NEURAL NETWORK BASED STEGANALYSIS FRAMEWORK TO DETECT STEGO-CONTENT IN CORPORATE EMAILS

P. T. Anitha
Department of Computer Applications
Karpagam College of Engineering,
Coimbatore 641032, Tamilnadu, India
anitha_pt@yahoo.com

M. Rajaram
Anna University of Technology,
Tirunelveli, Tamilnadu, India
rajaramgct@redifmail.com

S. N. Sivanandham
Karpagam Group of Institutions,
Coimbatore 641032, Tamilnadu, India
snsprof25@yahoo.com

Abstract

Today, email management is not only a filing and storage challenge. Because law firms and attorneys must be equipped to take control of litigation, email authenticity must be unquestionable with strong chains of custody, constant availability, and tamper-proof security. Information Security and integrity are becoming more important as we use email for personal communication and business. Email is insecure. This steganalysis framework checks the inbox content of the corporate mails by improving the S-DES algorithm with the help of neural network approach. A new filtering algorithm is also developed which will used to extract only the JPG images from the corporate emails. This frame work developed a new steganalysis algorithm based on neural network to get statistical features of images to identify the underlying hidden data. The Experimental results indicate this method is valid in steganalysis. This method will be used for Internet/network security, watermarking and so on.

Keywords: Steganalysis, Steganography, Information Hiding, LSB, Stegdetect, Stego, Outguess

1. Introduction

Steganalysis is to detect and/or estimate potentially hidden information from observed data with little or no knowledge about the steganography algorithm and/or its parameters. Steganalysis is both an art and a science. While it is possible to design a reasonably good steganalysis technique for a specific steganographic algorithm, the long term goal is to develop a steganalysis framework that can work effectively at least for a class of steganography methods, if not for all. Current trend in steganalysis seems to suggest two extreme approaches: (a) little or no statistical assumptions about the image under investigation. Statistics are learnt using a large database of training images and (b) a parametric model is assumed for the image and its statistics are computed for steganalysis detection. In this proposed research work developed a framework which is used to analyze the stego content in the corporate emails.

Steganalysis is the science of detecting the presence of hidden data in the cover media files and is emerging in parallel with steganography. Steganalysis has gained prominence in national security and forensic sciences since detection of hidden messages can lead to the prevention of disastrous security incidents.

2. Image Steganalysis

Algorithms for image steganalysis are primarily of two types: *Specific and Generic*. The *Specific approach* represents a class of image steganalysis techniques that very much depend on the underlying steganographic algorithm used and have a high success rate for detecting the presence of the secret message if the message is hidden with the algorithm for which the techniques are meant for. The *Generic approach* represents a class of image steganalysis techniques that are independent of the underlying steganography algorithm used to hide the message and produces good results for detecting the presence of a secrete message hidden using new and/or unconventional steganographic algorithms.

.

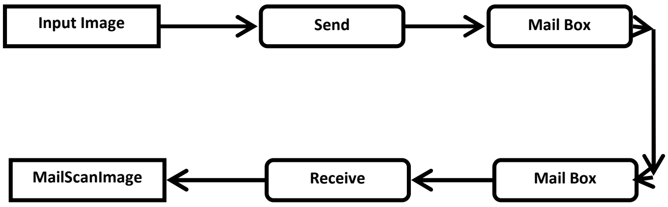


Fig. 1 Systems flow Diagram

ISSN : 2349 - 6363

3. Hybrid Algorithm

The S_DES is the best known and most widely used cryptosystem for civilian applications. It was developed at IBM and adopted by the National Bureau of Standards in the mid 1970s, and has successfully withstood all the attacks published so far in the open literature. The proposed work developed a frame work which contains the following tasks*: Image separation from corporate mails using the newly developed capturing algorithm, Compression, encryption, hiding, decryption, and decompression steps.*

3.1 The Capturing algorithm

The algorithm checks the mail inbox only for JPEG files. This filtering concept helps us to minimize the seeking time of filtering the JPEG files. After filtering those files they are stored in a large database for further processing. A sample image is taken from the database as covert channel which is used to hide the secret information. For our experiments, we created a database containing more than 20000 JPG images obtained from corporate mails. For each image, we embedded a random binary stream of different lengths using S-DES algorithm. The proposed research analyzes the performance of the improved version of image steganalysis algorithms in corporate mails. A large database is used to store the images. The performance and the detection ratio are going to be measured in corporate mails.

3.2 S-DES method of encryption

This method is an example of a block cipher: the plain text is split into blocks of a certain size, in this case 8 bits.

$$\text{plaintext} = b_1b_2b_3b_4b_5b_6b_7b_8$$
$$\text{key} = k_1k_2k_3k_4k_5k_6k_7k_8k_9k_{10}$$

Subkey generation

First, produce two subkeys K_1 and K_2:

$$K_1 = P8(LS_1(P10(\text{key})))$$
$$K_2 = P8(LS_2(LS_1(P10(\text{key}))))$$

where P8, P10, LS1 and LS2 are *bit substitution operators.* For example, P10 takes 10 bits and returns the same 10 bits in a different order:

$$P10(k_1k_2k_3k_4k_5k_6k_7k_8k_9k_{10}) = k_3k_5k_2k_7k_4k_{10}k_1k_9k_8k_6.$$

The plain text is split into 8-bit blocks; each block is encrypted separately. Given a plaintext block, the cipher text is defined using the two subkeys K_1 and K_2, as follows:

$$\text{ciphertext} = IP^{-1}(\ f_{K2}(\ SW(\ f_{K1}(\ IP(\ \text{plaintext}\ )\ )\ )\ )\ )$$

and $f_K(\ )$ is computed as follows. We write exclusive-OR (XOR) as +.

$$f_K(\ L, R\ ) = (\ L + F_K(R)\ , R\ )$$

$$F_K(R) = P4\ (\ \ S0(\ lhs(\ EP(R)+K\ ))\ \ ,\ \ S1(\ rhs(EP(R)+K\ ))\ \ )$$

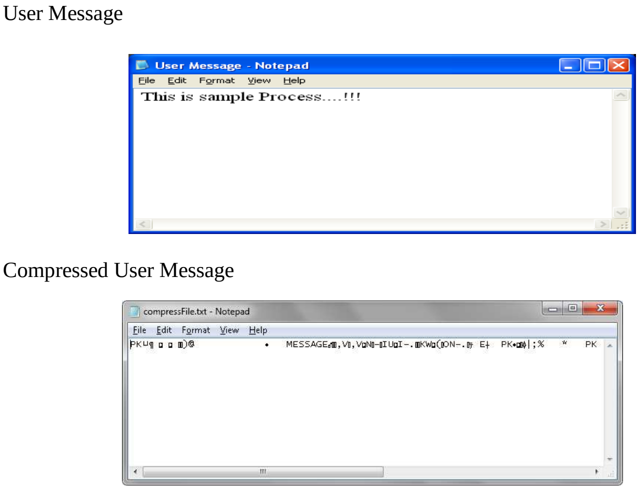
Once sample image and embedded information are finalized then it is compressed with the help of JPEG compression algorithm.

3.3 IMAGE compression

The compression of the image aims at reducing the number of bits needed to represent an image. Image compression algorithms take into account the psycho visual features both in space and frequency domain and exploit the spatial correlation along with the statistical redundancy. However, usages of the algorithms are dependent mostly on the information contained in images. In *JPEG compression*, the image is first divided into disjoint blocks of 8×8 pixels. For each block B_{orig} (with integer pixel values in the range 0−255), the discrete cosine transform (DCT) is calculated, producing 64 DCT coefficients. Let us denote the i-th DCT coefficient of the k- th block as

$$d_k(i),\ 0 \le i \le 64,\ k = 1, \dots T$$

where T is the total number of blocks in the image. The quantized coefficients $D_k(i)$ are arranged in a zigzag manner and compressed using the Huffman coder. The resulting compressed stream together with a header forms the final JPEG file.



User Message

User Message - Notepad
File Edit Format View Help

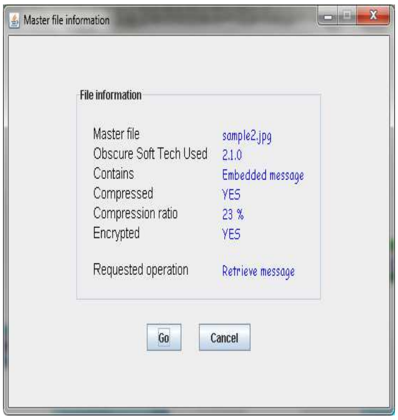
This is sample Process....!!!

Compressed User Message

compressFile.txt - Notepad
File Edit Format View Help

```
PK␣¶ ▫ ▫ ▯)@        •    MESSAGE▯▯,V▯,V▯N▯-▯IU▯I-.▯KW▯(▯ON-.▯ E+   PK•▯▯|;%    ᴴ    PK
```

Fig. 2 Compression



Master file information

File information

Master file sample2.jpg
Obscure Soft Tech Used 2.1.0
Contains Embedded message
Compressed YES
Compression ratio 23 %
Encrypted YES

Requested operation Retrieve message

Fig. 3 Ratio of Compression

Decryption

Decryption is a similar process.

plaintext = $IP^{-1}(f_{K1}(SW(f_{K2}(IP(ciphertext)))))$

Relation with DES

SDES is a simplification of a real algorithm. DES operates on 64 bit blocks, and uses a key of 56 bits, from which sixteen 48-bit subkeys are generated. There is an initial permutation (IP) of 56 bits followed by a sequence of shifts and permutations of 48 bits. F acts on 32 bits.

ciphertext = $IP^{-1}(f_{K16}(SW(f_{K15}(. . . (SW(f_{K1}(IP(plaintext)))). . .))))$

SDES do a lot of re-arranging of bits that makes it hard to analyze systematically. Additionally, the S-boxes mean that the output is not just a re-arrangement of the input bits, but is derived from the input bits in a non-linear way. This adds significantly to the security.

S-DES encryption (decryption) algorithm takes 8-bit block of plaintext (cipher text) and a 10-bit key, and produces 8-bit cipher text (plaintext) block. Encryption algorithm involves 5 functions: an initial permutation (IP); a complex function fK, which involves both permutation and substitution and depends on a key input; a simple permutation function that switches (SW) the 2 halves of the data; the function fK again; and finally, a permutation 2 function that is the inverse of the initial permutation (IP-1)[6].

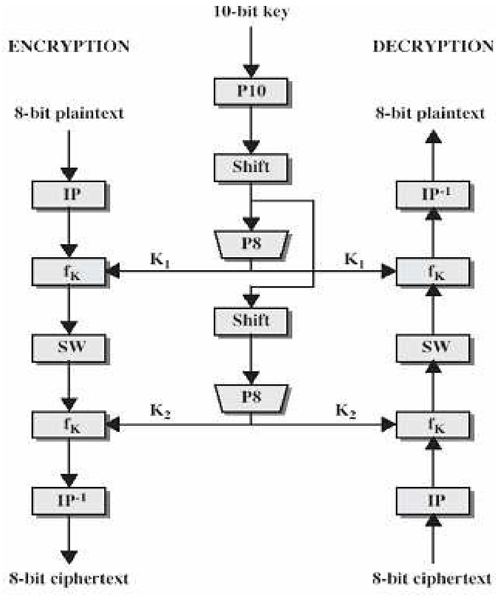


Fig. 4 Simplified DES Scheme

Decryption process is similar. The function fK takes 8-bit key which is obtained from the 10-bit initial one two times. The key is first subjected to a permutation P10. Then a shift operation is performed. The output of the shift operation then passes through a permutation function that produces an 8-bit output (P8) for the first subkey (K1). The output of the shift operation also feeds into another shift and another instance of P8 to produce the second subkey K2.

We can express encryption algorithm as superposition:

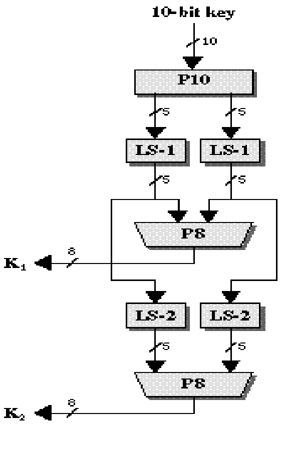


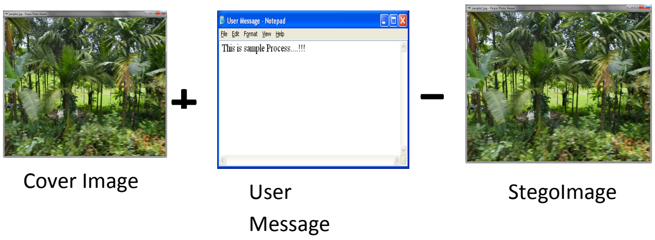
Fig. 5Key generation for Simplified DES

The 10-bit key is transformed into two 8-bit sub-keys K1 and K2.

4. Information Detection based on Neural Networks

The neural network approach is used to check for the discrepancy patterns and train itself for better accuracy by automating the whole process [7]. This study used neural network to analyze object digital image based on three different types of transformation which are Domain Frequency Transform (DFT), Domain Coefficient Transform (DCT) and Domain Wavelet Transform (DWT).

In this paper, we only consider following transforms, DFT, DCT and DWT. Firstly we analysis object digital image according these three different kinds transforms in this method. The object image is transformed into transform domain data according these three transforms. Then calculate these transforms data's statistical features which can be exploited to detect hided information. The reason for selecting DFT, DCT and DWT is that most data hiding method operate in these domains. These selected features should be significantly impacted by the data hiding processing. But it is difficult to find those features, so we select neural network to process this problem, neural network has the super capability to approximation any nonlinear functions. For these features which have more effected by data hiding process, neural network will assign larger weight coefficients and for these features which have less effected by data hiding process, neural network will assign less weight coefficients.



This is sample Process....!!!

Fig. 6 The Process Of Embedded Message

4.1 BACK-PROPAGATION ALGORITHM

Back-propagation algorithm [7] is a widely used learning algorithm in Artificial Neural Networks. The Feed-Forward Neural Network architecture (Fig. 7) is capable of approximating most problems with high accuracy and generalization ability.

$$y_k(t+1) = \mathcal{F}_k(s_k(t)) = \mathcal{F}_k\left(\sum_j w_{jk}(t)\, y_j(t) + \theta_k(t)\right)$$

This algorithm is based on the error correction learning rule. Error propagation consists of two passes through the different layers of the network, a *forward pass and a backward pass*. In the forward pass the input vector is applied to the sensory nodes of the network and its effect propagates through the network layer by layer. Finally a set of outputs is produced as the actual response of the network. During the forward pass the synaptic weight of the networks are all fixed. During the back pass the synaptic weights are all adjusted in accordance with an error-correction rule.

The actual response of the network is subtracted from the desired response to produce an error signal. This error signal is then propagated backward through the network against the direction of synaptic conditions. The synaptic weights are adjusted to make the actual response of the network move closer to the desired response. [8]

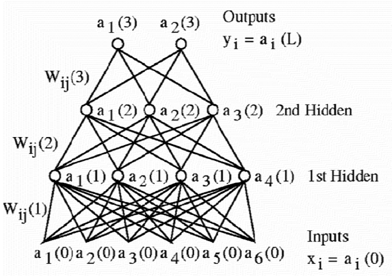


Fig. 7 Feed-Forward Neural Network Architecture

The output of the hidden units is distributed over the next layer of Nh;2 hidden units, until the last layer of hidden units, of which the outputs are fed into a layer of No output units.

5. Image Features Extracting

First we analysis image's discrete cosine transform domain's statistics features. We divide each image into 8×8 sub-block and then take DCT of each sub-block. Based on analysis of I. Aveibas et.al work [5], data hiding process possesses statistical difference in image quality metric scores obtained from blurred-and-hidden images as compared to blurred-but-non-hidden host images. We select spectral measures based on DFT and DCT. In DFT data hiding process, one quantize the magnitude to hide information and can't change the phase information (this is very important), so selecting metrics based on magnitude (two statistics, image and its sub block) In DWT, we select these same metrics with in DFT. Finally in DFT and DCT, we select 4 statistics.

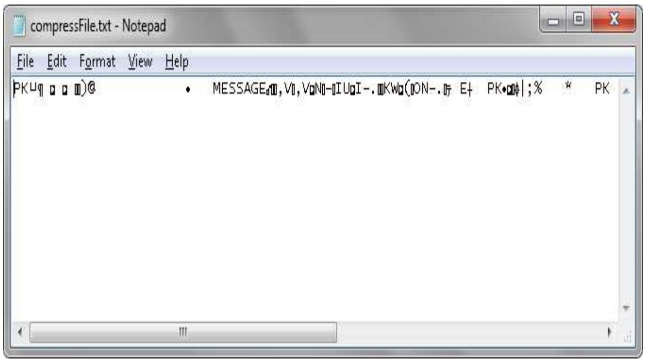
Next we take three levels DWT of each training images, and we calculate the mean value, variance, skew ness and kurtosis of each part of every level. Then according pyramid algorithm's characteristic to forecast the original data then calculate the error's statistics features [4]. Because in calculating process, variance is very larger than other statistics, we give up variance statistics. So every image only has 36 statistics. Added with DCT's 4 statistics based image metrics, each image has 40 statistics. So we set the number of neural network input as 40, the output is one.

6. Performance Analysis and Experiment Results

From the measured statistics of training sets of images with and without hidden information, our destination is to determine whether an image has been hidden information or not. Neural network has an excellent capability to simulate any nonlinear relation, so we make use of neural network to classify images [11]. In this paper we take use of BP neural network to train and simulate images [6]. This BP neural network uses three levels: Input level, Hidden level and Output level. In neural network, the important issue is the slow of convergence. In practice, this is the main limitation of neural network applications. And many new algorithms claimed fast convergence were developed. In this paper a single parameter dynamic search algorithm is used to accelerate network train. Each time only one parameter to be searched to achieve best performance, so this learning algorithm has a better improvement than other old algorithms ([9, 10]). We set the number of this network's input as features, and node number of hidden level is set to be 40, and output is either yes or no.

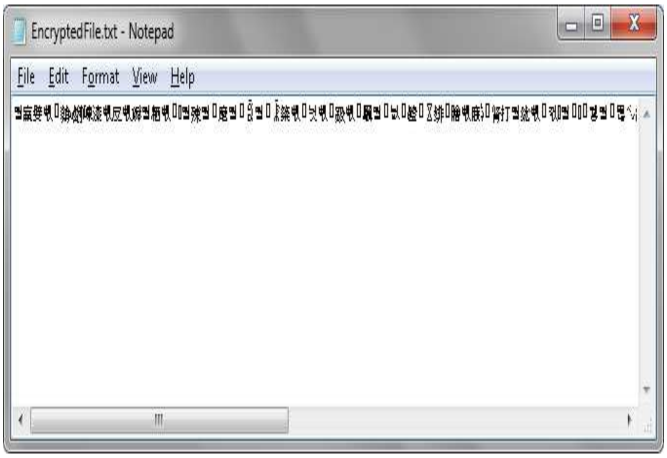
7. Test Results (GUI based)

The cover image was taken from the image database. The image was originally in JPEG format in 680x480 resolutions. Since a BMP image was also required for the evaluation, a second image in BMP format was generated using the same JPEG image using Gimp. Once both the cover images have been obtained, the proposed method generates the secret code for both the images were created.



```
PK⊔¶ ▫ ▫ ▯)@          •     MESSAGE◢▯,V▯,V▯N▯-▯IU▯I-.▯KW▯(▯ON-.▯ E‡   PK•▯▯|;%    *    PK
```

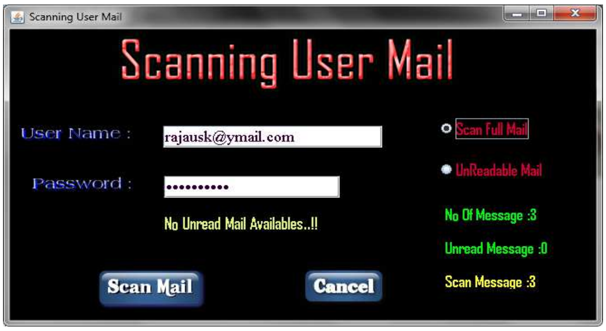
Fig. 8 After Compression User Message



[illegible]

Fig. 9 After Encryption User Message

Scanning Reports



User Name : rajausk@ymail.com

Password : ••••••••••

○ Scan Full Mail

● UnReadable Mail

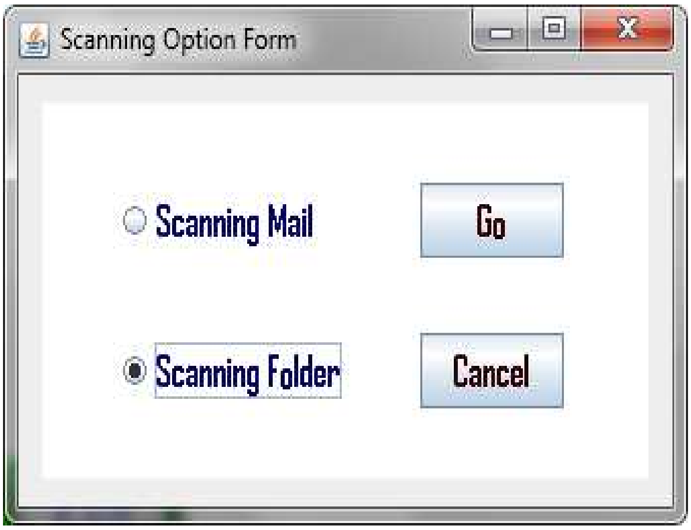
No Unread Mail Availables..!!

No Of Message :3

Unread Message :0

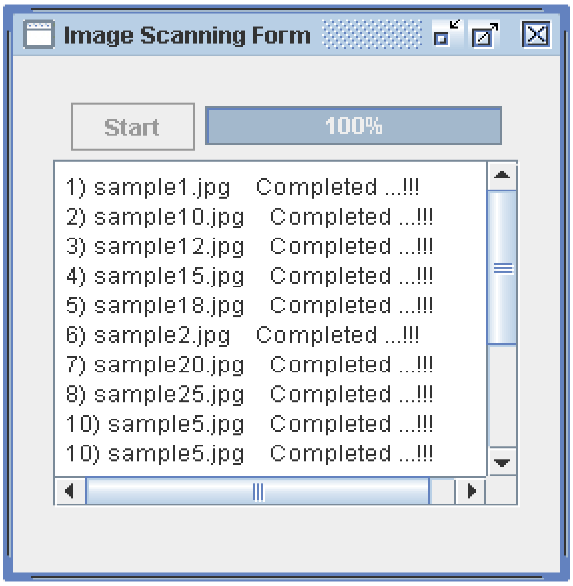
Scan Message :3

Select Scanning Option

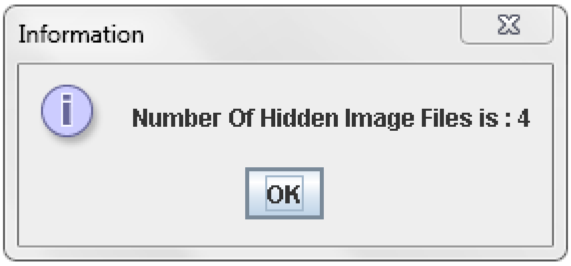


○ Scanning Mail

● Scanning Folder



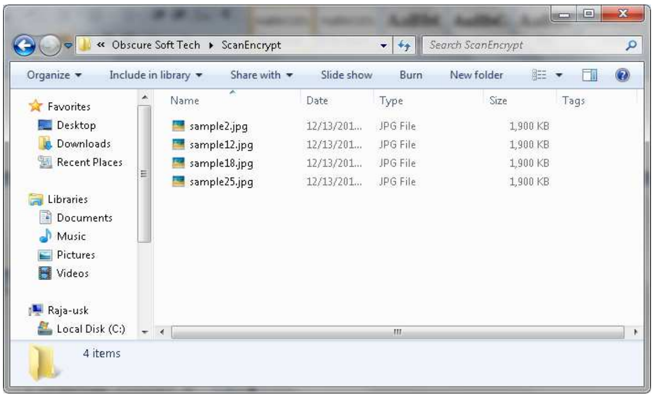
```
1) sample1.jpg   Completed ...!!!
2) sample10.jpg   Completed ...!!!
3) sample12.jpg   Completed ...!!!
4) sample15.jpg   Completed ...!!!
5) sample18.jpg   Completed ...!!!
6) sample2.jpg   Completed ...!!!
7) sample20.jpg   Completed ...!!!
8) sample25.jpg   Completed ...!!!
10) sample5.jpg   Completed ...!!!
10) sample5.jpg   Completed ...!!!
```



Number Of Hidden Image Files is : 4

The encrypted image thus obtained was steganographically concealed in the carrier image. The compression ratio and detection ratio of stego content is also analyzed. By analyzing the images in the sampled database the probability of occurrences of images with stego content in the corporate mails is zero.

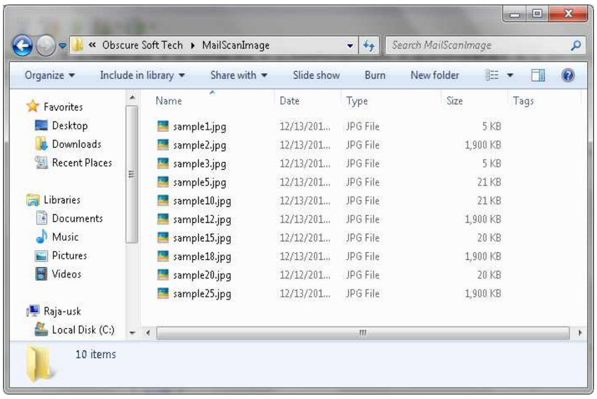
Hidden Image Files :



Name	Date	Type	Size	Tags
sample2.jpg	12/13/201...	JPG File	1,900 KB	
sample12.jpg	12/13/201...	JPG File	1,900 KB	
sample18.jpg	12/13/201...	JPG File	1,900 KB	
sample25.jpg	12/13/201...	JPG File	1,900 KB	

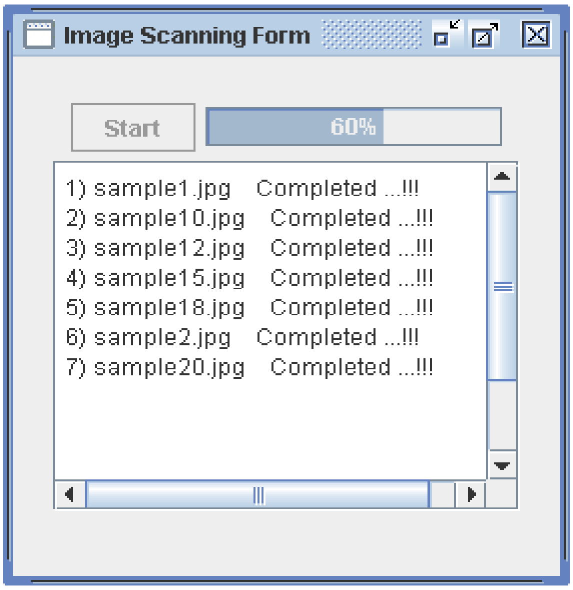
4 items

Scanning Mail Reports



Name	Date	Type	Size	Tags
sample1.jpg	12/13/201...	JPG File	5 KB	
sample2.jpg	12/13/201...	JPG File	1,900 KB	
sample3.jpg	12/13/201...	JPG File	5 KB	
sample5.jpg	12/13/201...	JPG File	21 KB	
sample10.jpg	12/13/201...	JPG File	21 KB	
sample12.jpg	12/13/201...	JPG File	1,900 KB	
sample15.jpg	12/12/201...	JPG File	20 KB	
sample18.jpg	12/13/201...	JPG File	1,900 KB	
sample20.jpg	12/12/201...	JPG File	20 KB	
sample25.jpg	12/13/201...	JPG File	1,900 KB	

10 items



```
1) sample1.jpg   Completed ...!!!
2) sample10.jpg   Completed ...!!!
3) sample12.jpg   Completed ...!!!
4) sample15.jpg   Completed ...!!!
5) sample18.jpg   Completed ...!!!
6) sample2.jpg   Completed ...!!!
7) sample20.jpg   Completed ...!!!
```

8. Discussion

In this paper, we have analyzed the steganalysis algorithms available for Image Steganography. The proposed mathematical web search model admits a wide variety of resource constraints. Depending on the application, implementation, hardware, and steganalysis probability of error constraints, a suitable resource model can be used to derive an optimal web search strategy using the proposed technique. Depending on the reliability of the steganalysis algorithms employed and the storage constraint one of two strategies, namely, coordinated search or random search can be chosen. It is seen that for a certain range of steganalysis reliability, both these methods give comparable performance.

9. Conclusion

In summary, each carrier media has its own special attributes and reacts differently when a message is embedded in it. Therefore, the steganalysis algorithms have also been developed in a manner specific to the target stego file and the algorithms developed for one cover media are generally not effective for a different media. This paper we conclude that it is possible to design efficient web search algorithms to detect covert messages in corporate emails.

References

[1] Ahmed Ibrahim, "Steganalysis in Computer Forensics", Security Research Centre Conferences, Australian Digital Forensics Conference, Edith Cowan University, 2007.

[2] Avcibas, I. Memon, N. and Sankur, B., "Steganalysis using image quality metrics," IEEE Trans. on Image Processing, vol. 12, no. 2, pp. 221–229, 2003.

[3] Chandramouli, R., "A Mathematical Approach to Steganalysis", Proc. SPIE Security and Watermarking of Multimedia Contents IV, California, 2002.

[4] Geetha ,S., Siva, S. and Sivatha Sindhu, "Detection of Stego Anomalies in Images Exploiting the Content Independent Statistical Footprints of the Steganograms", Department of Information Technology, Thiagarajar College of Engineering, Madurai, , Informatica(25–40), 2009.

[5] Greg Goth, "Steganalysis Gets Past the Hype", IEEE, Distributed Systems Online 1541-4922, Published by the IEEE Computer Society Vol. 6, No. 4, 2005.

[6] Sujay Narayana and Gaurav Prasad, "Two new approaches for secured image Steganography using cryptographic Techniques and type conversions", Department of Electronics and Communication, NITK, Surathkal, INDIA, 2010.

[7] Liu Shaohui, Yao Hongxun, and Gao Wen, "Neural network based steganalysis in still images", Department of Computer Science, Harbin Institute of Technology, ICME, 2003.

[8] Niels Provos, Peter Honeyman, "Hide and Seek: Introduction to Steganography", University of Michigan, Published by the IEEE Computer Society, 2003.

[9] Niels Provos and Honeyman P, "Detecting steganographic content on the internet", Retrieved from http://www.citi.umich.edu/u/provos/papers/detecting.pdf 2007.

[10] Samir K Bandyopadhyay, and Debnath Bhattacharyya, "A Tutorial Review on Steganography", University of Calcutta, Senate House, 87 /1 College Street, Kolkata, UFL & JIITU, 2008.