International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue-6, September 2015
ISSN: 2395-3470
www.ijseas.com

STEGANO-CRYPTO USING CHOAS BASED Sblock EMBEDDING TECHNIQUE

Shilpa Sangwan
Department of Computer Science & Engineering
Panchkula Engineering College, Mouli, Haryana

Amit Jain
Department of Computer Science & Engineering
Panchkula Engineering College, Mouli, Haryana

Abstract

Steganography is defined as the science of hiding or embedding "data" in a transmission medium. Its ultimate objectives, which are undetectability, robustness and capacity of the hidden data, are the main factors that distinguish it from Cryptography. Digital Image Cryptosystem with Adaptive Steganography has been presented. In order to further strengthen the encryption of the transformed image, a steganography approach for data hiding is also proposed. Experimental results have shown that the correlation and entropy values of the encrypted text before the insertion are similar to the values of correlation and entropy after the insertion. Since the correlation and entropy of chaotic have not changed while hiding necessary information, the method offers a good concealment of the data in the encrypted text, thus reduces the chance of the encrypted text being detected.

Two algorithms have been presented which can preserve the first order statistics of an image after embedding. The second approach aims at resisting Blind Steganalytic Attacks especially the Calibration based Blind Attacks which try to estimate a model of the cover image from the stego image. A generic framework for JPEG steganography has been proposed which disturbs the cover image model estimation of the blind attacks

Comparison results show that the proposed algorithm can successfully resist the calibration based blind attacks and some non-calibration based attacks as well.

1.) INTRODUCTION

Everyday tons of data are transferred through the Internet through e-mail, file sharing sites, social networking sites etc. to name a few. Steganography is an antique technology that has submissions even in today¨s modern culture. Steganography is the art of concealing information in ways that prevent the detection of hidden messages. Steganography include an array of secret message methods that hide the message from being seen or exposed. The

concept of steganography is to avoid illustration thought to the being of a hidden message. This method of information hiding has recently become significant in a number of ways. Digital audio, video, and pictures are increasingly equipped with unique but invisible marks, which may contain a hiding obvious notice or serial number or even help to prevent unauthorized replication straight. Any steganographic system can be studied as shown in Figure 1.1. For a steganographic algorithm having a stego-key, given any cover image the embedding process generates a stego image. The extraction process takes the stego image and using the shared key applies the inverse algorithm to extract the hidden message Wendy has no knowledge about the secret key that Alice and Bob share, although she is aware of the algorithm that they could be employing for embedding messages. In public key steganography, Alice and Bob have private-public key pairs and know each other's public key. In this thesis we confine ourselves to private key steganography only.

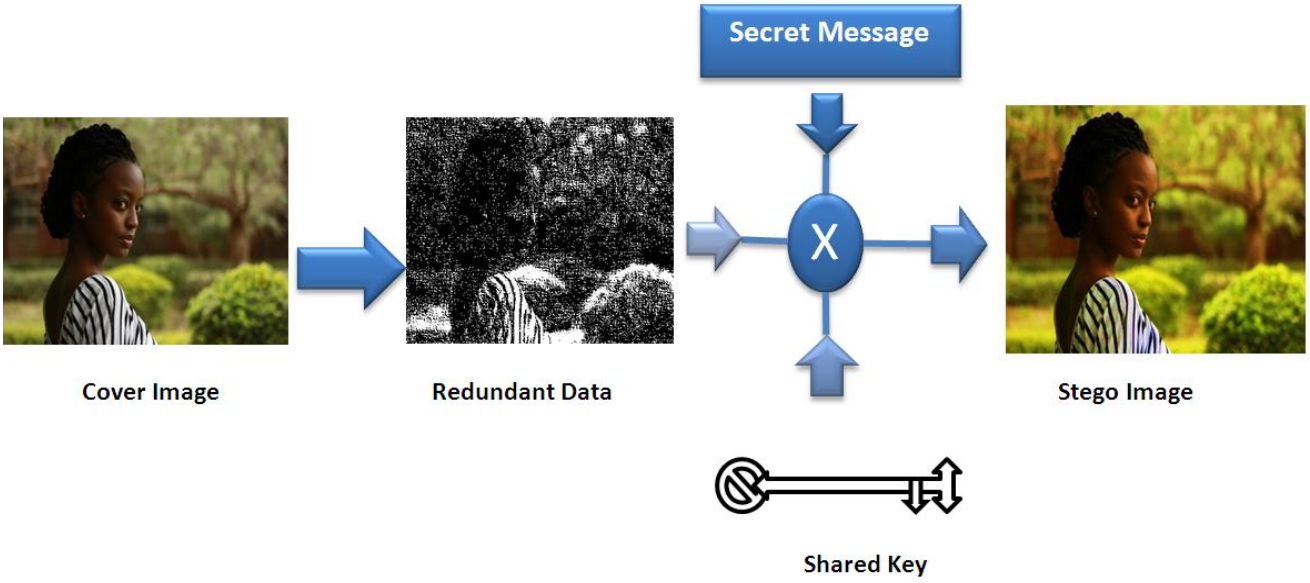


Figure 1.1 Private Key Steganography

1.1) A Cryptographic Framework

Cryptography ensures a method to authenticate and protect the transmission of information across insecure communication channels. It is a critical tool for protecting sensitive data in computer systems because it guarantees that unauthorized persons cannot read it. Cryptography offers the mechanisms necessary to provide accountability, accuracy and confidentiality of data.

2.) PROPOSED METHODOLOGY

2.1) DOMAINS USED

- **SPATIAL DOMAIN**

These techniques use the pixel gray levels and their color values directly for encoding the message bits. These techniques are some of the simplest schemes in terms of embedding and extraction complexity. This concept is used most often when discussing the frequency with which image values change, that is, over how many pixels does a cycle of periodically repeating intensity variations occur. One would refer to the number of pixels over which a pattern repeats (its periodicity) in the spatial domain. There are many versions of spatial steganography, the most widely known steganography algorithm is based on hiding the secret message in the LSBs (sequentially or randomly) of pixel values without introducing visual traces

- **TRANSFORM DOMAIN**

These techniques try to encode message bits in the transform domain coefficients of the image. Data embedding performed in the transform domain is widely used for robust watermarking. Similar techniques can also realize large-capacity embedding for steganography. Candidate transforms include Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Discrete Fourier Transform (DFT). In the proposed method Discrete Cosine Transform (DCT) is applied to the given cover image to get the DCT coefficients. The DCT transforms cover image from an image representation into a frequency representation, by grouping the pixels into non-overlapping blocks of 8×8 pixels and transforming the pixel blocks into 64 DCT coefficients each [8-10].

- **BLIND ATTACK DOMAIN**

The blind approach to steganalysis is similar to the pattern classification problem. The pattern classifier, in our case a Binary Classifier, is trained on a set of training data. The training data comprises of some high order statistics of the transform domain of a set of cover and stego images and on the basis of this trained dataset the classifier is presented with images for classification as a non-embedded or an embedded image. Many of the blind steganalytic techniques often try to estimate the cover image statistics from stego image by trying to minimize the effect of embedding in the stego image. This estimation is sometimes referred to as “Cover Image Prediction”

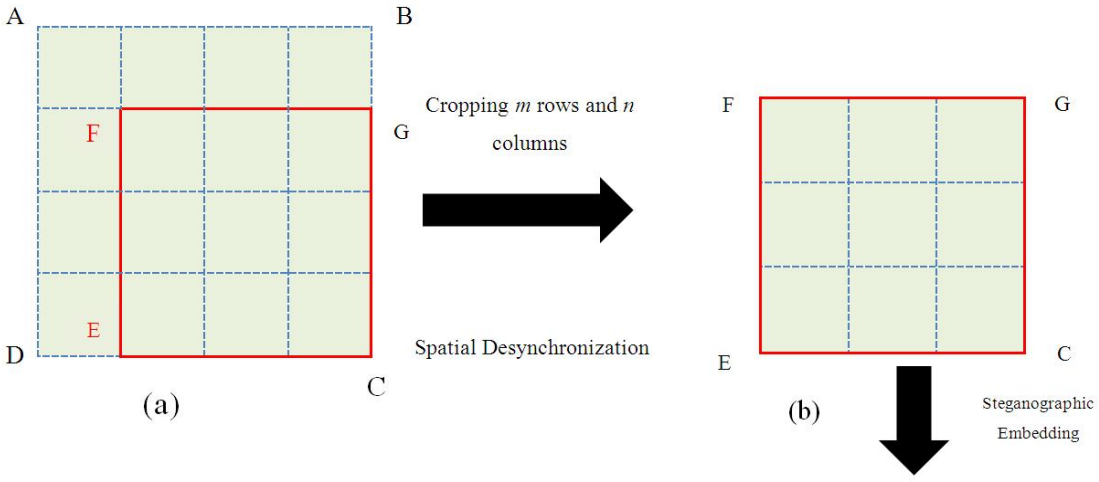
3.) PROPOSED SCHEME

A new steganographic framework is proposed to resist calibration based blind steganalytic attacks. The proposed framework which is based on spatial block desynchronization to disturb the successful prediction of cover image statistics from the stego image which is the key feature of calibration based steganalytic attacks. The proposed framework has been extended to a new steganographic algorithm called “S-BLOCK:(Low Detection

Steganography) using Modified Spatially Desynchronized Steganographic Algorithm". A comparative study with existing steganographic schemes has been carried out at different embedding rates on the basis of Area under the ROC and Detection Accuracy. It has been found that proposed algorithm shows better results than existing schemes in terms of detect ability against calibration based steganalytic attacks.

The main aim of the proposed scheme is to embed data in a spatially desynchronized version of the cover image so that the cover image statistics cannot be easily recovered from the stego image. The cover image is desynchronized by the partitioning scheme discussed above. The cropped version of the image $\hat{I}_{u,\,v}$ is used for steganographic embedding using any DCT domain scheme. After embedding, this embedded portion of the image is stitched with $I^{\delta}_{u,\,v}$to obtain the stego image $I_{\,s}$. The JPEG compressed version of $I_s$is communicated as the stego image.

Below a stepwise description of the algorithm is given.



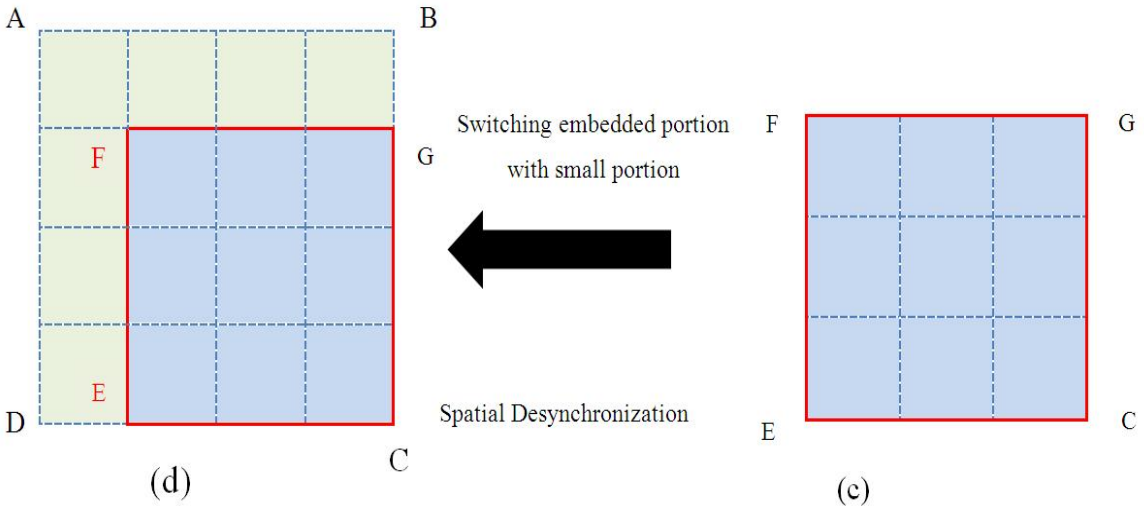


Figure 4.1: Spatial desynchronization used in the proposedS-BLOCKAlgorithm

4.) RESULT ANALYSIS

The MSBLOCK algorithm has been exposed pictorial original cover image from which the cropped image Î u, v portion is labeled as EFGH is extracted. Î u, v is then divided into non overlapping blocks size $m \times n$ as shown by solid lines. A DCT domain stenographicstructure is then applied to some of these blocks and Î u, v is finally attached with Iδ*u*, *v* to get the stego image Îs.

☐ Then the embedded image experiences JPEG compression before being connected to the decoding end, some of the embedded data bits might get lost in the procedure because of the quantization step through JPEG compression. Also embedded data can be made secure by adding some terminated bits in the data stream and using error-control coding methods. This problem of using error-control coding for securing the data bits has been addressed in (Solanki et al., 2009)albeit at the cost of *low embedding rate*. We would like to mention here that in our implementations of QIM, SSBA and SDSA we have not comprised any error-control technique. Let's associate the three schemes and verify our argument

Using Perfected outcome Hypothesis

Table 1.1: p-value of Rank Sum Test for 23 DCA

Embedding Rate(bpnc)	**QIM *p*-value**	**SSBA p-value**	**S-BLOCK: Low detection SDSA 8X8 p-value**

0.05	2.15×10^{-8}	0.0042	0.1180
0.10	0	2.44×10^{-4}	0.0065
0.25	0	1.12×10^{24}	4.23×10^{-6}
0.50	0	0	7.53×10^{-10}

Table 1.2: p-value of Rank Sum Test for 274 DCA

Embedding Rate(bpnc)	**QIM *p*-value**	**SSBA p-value**	**S-BLOCK: Low detection SDSA 8X8 p-value**
0.05	0.1907	0.7947	0.8652
0.10	0.0059	0.6734	0.7853
0.25	1.028×10^{-16}	0.3170	0.5213
0.50	0	9.27×10^{-6}	0.3525

5.) CONCLUSION

In this thesis we have explored two different approaches to Steganography. The first approach was aimed at preservation of the marginal statistics of a cover image. The preservation of marginal statistics helps in defeating the targeted attacks designed for specific steganographic algorithms. We covered two kinds of algorithms under this approach. The first algorithm was designed to inherently preserve the first order statistics of the cover image while embedding itself. It has been shown that this approach is able to resist first order statistics based targeted attacks while maintaining an acceptable quality of the stego image. The second algorithm was an attempt at explicitly restoring the marginal statistics which is inspired by chaos concept of the image after data has been embedded in the image. It was found that under a specified constraint the suggested algorithm is optimal in terms of the noise added due to the restoration procedure. It was also observed that although the restoration of the image statistics can resist targeted attacks, it does not improve the security of an embedding algorithm against blind attacks.

6.) REFERENCES

[1] Gunjan Nehru and Puja Dhar, "A Detailed Look Of Audio Steganography Techniques Using LSB And Genetic Algorithm Approach", International Journal of Computer Science (IJCSI),Vol.9,pp.402-406,Jan.2012.

[2] Fridrich, J. (2012). Modern Steganalysis Can Detect SSBA, 350.

[3] Gunjan Nehru and Puja Dhar, "A Detailed Look Of Audio Steganography Techniques Using LSB And Genetic Algorithm Approach", International Journal of Computer Science (IJCSI),Vol.9,pp.402-406,Jan.2012.

[4] Bhattacharyya, S., Banerjee, I., & Sanyal, G. (2011). A Survey of Steganography and Steganalysis Technique in Image , Text , Audio and Video as Cover Carrier. (I. Banerjee, Ed.)Journal of Global Research in Computer Science, 2(4).

[5]Kumar, M. (2011). Steganography And Steganalysis Of Joint Picture Expert Group (Jpeg) Images.

[6]Goljan, M., Fridrich, J., & Holotyak, T. (2011). New Blind Steganalysis and its Implications.

[7]Kumar, M. (2011). Steganography And Steganalysis Of Joint Picture Expert Group (Jpeg) Images.

[8]Budiman, A. (2010). Steganography Application On Video With Least Significant Bit (LSB) METHOD.

[9]Zhang, W., Zhang, X., & Wang, S. (2010). A Double Layered " Plus-Minus One " Data Embedding Scheme, *14*(11), 2010.

[10] A. C., Condell, J., Curran, K., & Kevitt, P. M. (2010). Digital image steganography : Survey and analysis of current methods. Signal Processing, *90*(3), 727–752. doi:10.1016/j.sigpro.

[11]Danti, A.; and Acharya, P. (2010). Randomized Embedding Scheme Based on DCT Coefficients for Image Steganography. IJCA Special Issue on "Recent Trends in Image Processing and Pattern Recognition", 2, 97-103.

[12] Krishna Bhowal, Anindya Jyoti Pal, Geetam S. Tomar, P.P. Sarkar, "Audio Steganography Using GA", CICN, 2010, Computational Intelligence and Communication Networks, International Conference on, Computational Intelligence and Communication Networks, International Conference on 2010, pp. 449-453, doi:10.1109/CICN.2010.

[13] Samir Kumar Bandyopadhyay*1, Tuhin Utsab Paul2 and Avishek Raychoudhury3," Genetic Algorithm Based Substitution Technique Of Imagesteganography", Journal of Global Research in Computer Science ISSN-2229-371X , Volume 1, No. 5, December 2010

[14] Lifang Yu · Yao Zhao · Rongrong Ni · Zhenfeng Zhu, "PM1 steganography in JPEG images using genetic algorithm" Soft Comput (2009) 13:393–400 DOI 10.1007/s00500-008-0327-7