although we covered a number of security and capacity definitions, there has been no work successfully formulating the relationship between the two from the practical point of view. We also reviewed a number of embedding algorithms starting with the earliest algorithm proposed which was the LSB technique. At some point LSB seemed to be unbreakable but as natural images were better understood and newer models were created LSB gave way to new and more powerful algorithms which try to minimize changes to image statistics. But with further improvement in understanding of the statistical regularities and redundancies of natural images, most of these algorithms have also been successfully steganalysed.

Compared to LSB methods stochastic modulation can embed bigger payloads without using error correction schemes or de-noising algorithms at the receiving end, which makes the algorithm significantly simpler and faster. Because the noise distribution can be arbitrarily adjusted, this method provides much greater flexibility than LSB Embedding methods.The security of data hiding by adding noise to the cover image depending on

the key value has been addressed in this project. From this the attacks do not work well for images and may produce a significant rate of false positives thus misguiding the stego analyst and ensure the highest level of security.

The project's concept can also be implied in developing the new algorithms for the various colour images with different formats which will lead to new innovations in the field of image steganography.

V. REFERENCES

1. Jessica Fridrich and Miroslav Goljan "*Digital image steganography using stochastic modulation***"** Department of Electrical and Computer Engineering, SUNY Binghamton, Binghamton, NY13902-6000, USA

2. F. Alturki and R. Mersereau, "*A Novel Approach for Increasing Security and Data Embedding Capacity in Images for Data Hiding Applications*". *Proc. of ITCC*, Las Vegas, Nevada, 2001, pp. 228–233.

3. S. Dumitrescu, Wu Xiaolin, and Z. Wang, "*Detection of LSB Steganography via Sample Pair Analysis*". Preproceedings 5th Information Hiding Workshop, Noordwijkerhout, Netherlands, Oct. 7−9, 2002.

4. J. Fridrich, M. Goljan, and R. Du, "*Detecting LSB Steganography in Color and Gray-Scale Images*", Magazine of IEEE Multimedia, Special Issue on Security, October-November issue, 2001, pp. 22–28.

5. J.J. Harmsen and W. A. Pearlman, "*Steganalysis of Additive Noise Modelable Information Hiding*", *Proc. SPIE Electronic Imaging*, Santa Clara, January 21–24, 2003.

6. G.E. Healey and R. Kondepudy, "*Radiometric CCD Camera Calibration and Noise Estimation". IEEE Trans. on Pattern Analysis and Machine Intelligence*, Vol. **16**(3), March 1994, pp. 267–276.

7. M. Holliman, N. Memon, and M. M. Yeung, "*On the Need for Image Dependent Keys for Watermarking*", *Proc. Content Security and Data Hiding in Digital Media*, Newark, NJ, May 14, 1999.

8. L.M. Marvel, C.G. Boncelet, and C.T. "*Retter, Reliable Blind Information Hiding for Images"*. In: D. Aucsmith (eds.):*Information Hiding: 2nd International Workshop*, LNCS, Vol. 1525. Springer-Verlag, New York, 1998, pp. 48–61.

9. T. Sharp, "*An Implementation of Key-Based Digital Signal Steganography*", In: I. S. Moskowitz (eds.): *4th International Workshop on Information Hiding*, LNCS 2137, Springer-Verlag, New York, 2001, pp. 13–26.

10. A. Westfeld and A. Pfitzmann, "*Attacks on Steganographic Systems*". In: A. Pfitzmann (eds.): *3rd International Workshop on Information Hiding*. LNCS, Vol.1768. Springer-Verlag, New York, 2000, pp. 61−75.

11. A. Westfeld, "*High Capacity Despite Better Steganalysis (F5–A Steganographic Algorithm)*". In: Moskowitz, I.S. (eds.): *4th International Workshop on Information Hiding*, LNCS, Vol. 2137. Springer-Verlag, New York, 2001, pp. 289–302.

12. A. Westfeld, "*Detecting Low Embedding rates*". In: Petitcolas et al. (eds.): *Preproceedings 5th Information Hiding Workshop*. Noordwijkerhout, Netherlands, Oct. 7−9, 2002.