Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 2; January-March, 2015 pp. 121-126

http://www.krishisanskriti.org/acsit.html

# Analysis and Development of Information Hiding Techniques using Steganography and Cryptography

Saeed Anwar Jamal Ansari[1] and Ms. Manisha Dawra[2]

*[1]Student M.Tech [CSE] Department of Computer Science &Engineering*
*Al-Falah School of Engineering and TechnologyDhauj, Faridabad, Haryana*
*[2]CSE Dept. Al-Falah School of Engineering and Technology Dhauj, Faridabad, Haryana*
*E-mail: [1]saeedlko@gmail.com*

## 1. INTRODUCTION

Steganography is the practice of hiding private or sensitive information within something that appears to be nothing out to the usual.

Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information.

The difference between two is that steganography involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information.

The most common use of steganography is to hide a file inside another file.

### History of Steganography

Throughout history Steganography has been used to secretly communicate information between people.

Some examples of use of Steganography is past times are:

1. During World War 2 invisible ink was used to write information on pieces of paper so that the paper appeared to the average person as just being blank pieces of paper. Liquids such as milk, vinegar and fruit juices were used, because when each one of these substances is heated they darken and become visible to the human eye.
2. In Ancient Greece they used to select messengers and shave their head, they would then write a message on their head. Once the message

After the hair grew back the messenger was sent to deliver the message, the recipient would shave off the messengers hair to see the secrete message.

### Detecting Steganography

The art of detecting Steganography is referred to as **Stegoanalysis t**o put is simply Stegoanalysis involves detecting the use of Steganography inside of a file. Stegoanalysis does not deal with trying to Decrypt the hidden information inside of a file, just discovering it.

There are many methods that can be used to detect Steganography such as:

"Viewing the file and comparing it to another copy of the file found on the Internet (Picture file). There are usually multiple copies of images on the internet, so you may want to look for several of them and try and compare the suspect file to them. For example if you download a JPED and your suspect file is also a JPED and the two files look almost identical apart from the fact that one is larger than the other, it is most probable you suspect file has hidden information inside of it.[8]

### Goal of Steganography

The goal of steganography is covert communication. So, a fundamental requirement of this steganography system is that the hider message carried by stego-media should not be sensible to human beings.

This approach of information hiding technique has recently become important in a number of application areas.

This project has following objectives:

- To product security tool based on steganography techniques.

- To explore techniques of hiding data using encryption module of this project
- To extract techniques of getting secret data using decryption module.

## 2. STEGANOGRAPHY VS. CRYPTOGRAPHY

Basically, the purpose of cryptography and steganography is to provide secret communication. However, steganography is not the same as cryptography. Cryptography hides the contents of a secrete message from a malicious people, whereas steganography even conceal the existence of the message. In cryptography, the system is broken when the attacker can read the secret message. Breaking a steganography system need the attacker to detect that steganography has been used.

It is possible to combine the techniques by encrypting message using cryptography and then hiding the encrypted message using steganography. The resulting stego-image can be transmitted without revealing that secret information is being exchanged. [6]

### 2.1. Cryptography

There are many aspects to security and many applications. One essential aspect for secure communications is that of cryptography. But it is important to note that while cryptography is necessary for secure communications, it is not by itself sufficient. There are some specific security requirements for cryptography, including Authentication, Privacy/confidentiality, and Integrity Non-repudiation. The three types of algorithms are described: [6]

(i) Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption
(ii)Public Key Cryptography (PKC): Uses one key for encryption and another for decryption
(iii)Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information.

### 2.2. Steganography

Steganography is the other technique for secured communication. It encompasses methods of transmitting secret messages through innocuous cover carriers in such a manner that the very existence of the embedded messages is undetectable. Information can be hidden in images, audio, video, text, or some other digitally representative code. Steganography systems can be grouped by the type of covers used (graphics, sound, text, executables) or by the techniques used to modify the covers

a) Substitution system.

b) Transform domain techniques

c) Spread spectrum techniques

d) Statistical method

e) Distortion techniques

f) Cover generation methods

### 2.3. AES algorithm for Cryptography

This standard specifies the Rijndael algorithm a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. The input, the output and the cipher key for Rijndael are each bit sequences containing 128, 192 or 256 bits with the constraint that the input and output sequences have the same length. In general the length of the input and output sequences can be any of the three allowed values but for the Advanced Encryption Standard (AES) the only length allowed is 128. [5]

### 2.3. Advantages of using AES Algorithm

1. Very Secure.

2. Reasonable Cost.

3. Main Characteristics:

I. Flexibility, II. Simplicity [5]

### 2.4. Crypto Module:

For Crypto Module the following steps are considered for encrypting the data. [6]

- Insert text for encryption.
- Apply AES algorithm using 128 bit key (Key 1).
- Generate Cipher Text in hexadecimal form.

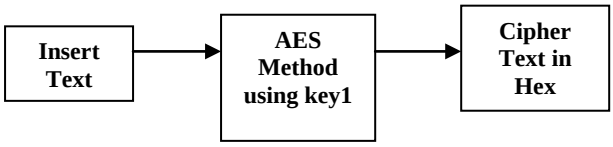



Fig. 1: Crypto-Module

### 2.5. Security Module

This is an intermediate module which provides an extra security features to our newly developed system. This module is used to modify the cipher text and to generate two extra keys. In the reverse process it regenerates the original cipher text (Refer Figure2) .Before the hiding process this module works as follows:

Separate the alphabets and digits from the cipher text.

Keep track of the original position of the alphabet and the digits in the form of a secret key (Key 3). [6]

Separate first seven alphabets retrieved from first step and add the remaining alphabets at the end of the separated digits as in the first step. This generates the second key (Key 4).

### 2.6. Steganography vs. Watermarking

Steganography pay attention to the degree of Invisibility while watermarking pay most of its attribute to the robustness of the

message and its ability to withstand attacks of removal, such as image operations(rotation, cropping, filtering), audio operations(rerecording, filtering)in the case of images and audio files being watermarked respectively.

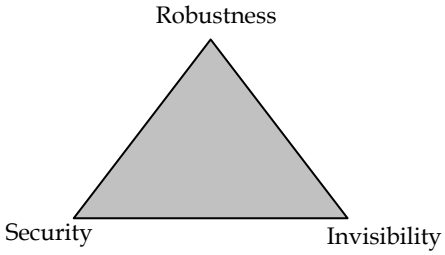



Fig. 2 [A typical triangle process]

That is the way the algorithm changes the vessel and the severity of such an operation determines with no doubt the delectability of the message, since delectability is a function of file characteristics deviation from the norm, embedding operation attitude and change severity of such change decides vessel file delectability. A typical triangle of conflict is message Invisibility, Robustness, and Security. Invisibility is a measure of the in notability of the contents of the message within the vessel.

**2.7. Security**

Is sinominous to the cryptographic idea to message security, meaning inability of reconstruction of the message without the proper secret key material shared.

**2.8. Robustness**

Refers to the endurance capability of the message to survive distortion or removal attacks intact. It is often used in the watermarking field since watermarking seeks the persistence of the watermark over attacks, steganographic messages on the other hand tend to be of high sensitivity to such attacks. The more invisible the message is the less secure it is (cryptography needs space) and the less robust it is (no error checking/recovery introduced).The more robust the message is embedded the more size it requires and the more visible it is. [8]

2.9. ADVANTAGES:

- Less computational time
- Highly secure.

## 3. VARIOUS TYPES OF IMAGE STEGANOGRAPHY

Image steganography techniques can be divided into two groups: those in the Image Domain and those in the Transform Domain. Image - also known as spatial - domain techniques embed messages in the intensity of the pixels directly, while for transform also known as frequency - domain, images are first transformed and then the message is embedded in the image .Image domain techniques encompass bitwise methods that apply bit insertion and noise manipulation and are sometimes characterized as "simple systems". The image formats that are most suitable for image domain steganography are lossless and the techniques are typically dependent on the image format. [3]

### 3.1.1. Hash-based Approach for Color Image Steganography

The hash algorithm randomly generates a hash-key that is afterwards used by the algorithm to generate a pattern of pixels, where the data will be stored the data is coded on a new pattern that makes the coding of data very efficient. For decoding textual data in the image, the hash key is used that was generated to during coding by using the hash-key the used algorithm generates the exactly same pattern that was used at the time of coding. The most important part of the proposed algorithm is the perfect hashing as hash-function (H) algorithm. A function for perfect hashing is defined for set N to map distinct elements in N to distinct integers, without any collisions. A perfect hash function supports efficient lookups by placing hash-keys from N to a hash-table.

There are number of advantages of using perfect hashing over other hashing techniques. Perfect hashing is faster than other techniques. It can also handle large datasets effectively. [3]

### 3.2.2. Blind Detection Method for Additive Noise Steganography

Based on the intrinsic statistical attributes of discrete cosine transform (DCT) ac coefficients in IPEG pre-compressed images and the effects of data embedding on the statistical distribution of ac coefficients, we propose a novel blind steganalyzer for additive noise steganography in JPEG decompressed images as shown

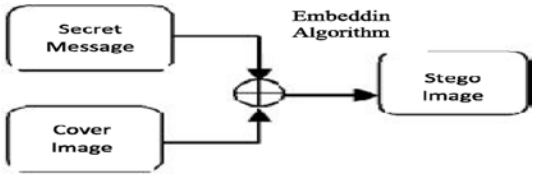



Fig. 3: Additive Noise Steganography Model

The proposed method is less sensitive to image contents and sources. Its detection reliability is quite high even for a very low embedding rate such as 0.01 bpp. In fact any steganographic algorithms in a IPEG pre-compressed image will destroy the intrinsic character of decompressed images. Consequently, the above method is also effective for those steganographic algorithms being not suitable for additive noise model, which would be regarded as one of the future research directions. [3]

## 4. BACK GROUND ON INFORMATION HIDING IN JPEG

A natural way for embedding a message (also called payload) into a media host without inducing any perceptual distortion is to modify the least significant bit of the media samples. This technique is called least significant bit or LSB embedding. In JPEG, the secret data is embedded into the LSB of the rounding quantized DCT coefficients whose values are not -1, 0 or 1. The constraints on the value of coefficients allow avoiding possible ambiguity in the secret data extracting process.

Another class of data embedding, called quantization index modulation (QIM) is proposed by Chen and Wornell. The data is hidden by basing the choice of a quantize on the message to be hidden. A bit b ∈ {0, 1} is embedded in one coefficient x such that

y = $^{Q}$b (x) where $^{Q}$1 and $^{Q}$0 are two different quantizes. Data embedding is applied with quantizing C (i, j) by using quantizer Qb chosen between $^{Q}$0 (C (i, j)) and $^{Q}$1 (C (i, j)). For more details about QIM, readers are invited to read .Based on QIM embedding, Proposed SEC (selectively embedding coefficient) algorithm for data hiding. SEC uses DCT coefficient level to embed data. The data embedding is performed by choosing a QIM scalar quantize. [1]

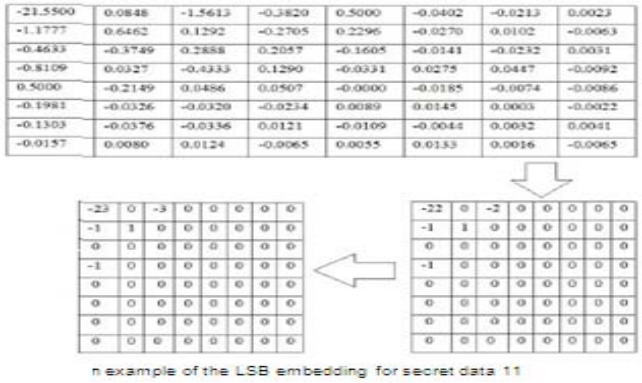



Fig. 4: [LSB embedding for secret data]

### 4.1. Embedding process:

Embedding process is performed within the receiving blocks in zigzag way in order to preserve the JPEG quality. We have to mention that embedding is performed with respect to a given threshold T. If T increases, fewer coefficients are used for embedding, and hence the payload size will decrease. Our steganography technique integrates embedding and rounding which are involved in increasing compression, such that if T = 0 portion of embedding is maximum (with increasing file size), and if T = 1 portion of rounding is maximum (while embedding is high without increasing file size). We highlight that our embedding process is inspired with the following difference. [1]

When _

$T-1 \le Ci\,(i;j) < T$ (knowing the fact that T ≥ 1), an ambiguity during data extraction will appear.

For example, if T = 2 and Ci (i, j) = $\overline{2.4}$, the

$^{Q}$0 (Ci (i, j)) = 2. In this situation we cannot decide whether there is hidden data or not. As a solution, the coefficients between T and T − 0.5 are rounded to T − 1. [3]

### 4.2. Stego-JPEG encoder

Input: Quantized coefficients of block *Bi* from an image I of *N* ×*M* pixels,

Where $i \in [1;\,(N \times M) = (8 \times 8)]$.Output: A compressed Stego-JPEG image. The following steps of the embedding process are executed:

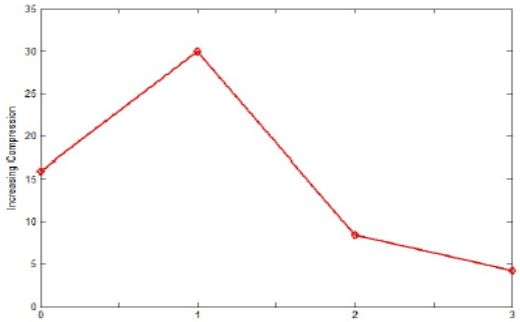
1) Apply Rounding step to block *Bk*.
2) Compress $^{B}k$ using lossy JPEG.
3) Hide the current bits of compressed block $^{B}k$ in the *n* coefficients of the subsequent blocks $^{B}k$+1*; :::;*$^{B}l$ where *n* = $^{n}k$+1 +$^{n}k$+2 +*:::*+$^{n}l$, $^{n}i$ being the number of coefficients used in the $i^{th}$ block such that:

$$C_i(i,j) = \begin{cases} Q_b(\bar{C}_i(i,j)) & |\bar{C}_i(i,j)| \ge T \\ \lfloor \bar{C}_i(i,j) \rfloor & T-1 \le |\bar{C}_i(i,j)| < T \\ \lfloor \bar{C}_i(i,j) + 0.5 \rfloor & \text{Otherwise} \end{cases} \quad (1)$$

While $k \le \lfloor N \times M = m \times m \rfloor$, $k = l + 1$, repeat 1-3.

### 4.3. Extraction process

The way to extract the embedded blocks from a compressed image is the same as that one used for embedding process. First, the JPEG decoding procedure for decompression is performed. Then, the embedded blocks are extracted by checking odd and even $^{C}$i(i; j) coefficients from n coefficients of sequential blocks. It should be noted that the decoder disregards all coefficients that quantize to a value with magnitude T or smaller. Finally, inverse DCT is used for extracted blocks and original blocks.



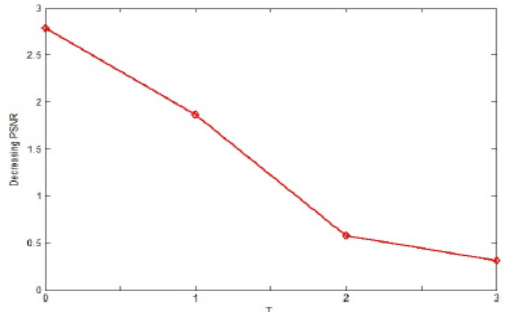



Fig. 5: Average compression ratio and decrease of PSNR

Average compression ratio and decrease of PSNR when T=0, 1, 2, 3 for Lena, Pepper, Baboon and House A) Average compression ratio B) decrease of PSNR.[1]

### 4.4. Stego-JPEG decoder:

Input: A compressed Stego-JPEG image.

Output: A decompressed image *I*.

The following steps of the embedding process are executed:

1) Decompress blocks by lossy JPEG decoding.
2) Extract the embedded block of $Bk+1;:::; {}^{B}l$ coefficients $Ci\ \ (i;\ j)| \geq T$ from the subsequent blocks such that:

$$Embeddedbit = \begin{cases} 1 & C_i(i,j) = odd \\ 0 & C_i(i,j) = even \end{cases}$$

3) Apply lossy JPEG decoding for embedded block.
4) While $l \leq [N \times M\, m \times m]$, $l = l + 1$,
repeat 1-3.

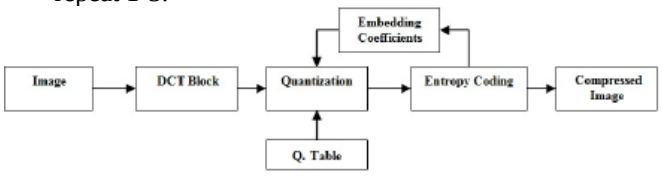



Fig. 6: Block Diagram of embedding

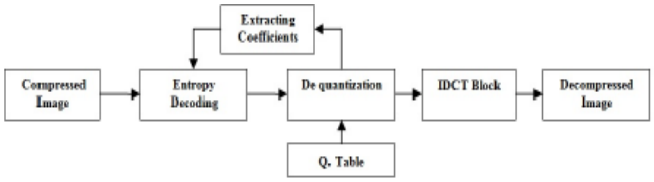



Fig. 7: Block Diagram of extraction

Table -1.0

| | Inc. Compression | | Dec. PSNR | |
|---|---|---|---|---|
| | $\mu$ | $\sigma^2$ | $\mu$ | $\sigma^2$ |
| QF=25 | 31.71 | 0.17 | 1.54 | 0.14 |
| QF=50 | 30.57 | 0.13 | 1.63 | 0.18 |
| QF=75 | 29.12 | 0.16 | 2.04 | 0.47 |

AVERAGE COMPRESSION RATIO AND DECREASE OF PSNR FOR 315 IMAGES [1]

### 4.5. Least significant bit (LSB):

Insertion is a simple approach to embedding information in image file. The simplest steganography techniques embed the bits of the message directly into least significant bit plane of the cover-image in a deterministic sequence. Modulating the least significant bit does not result in human perceptible difference because the amplitude of the change is small. In this technique, the embedding capacity can be increased by using two or more least significant bits. At the same time, not only the risk of making the embedded message statistically detectable increase but also the image fidelity degrades.

Although LSB hides the message in such way that the humans do not perceive it, it is still possible for the opponent to retrieve the message due to the simplicity of the technique. Therefore, malicious people can easily try to extract the message from the beginning of the image if they are suspicious that there exists secret information that was embedded in the image.

### 4.6. Advantage of LSB technique

- It is simple to implement. This is especially true in the 24-bit bitmap case.
- It also allows for a relatively high payload, carrying one bit of the secret message per byte of pixel data.
- It is also seemingly undetectable by the average human if done right.

## 5. ENCRYPTION-DECRYPTION PROCESS

Encryption is a well known procedure for securing data transmission or storage. Many encryption methods have been developed throughout the years, such as: DES (Data Encryption Standard), AES (Advanced Encryption Standard) and RSA. Many information security algorithms have been developed combining both encryption and steganography algorithms to enhance information security. So that if an attacker succeeds in detecting and extracting the secret, he/she will find it encrypted. If the encryption algorithm is known, then using brute-force attack to decrypt the secret has a complexity of O ($2^N$), where N is the length of the encryption key. In t is work, we develop a new secure steganography algorithm that utilizes the concept of permutation. Permutation is defined as the act of changing the arrangement of a given number of elements, and it is widely-used as part of many encryption algorithms, such as DES, AES, RSA. [7]

### 5.1. Limitation of encryption

Cryptanalysis, or the process of attempting to read the encrypted message without the key, is very much easier with modern computers than it has ever been before. Encryption

does not make your data secure. Not using encryption, however, means that any data in transit is as easy to read as the contents of a postcard, sent in regular mail. Encryption at least ensures that anyone who does read your messages has worked hard at it. [8]

### 5.2. Decryption Process

Decryption is generally the reverse process of encryption. It is the process of decoding the data which has been encrypted into a secret format. An authorized user can only decrypt data because decryption requires a secret key or password.[7]

Decryption definition Decryption is the process of decoding encrypted information so that is can be accessed again by authorized users.

### Encryption - Decryption Cycle:


**Fig.** 8: Encryption-decryption Cycle

To make the data confidential, data (plain text) is encrypted using a particular algorithm and a secret key. After encryption process, plain text gets converted into cipher text. To decrypt the cipher text, similar algorithm is used and at the end the original data is obtained again. [8]

## 6. CONCLUSION

Steganography can be used for hidden communication. We have explored the limits of steganography theory and practice. A stego-key has been applied to the system during embedment of the message into the cover image.

The recent explosion of research in watermarking to protect intellectual property is evidence that steganography is not just limited to military or espionage applications. Steganography, like cryptography, will play an increasing role in the future of secure communication in the “digital world”. Future work to provide more secure data to use the OTP (One Time Password) on data file.

## REFERENCES

[1] Jafari, R.; Ziou, D. Mammeri "Increasing compression of JPEG images using Steganography”A.Robotic and Sensors Environments (ROSE), 2011 IEEE International Symposium on DOI: 10.1109/ROSE .2011.6058519 Publication Year: 2011

[2] LiTong "A New Algorithm for Information Hiding in Digital Image". Computer Science and Information Processing (CSIP), 2012 International Conference on DOI: 10.1109/CSIP.2012.6308818 Publication Year: 2012.

[3] Ashwin, S., Ramesh, J., Kumar, S.A., Gunavathi, K."Novel and Secure Encoding and Hiding Techniques using Image Steganography: A Survey". Emerging Trends in Electrical Engineering and Energy Management (ICETEEEM), 2012 International Conference on DOI: 10.1109/ICETEEEM.2012.6494463 Publication Year: 2012.

[4] Paul, R.; Acharya, A.K.; Yadav, V.K.; Batham, S. “Hiding Large Amount of Data using a New Approach of Video Steganography". Confluence 2013: The Next Generation Information Technology Summit (4th International Conference) DOI: 10.1049/cp.2013.2338 Publication Year: 2013.

[5] C.E., Shannon, (1949), Communication theory of secrecy systems, Bell System Technical Journal, 28, 656-715.

[6] Dipti Kapoor Sarmah, Neha Bajpai “Proposed System for data hiding using Cryptography and Steganography”.International journal of Computer Application. 2010.

[7] http://www.google.com
http://www.microsoft.com
http://www.asp.net
http://www.wikipedia.org

### Books

Following books and eBooks are used to complete this project reports.
Visual Cryptography and Secret Image Sharing (Digital Imaging and Computer Vision) by Stelvio Cimato (Editor), Ching-Nung Yang (Editor)
SQL Server Bible (Paperback)
.NET Black Book (Paperback)