Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 8, August 2015, pg.447 – 456

RESEARCH ARTICLE

SECURITY ENHANCEMENT: STEGANO-CRYPTO USING CHOAS BASED Sblock EMBEDDING TECHNIQUE

Shilpa Sangwan
Department of Computer
Science & Engineering
Panchkula Engineering
College, Mouli, Haryana
sangwanshilpa@gmail.com

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

Abstract

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. In this paper a study on digital image/text crypto- stegano has been presented. In order to further strengthen the encryption of the distorted image, a steganography approach for data hiding is also proposed. Experimental results have exposed that the association and entropy values of the encrypted text before the addition are same to the values of correlation and entropy after the insertion. Since the correlation and entropy of chaos base spastically block have hiding essential data, the method offers a good disguise of the data in the encrypted text/image, thus decreases the chance of the encrypted text actuality detected.

The first approach tries to overcome the targeted Steganalytic attacks. The work emphasis mainly on the first order data based targeted attacks. Two algorithms have been obtainable which can arrange the first order statistics of an image after embedding. The second approach aims at battling chaos based statically domain based Blind Attacks which try to estimate a model of the cover image from the stego image. Arithmetical Hypothesis Testing framework has been advanced for testing the efficiency of a blind attack and advances the effectiveness. In the proposed algorithm, the plain image is first decomposed into 8x8 size blocks and then the block based shuffling of image is carried out.

1.) INTRODUCTION

Due to the fast development of communication technology, it is convenient to acquire multimedia data. Unfortunately, the problem of illegal data access occurs every time and everywhere. Hence, it is important to protect the content and the authorized use of multimedia data against the attackers. Data encryption is a strategy to make the data unreadable, invisible or incomprehensible during transmission by scrambling the content of data.

In an image cryptosystem, it uses some reliable encryption algorithms or secret keys to transform or encrypt secret images into ciphered images. Only the authorized users can decrypt secret images from the ciphered images. The ciphered images are meaningless and non-recognizable for any unauthorized users who grab them without knowing the decryption algorithms

steganographic techniques refer to methods of embedding secret data into cover data in such a way that people cannot discern the existence of the hidden data. The image steganographic methods (or called virtual image cryptosystems) are proposed to hide the secret images into readable but non-critical cover images. They are designed to reduce the notice of illegal users. Common methods for data hiding can be categorized into spatial and transform domain methods. In the spatial domain, information hiding is an emerging research area, which encompasses applications such as copyright protection for digital media, watermarking, fingerprinting, and steganography.

In watermarking applications, the message contains information such as owner identification and a digital time stamp, which usually applied for copyright protection. Fingerprint, the owner of the data set embeds a serial number that uniquely identifies the user of the data set. This adds to copyright information to makes it possible to trace any unauthorized use of the data set back to the user. Steganography hide the secret message within the host data set and presence imperceptible and is to be reliably communicated to a receiver. The host data set is purposely corrupted, but in a covert way, designed to be invisible to an information analysis.

1.1) Blind Attacks

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”. Some of the most popular blind attacks are defined next.

Wavelet Moment Analysis (WAM): Wavelet Moment Analyzer (WAM) is the most popular Blind Steganalyzer for Spatial Domain Embedding. It has been proposed by

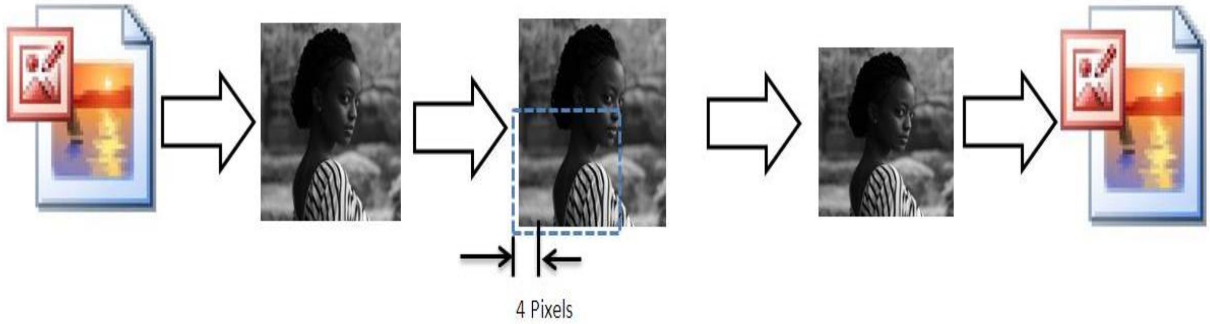


Figure 1.3 Calibration Of The Stego Image For Cover Statistics Estimation

As the filtering is performed in the wavelet domain, all the features (statistical moments) are calculated as higher order moments of the noise residual in the wavelet domain. The detailed procedure for calculating the WAM features in a gray scale image can be found in (Goljan et al., 2011). WAM is based on a 27 dimension feature space. It then uses a Fisher Linear Discriminant (FLD) as a classifier. It must be noted that WAM is a state of the art steganalyzer for Spatial Domain Embedding and no other blind attack has been reported which performs better than WAM.

2.) PROPOSED WORK

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.

2.1) S-BLOCK (LOW DETECTION STEGANOGRAPHY) USING MODIFIED STEGANOGRAPHIC ALGORITHM

AlgorithmS-BLOCK: Modified S-Steganographic Algorithm (MSblock)

Input: Cover Image I

Input Parameters: Rows and Columns to be cropped(**u, v**),Block size(**m× n**),Quantization Matrix (Q)

Output: Stego Image Is

Begin

1. Partition the cover image Ì into Î u, vand Ì u, v and $I^{\delta}_{U, V}$ by cropping *u* topmost rows and *v* leftmost columns.

2. Perform m×n non-overlapping block partitioning on $\hat{I}_{U, V}$.
Let us denote this set of blocks by$P_{I\ u,\ v}^{(m\times n)}$
3. Choose a set of blocks from $P_{\hat{I}\ u,\ v}^{(m\times n)}$ (using a key shared by both ends) and perform the embedding in each of the selected blocks using any standard DCT based steganographic scheme. The quantization matrix Q which is a shared secret is used for obtaining the quantized coefficients.
4. Apply dequantization and Inverse Discrete Cosine Transform (IDCT) to the set of blocks used for embedding in Step 3.
5. Join $I^{\delta}_{U,\ V}$with the resulting image obtained at Step 4. This combined image is the outputs Stego image I_S which is compressed using JPEG compression and communicated as the stego image.
EndModifiedSpatiallyDesynchronisedSteganographic Algorithm (MSblock)

2.2) MATHEMATICAL FORMULATION OF PROPOSED SCHEME

The proposed restoration scheme is dependent on the embedding scheme. The whole idea of embedding and restoring is that some of image pixels are used for embedding and rest are used for restoration. Without loss of generality, we can say that if number of pixels used for embedding is greater than 54% of the whole image then complete restoration is not possible but converse is not always true. One cannot say that if the numbers of available compensation pixels are greater than or equal to 54% of the whole image, then full compensation is possible. But we can certainly see that the probability of full compensation increases with increase in the number of pixels available for compensation.

Suppose Cij, Sij and Rij represent the (i, j) the pixel of C, S and R images respectively (0 <i< m, 0 < j < n, m is number of rows and n is number of columns of image matrices).

Embed Matrix (Ψ): It is a **m × n** characteristic matrix representing whether a pixel has been used for embedding or not.

$$\Psi\ (i, j) = \begin{cases} 1 & \text{If } (i, j)^{Th}\text{pixelis used for embedding} \\ 0 & \text{If } (i, j)^{Th}\text{pixel is not used for embedding} \end{cases} \qquad (3, 1)$$

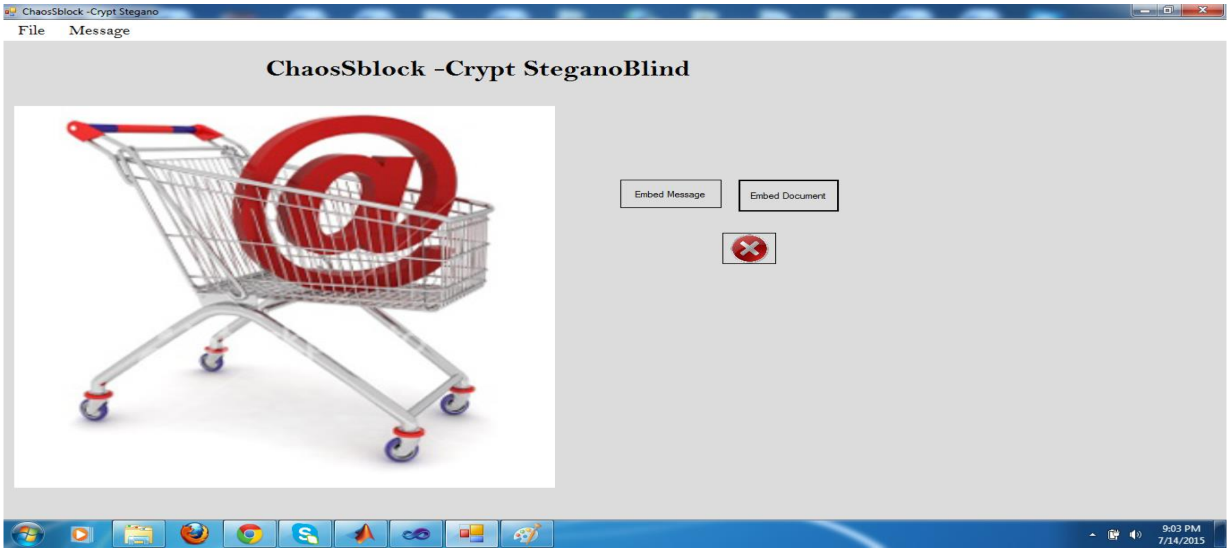
i. Compensation Vector *(Ω):* It is a one dimensional vector with length L where L is number of existing gray levels in the cover image (C). Ω (k) = u means that u number of pixels with gray value k can be used for restoration.

ii. Changed Matrix *(Γ):* It is an L × L matrix where L is number of existing gray levels in the cover image (C). Γ(x, y) = λ means during embedding λ number of pixels are changed from gray value x to gray value y.

3.) RESULT

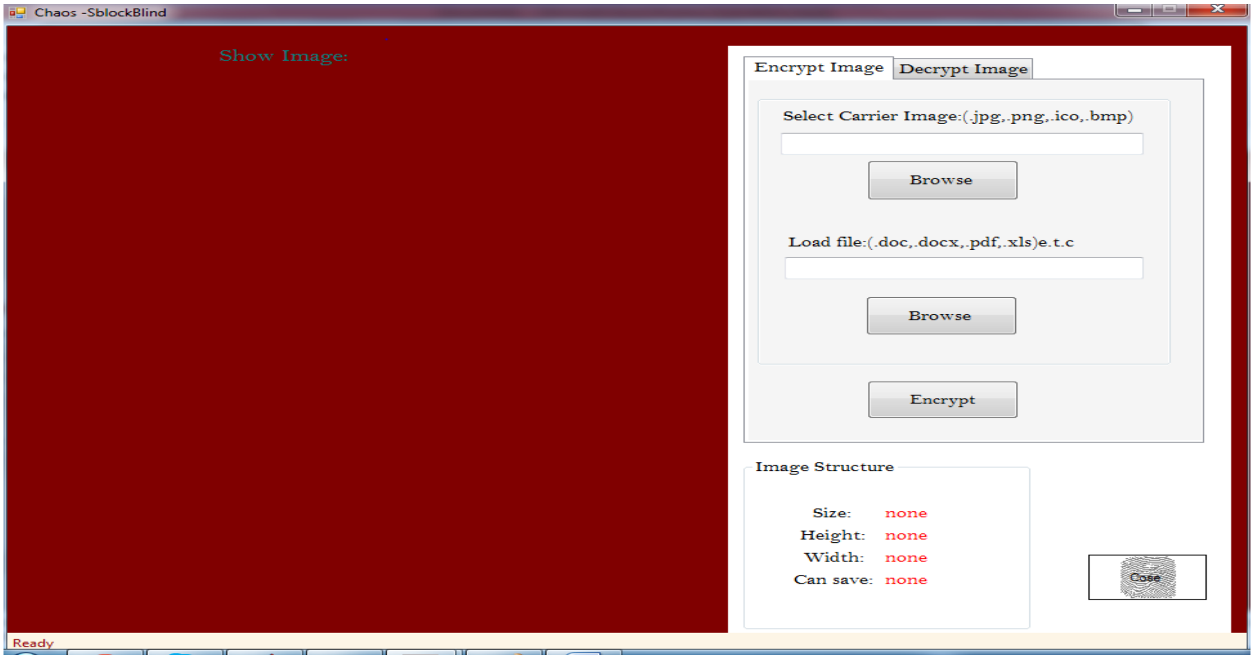
Stepwise analysis of the result is shown below:

1.)



ChaosSblock -Crypt SteganoBlind

2.)



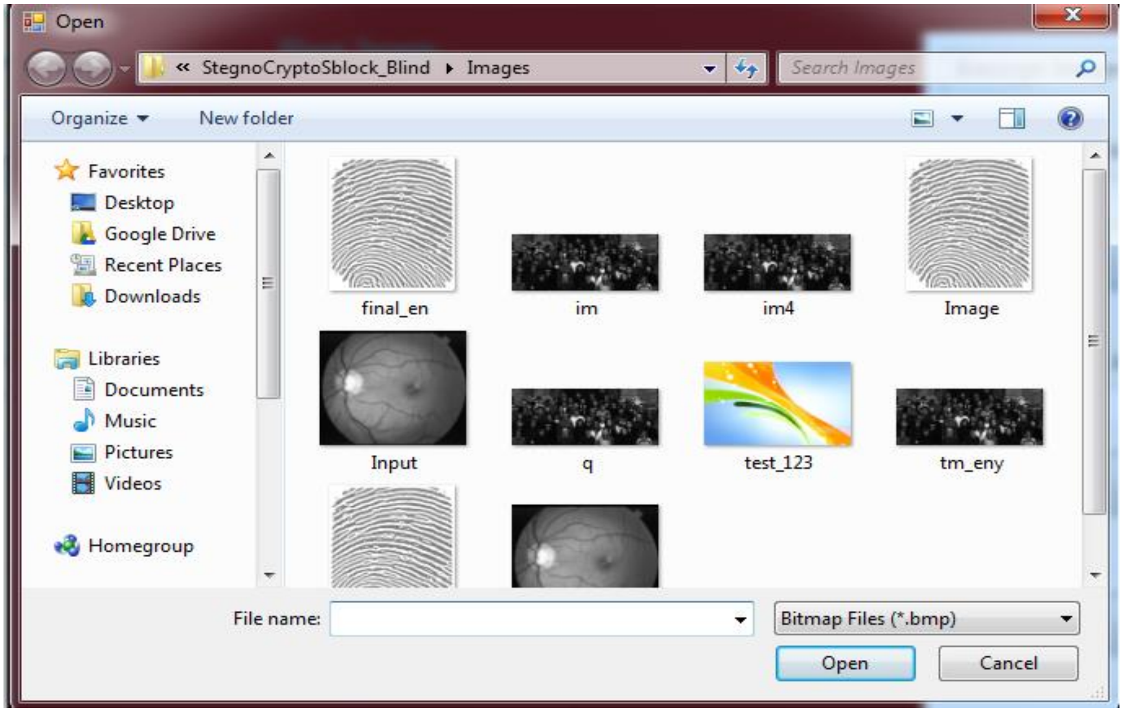
Select Carrier Image:(.jpg,.png,.ico,.bmp)

Load file:(.doc,.docx,.pdf,.xls)e.t.c

Image Structure

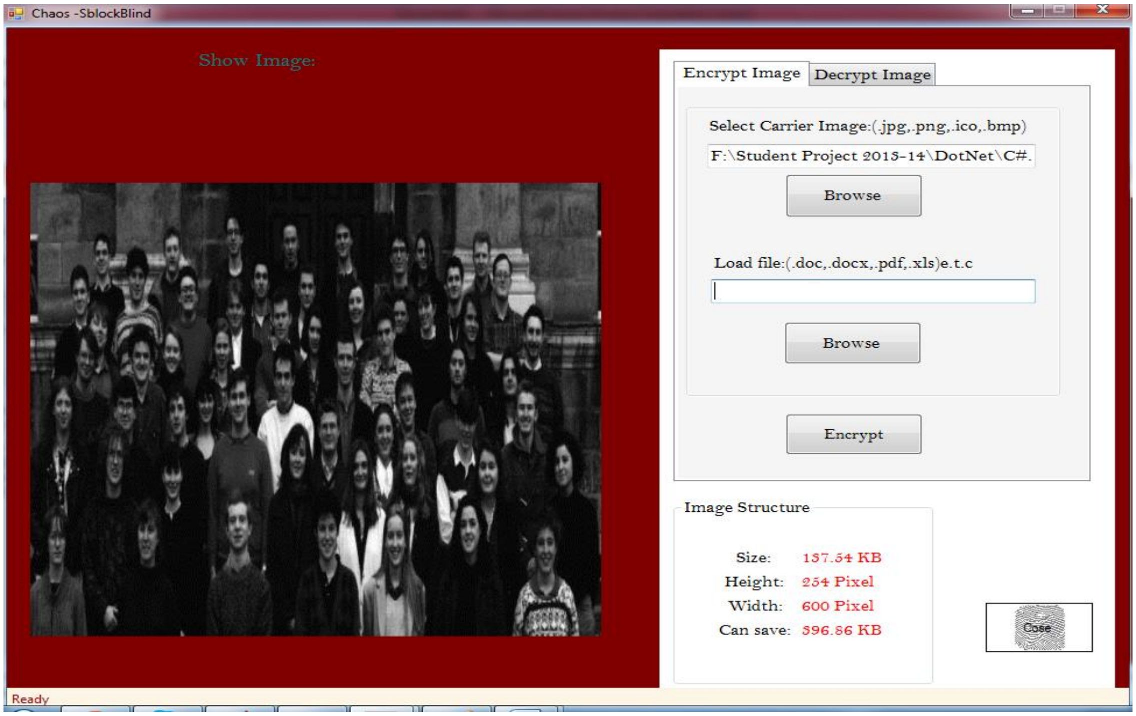
Size: none
Height: none
Width: none
Can save: none

3.)



Bitmap Files (*.bmp)

4.)



Select Carrier Image:(.jpg,.png,.ico,.bmp)

F:\Student Project 2013-14\DotNet\C#.

Load file:(.doc,.docx,.pdf,.xls)e.t.c

Image Structure

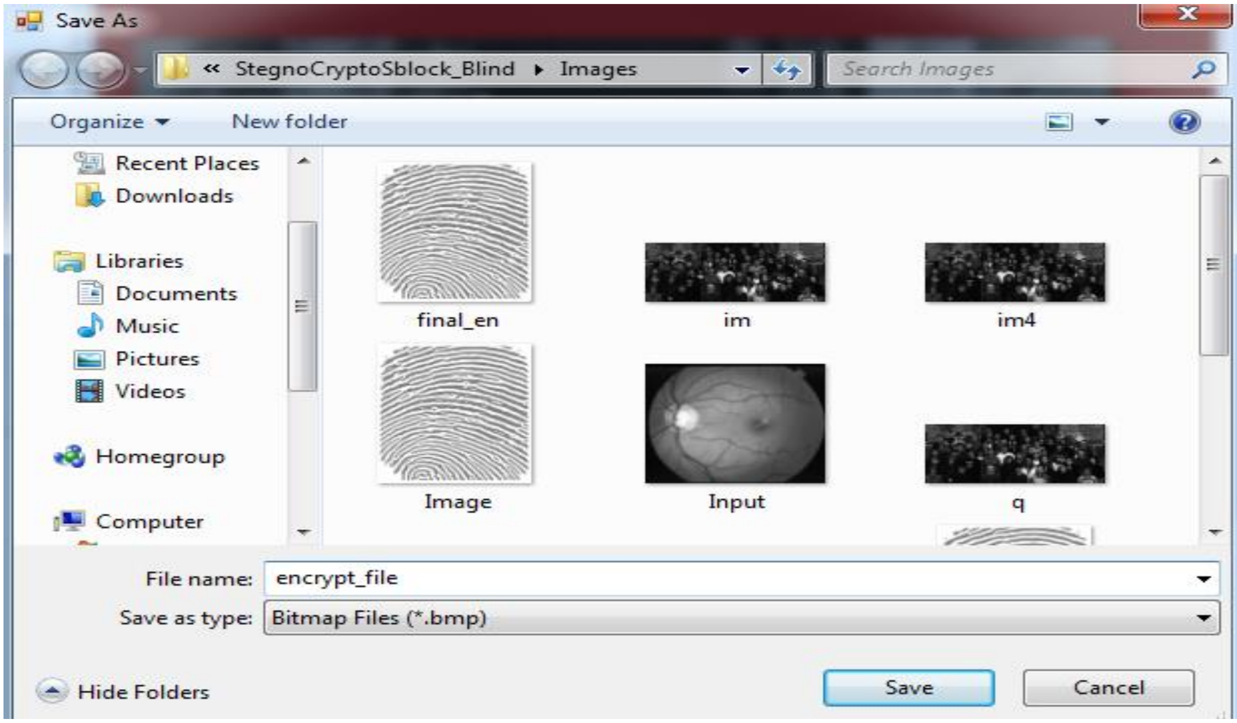
Size: 157.54 KB

Height: 254 Pixel

Width: 600 Pixel

Can save: 396.86 KB

5.)



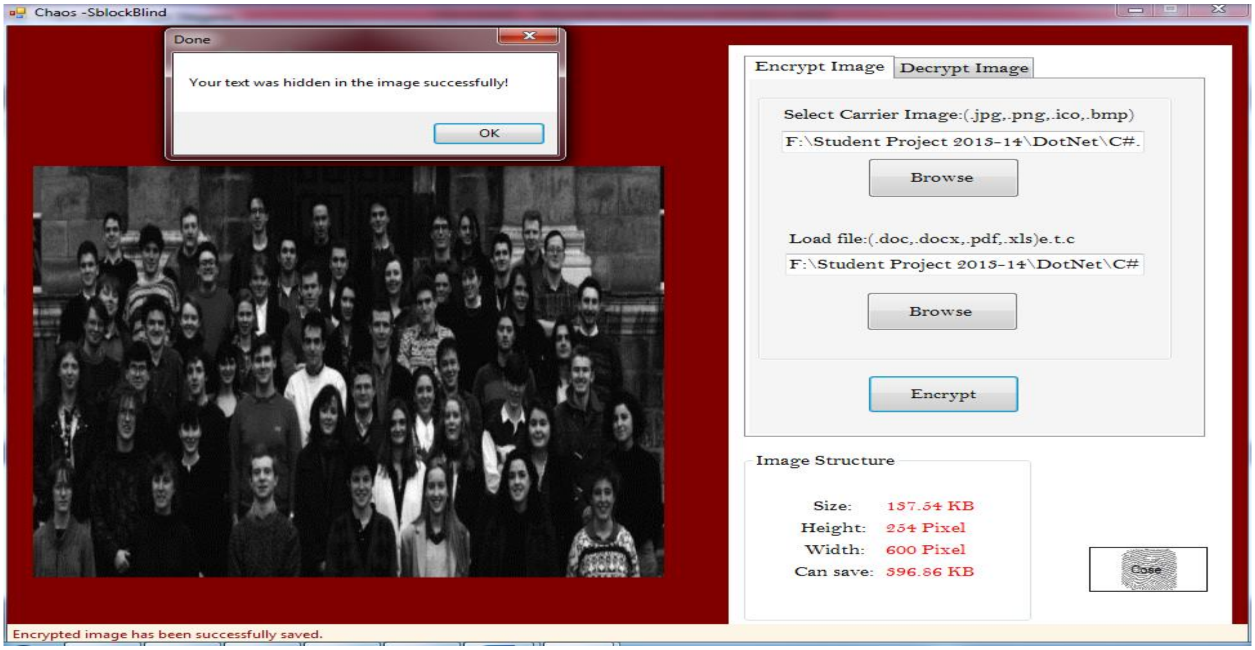
Save As

« StegnoCryptoSblock_Blind ▸ Images

File name: encrypt_file

Save as type: Bitmap Files (*.bmp)

6.)



Chaos -SblockBlind

Done

Your text was hidden in the image successfully!

Select Carrier Image:(.jpg,.png,.ico,.bmp)

F:\Student Project 2013-14\DotNet\C#.

Load file:(.doc,.docx,.pdf,.xls)e.t.c

F:\Student Project 2013-14\DotNet\C#

Image Structure

Size: 157.54 KB

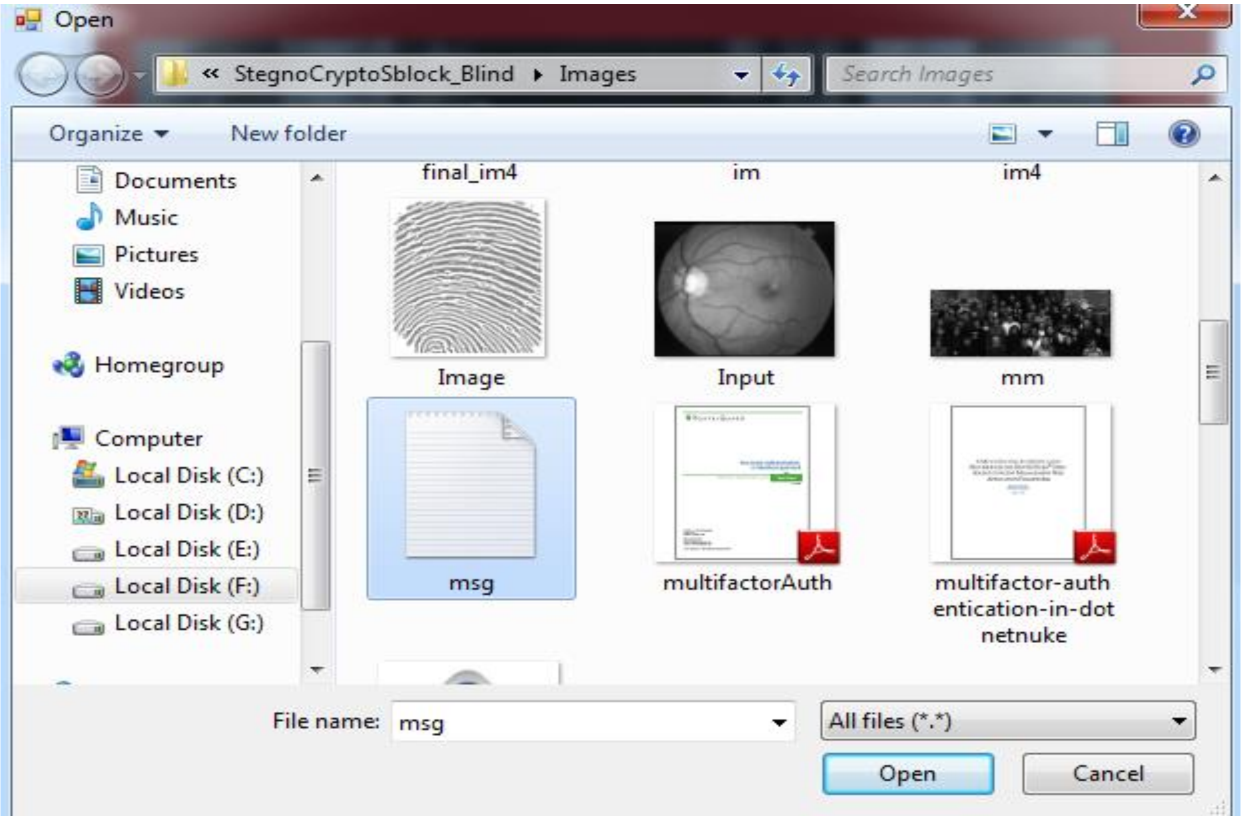
Height: 254 Pixel

Width: 600 Pixel

Can save: 396.86 KB

Encrypted image has been successfully saved.

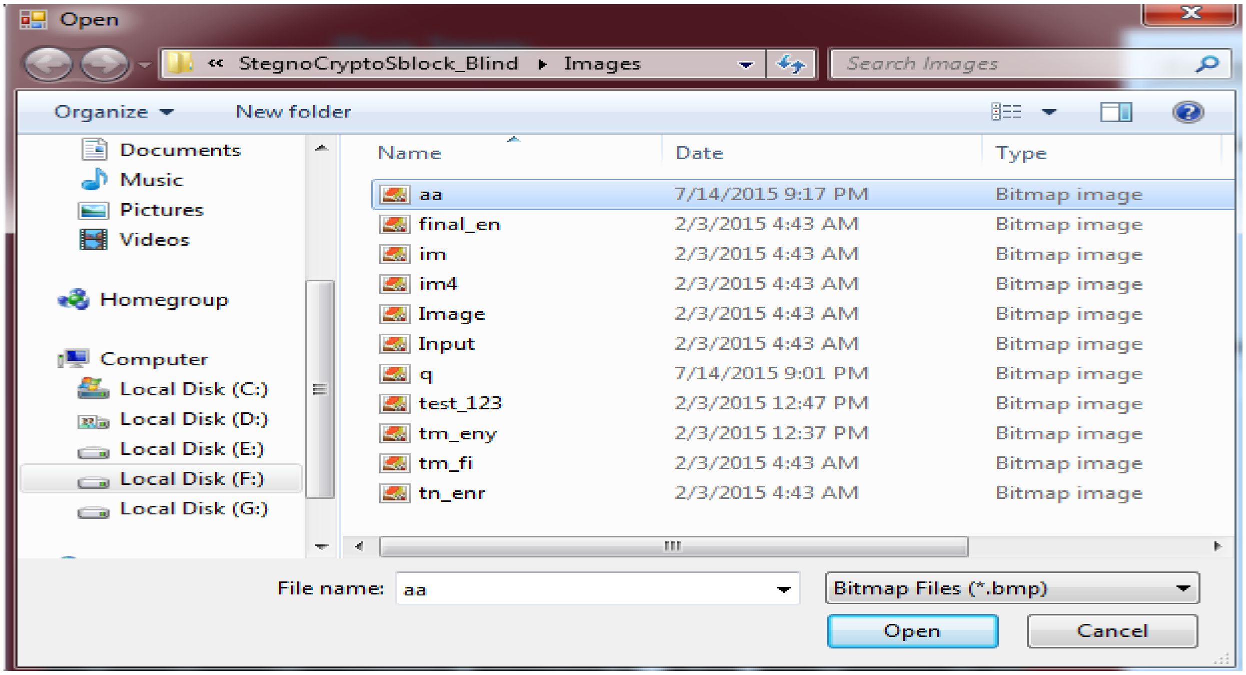
7.)



File name: msg

All files (*.*)

8.)

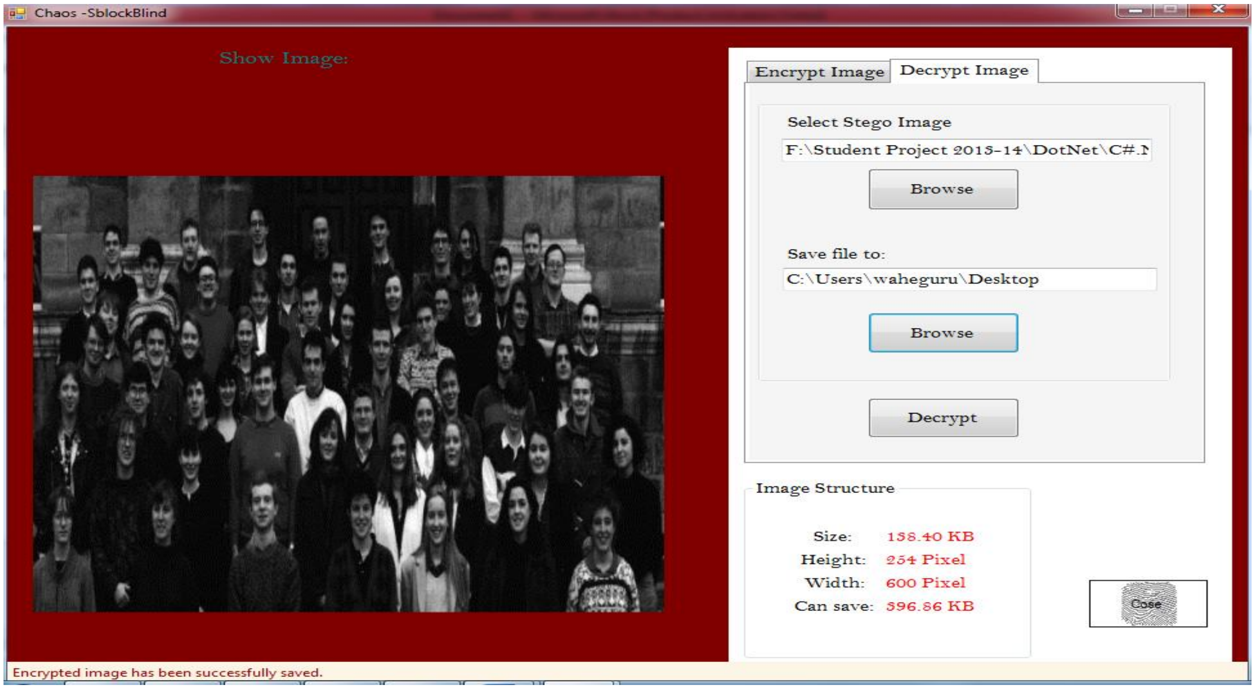


Name	Date	Type
aa	7/14/2015 9:17 PM	Bitmap image
final_en	2/3/2015 4:43 AM	Bitmap image
im	2/3/2015 4:43 AM	Bitmap image
im4	2/3/2015 4:43 AM	Bitmap image
Image	2/3/2015 4:43 AM	Bitmap image
Input	2/3/2015 4:43 AM	Bitmap image
q	7/14/2015 9:01 PM	Bitmap image
test_123	2/3/2015 12:47 PM	Bitmap image
tm_eny	2/3/2015 12:37 PM	Bitmap image
tm_fi	2/3/2015 4:43 AM	Bitmap image
tn_enr	2/3/2015 4:43 AM	Bitmap image

File name: aa

Bitmap Files (*.bmp)

9.)



F:\Student Project 2013-14\DotNet\C#.N

C:\Users\waheguru\Desktop

Size: 138.40 KB
Height: 254 Pixel
Width: 600 Pixel
Can save: 396.86 KB

Encrypted image has been successfully saved.

4.) CONCLUSION

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.

The framework was extended to a new algorithm for JPEG domain steganography. This algorithm was evaluated in the proposed statistical testing framework and it was found that the algorithm is successful in breaking the calibration based blind attacks.

REFERENCES

[1] M. Ramkumar & A.N. Akansu.(2009) "Some Design Issues For Robust Data hiding Systems", url:http://citeseer.nj.nec.com/404009.html

[2] Kodovský, J., & Fridrich, J. (2009). What is Calibration?

[3] Mazdak Zamani1, Azizah A. Manaf2, Rabiah B. Ahmad3, Akram M. Zeki4, and Shahidan Abdullah5, "A Genetic- Algorithm-Based Approach for Audio Steganography", World Academy of Science, Engineering and Technology 54 2009

[4].Mazdak, Z., A.M. Azizah, B.A. Rabiah, M.Z. Akram and A.., Shahidan, " A genetic-algorithm-based approach for audio steganography", World Acad. Sci.Eng.,-2009 Technol., 52: 360-363.

[5] Zamani, M., Manaf, A, Ahmad, R.B., Jaryani, F., Taherdoost H., Zeki, AM.,"A secure audio steganography approach", International Conference for Internet Technology and Secured Transactions 2009, Page(s):1 - 6.

[6] Solanki, K., Dabeer, O., Madhow, U., Manjunath, B. S., & Chandrasekaran, S. (2009). Robust Image-Adaptive Data Hiding : Modeling , Source Coding and Channel Coding Image-adaptive Hiding via Selective Embedding in Coefficients.

[7] Science, C., & Goel, P. (2008). Data Hiding in Digital Images: A Steganographic Paradigm, (03).

[8] H.-C Huang, J. S. Pan, Y. H. Huang, and K.-C. Huang, "Progressive watermarking techniques using Genetic Algorithms", Circuits, Systems, and Signal Processing,8,(2007)58-68.

[9] Ker, A. (2007). A Fusion of Maximum Likelihood and Structural Steganalysis A Fusion of Maximum Likelihood and Structural Steganalysis Outline, (June).

[10] Fridrich, T. Pevny, and J. Kodovsky, "Statistically Undetectable JPEG Steganography: Dead Ends, Challenges, and Opportunities", in Proc. ACMMultimedia and Security Workshop, Dallas, TX, 20-21 Sept. 2007, pp. 3-14.

[11] Fridrich, M. Goljan, and T. Holotyak, "New Blind Steganalysis and its Implications", in Proc. SPIE Security, Steganography, andWatermarking of Multimedia Contents VIII, vol. 6072, pp. 607201, Jan. 2006

[12] J. Fridrich, and D. Soukal, "Matrix Embedding for Large Payloads", IEEE Trans. on In- formation Forensics and Security, vol. 1, Sept. 2006, pp. 390-395

[13] Sullivan, K., Solanki, K., Manjunath, B. S., Madhow, U., & Chandrasekaran, S. (2006). S. Manjunath, U. Madhow,, 121–124.

[14]Mao, Wenbo (2004).Modern Cryptography Theory and Practice ISBN 0-13-066943-1. An up-to-date book on cryptography.