ISSN XXXX XXXX © 2018 IJESC

Research Article Volume 8 Issue No.5

Improved Steganography and Steganalysis using Image Processing Technique

Mishmala Sushith[1], A. Keerthana[2]
Associate Professor[1], ME Student[2]
Department of CSE
KIT- Kalaignarkarunanidhi Institute of Technology, Coimbatore, Tamilnadu, India

Abstract:
Information security and secret sharing plays an important role. Image processing is an effective way to achieve high security. The paper proposes two steganography techniques and one steganalysis technique in a hybrid way. The first steganography technique is based on Hybrid technique, which combines integer wavelet transform (IWT) and singular value decomposition (SVD) to hide the images. This method is quite robust to different attacks such as compression, cropping, impulse noise, Gaussian noise and Gamma correction attacks. The second steganography technique is based on embedding the secret message in edge regions of the images. Powerful steganalysis methods fail to estimate the length of hidden message from the stego-images. The proposed steganalysis technique is based on improved non-causal linear predictor, which estimates the embedded message by using linear prediction coefficients obtained from a block of pixels from stego-images that are created by steganography technique. The proposed techniques are tested on different types of images and stego-images. It is found that these new developments in steganography and steganalysis techniques have impressive overall performance comparable to or even better than the performance of some of the best methods.

Keywords: Information security, steganography, steganalysis, stego-images, Hybrid technique.

I. INTRODUCTION

Information security requires high alert as illegal hacking increases. The growing possibility of modern Communications through internet requires a special type of security on computer networks. The Security is comes into exist when its need or desire to guard the message broadcast from a hacker who might present a threat to secrecy of data, genuineness, data integrity and so on. The secrecy and data integrity is maintained to protect against illegal access and use. The requirement of information security has undergone two major changes in the last few decades, namely computer security and network security. The fast growth of the electronic era has led to all documentations, image and video being digitized. This has increased the requirement for ensuring the safety and reliability of any document, image and video to maintain privacy, and to prevent piracy and mass reproduction. This requirement varies from an individual to individual. The techniques used for ensuring this are cryptography and steganography of which the former is perceptible as noise while the latter is imperceptible to the human eye.

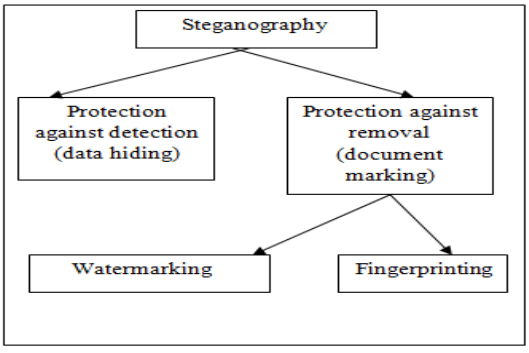

Figure.1. Information hiding techniques

The research developed a hybrid technique for effective data hiding and hidden data analysis. This process is known as steganography and steganalysis. Steganography is a method that hides data among the bits of a cover file like a graphic or an image file. Authors in [1] illustrated the concept of steganography with an example called the "Prisoners' Problem." In this example, the two users communicate with shared secret key.

This secures the communication between the two persons. This process is depicted for the importance of steganography. The communication initiator sends the message using a key; the receiver can receive and extract the content using the shared secret key, which is pre-distributed by the sender earlier. This might be done by steganography. Recent usage of steganography has some special inks for hidden messages on currencies, some form of steganography used watermarking [2] techniques and few used fingerprinting for copyright protection. Information hiding is disseminated in Figure 1.0.

STEGANOGRAPHY TECHNIQUES

Steganography provides a way to communicate secretly as long as an attacker doesn't find a way to detect the message [3]. The most suitable types of files for steganography transmission being, media files due to their large size. The host files concealing other files are usually called carriers. The carrier files are functional files and does not raise a question or arouse suspicion. This section lists a number of hiding techniques [4] that are being used presently. The secret information can be image, video, image, text etc. The image steganography is segmented into two steps such as Embedding and extraction shown in figure 1.1.

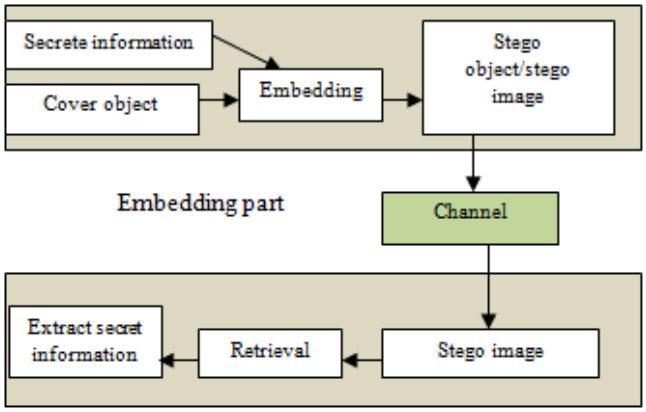

Figure.2. Process involved in information hiding

Data can be embedded within a file by taking advantage of human perception. The prime objective of this research is to identify new techniques for steganography and steganalysis. Creating the strong steganography techniques and effective steganalysis for information verification is the major objective of the proposed research. This research work also aspires, To develop security algorithms for secured data communication using steganography, to meet Confidentiality, Integrity, Authentication and Non-repudiation requirements, to implement new techniques of best possible pure and secret key steganography, To implement an effective stego system with maximum payload, good imperceptibility, minimum key length with more complexity against hackers through Random scan, Cryptography, Compression and Pixel Indicator Methodologies., To analyze the image with the size of hidden data using effective steganalysis method, To develop a security tool based on steganography techniques and explore techniques of hiding data using steganography and to develop and authenticate a new approach to provide performance enhancements over the steganography methods proposed in the existing.

OVERALL DESCRIPTION ABOUT EXISTING AND PROPOSED SYSTEM

In the existing system, many approaches were used content-adaptive spatial image steganography. This kind of techniques is minimizing the heuristically defined embedding distortion functions, which are created with statistical delectability. The secret bits are embedded into the noisy and textured areas. And many used LSB based techniques to perform the steganography. There are numerous studies performed the stenography and steganalysis process. However, the techniques are insecure and sometimes loss the optimality in different parameters. And there is another issue that the image quality. In the proposed system, a new hybrid steganography based approach is used to effectively embed, extract and secret messages. In the earlier work, the steganalysis also performed, but the size of secret messages is not able to detect. The proposed system effectively performs steganography and steganalysis without compromising the quality related results.

II. LITERATURE REVIEW

The recent steganography schemes are described in this section, the existing techniques such as LSB, IP, Pixel Value Differencing (PVD) and Pixel Indicator (PI) methods.

A. Least Significant Bit Data Embedding Scheme

The primary reasons for the LSB Substitution method to be popular are, this is very ease of computation is very high because of its straight forward implementation. Large amount of information or payload can be hidden in the cover image without distorting it. Human eye is sensitive only to the changes in the smooth areas of an image So the alterations are made in the less sensitive edge areas of the image [7]. Since it is a well known method, the message embedded using this method is vulnerable. And the number of bits to be embedded in each pixel is same. Hence the decoding of the embedded image is very easy and security of the message is low. Visual degradation is possible if more number of message bits are embedded in the edge areas of the image, hence for fully embedded image visual degradation will be high. This method is not robust. i.e., when subjected to image processing, it will lose the confidential information.

B. Optimum Pixel Adjustment Procedure (OPAP)

OPAP reduces the distortion caused by the LSB substitution method. The pixel value is adjusted after the embedding of the secret information is done, to get better quality of the stego image without disturbing the data embedded [8]. This is very Simple methodology and Easy to retrieve.

C. Inverted Pattern Approach (IP)

This IP LSB substitution approach uses pre processing of the secret information. In this method for each section of secret images it is determined whether it is to be inverted or not before it is embedded. In addition, the bits which are used to record the transformation are treated as secret keys or additional bits to be re-embedded [9]

D. Pixel Value Differencing (PVD) methods

The number of insertion bits is dependent on whether the pixel is in an edge area or smooth area. In edge area, the difference between the adjacent pixels is more, whereas in the smooth area it is less as human perception is less sensitive to subtle changes in edge areas of a pixel [10].

E. Pixel Indicator (PI) Method

One channel is fixed as an indicator and the specified amount of bits by user (say k bits) are then embedded in the other two channels depending upon the last two bits of the indicator channel [11].

F. Grey Level Modification

In this method, actually no information is to be hidden. Mathematical relationship is developed for finding the relevance between original cover image and secret information to be hidden. Advantage of this method is high PSNR with less computational complexity [12]

III.PROPOSED SYSTEM

Due to growing demand for privacy and security, a need for a variety of data hiding methods which lead to the progress of several methods for embedding and retrieval. The security is also an important issue to prevent extraction of hidden image or information by any third party. The Steganography is a powerful method of embedding secret data for covert communication. The image based steganography has become an important discipline in signal processing, image processing and security systems. All of the existing techniques of steganography focus on the embedding policy and given more attention towards encryption, which depend on the usual encryption techniques. These

techniques are not tailored to steganography applications where robustness, flexibility and security are required. The development of steganography techniques based on both spatial and transform domain techniques are focused towards high capacity and security. The thesis proposes two steganography techniques and one steganalysis technique. The first steganography technique is based on Hybrid technique, which combines **integer wavelet transform** (IWT) and singular value decomposition (SVD) to hide the images. This method is quite robust to different attacks such as compression, cropping, impulse noise, Gaussian noise and Gamma correction attacks. The second steganography technique is based on embedding the secret message in edge regions of the images. Powerful steganalysis methods fail to estimate the length of hidden message from the stego-images. The proposed steganalysis technique is based on improved non-causal linear predictor, which estimates the embedded message by using linear prediction coefficients obtained from a block of pixels from stego-images that are created by steganography technique. The proposed techniques are tested on different types of images and stego-images. It is found that these new developments in steganography and steganalysis techniques have impressive overall performance comparable to or even better than the performance of some of the best methods.

ADVANTAGES

- The hybrid steganography technique improves the perceptual quality of Stego images.
- It also performs the steganalysis process, where the length of hidden message from the stego-images can be detected easily.

In these types of attacks with a help of a system or through check with a naked eye it disclose the presence of concealed information, which helps to divide the image into bit planes for further analysis.

Steganalysis

The proposed system also performs the steganalysis additionally, which has been performed using non-causal linear predictor. This has the capability to detect the secret message size and the presence on the cover image. This can be performed with the desired key. The technique performs the least noise pixels and analysis its originality to detect the secret message.

Quantization Processes

The quantization processes determine the strength of the secret message signal embedded in the wavelet coefficient. The wavelet coefficient in the middle process such as *fk2, l (m, n)* must be quantized to embed to secret message, the value range between *fk1, l (m, n), fk3,l (m, n)* bins is divided into the width that using the following equation:

$$\Delta = \frac{fk3,l(m,n) - fk1,l(m,n)}{2Q-1} \qquad \textbf{(1.1)}$$

Where Q is the user-defined variable and *fk2, l (m, n)* is quantized to the nearest value. To enhance the embedding strength of the secret message and an attacker doesn't determine the key and secret message where the HSA kept secret and quantization is unknown. The experimental result shows the performance and the efficiency of the proposed method, where the executive tests have taken place. The implementation performed on a various images with different variable parameter size and embedded the secret message. The HAS is implemented in JPEG images. They were resized to different sizes such as 256×256 from the center of the original images. It could measure the relative complexity of the algorithm in the form of the amount of data to be embedded, and how secured the secret information should be, and how robust the algorithm. Considering the differences between the original and hidden data are slightly smaller to the human being perception. Therefore, the differences might be mathematical or perceptual that should be obvious from the context, whether the results of authentication of image processing techniques are required for both quantitative performance measures and visual inspection.

Here the proposed system deals with various experimental evaluation methods and their results Original and stego of image data such as quality measures. It covers the experiments based on Least significant Bit (LSB), Discrete cosine transform (DCT) [6], and Discrete wavelet transform (DWT) techniques, which is implemented on Various standard images to determine the differences between the original and hidden data.

Evaluation of Image Quality Measurement

In the objective measures of the Image Quality is to calculate the difference between the original and the stego image by a predefined function. These measures are widely used in the literature. The approach image quality would be given to calculate the mean values and variances of some small regions in the image, and then compare them between the original and the hidden data image. There are many objective quality measuring methods which have been developed for image quality evaluation in the literatures. They are based on numerical measures of image quality and computable distortion measures. The quantitative of Image Quality measurement of images is commonly measured by The Mean Square Error (MSE), Peak Signal to noise ratio (PSNR), Normalized correlation (NC), and Normalized Cross–correlation. The MSE, PSNR and NC are most commonly used Objective quality measures for image quality evaluation. Because they are simple to calculate, have clear physical meanings and are mathematically convenient in the context of optimization.

The Mean Square Error (MSE) is one of the most commonly used performance measures represents the cumulative squared error between the embedded and the original image. For an image of size N x M, it can be defined as

$$MSE = \frac{1}{MN}\sum M_{j=1}\sum N_{k=1}(xj,k - x'j,k)2 \quad (1.2)$$

Where x (n, m), x' (n, m) are original and embedded image respectively.

Peak Signal to noise ratio (PSNR)

$$PSNR = 10log\frac{(2^n-1)^2}{MSE} = 10log\frac{255^2}{MSE} \quad (1.3)$$

It represents the cumulative squared error between the embedded and the original image. However, the PSNR alone cannot judge the quality of an image and hence, the other quality metrics are also evaluated for the other techniques.

Normalized Cross –correlation (NC)

$$NC = \sum_{j=1}^{M}\sum_{k=1}^{N} x_{j,k} \cdot x'_{j,k} \quad (1.4)$$

The combination of text and image for the purpose of hiding the information, in order to provide more security and to minimize the distortion of the stego image, novel technique using the hybrid of text and image is presented in this section. The main proposed combinational of text and image steganography possesses the following advantages.

Universal Image Quality Index (UIQI):

This quality index models any distortion as a combination of three different factors: loss of correlation, luminance distortion, and contrast distortion. It is given by

$$Q = \frac{4\times\sigma_{xy}\times\bar{x}\times\bar{y}}{(\sigma_x{}^2+\sigma_y{}^2)\times(\bar{x}^2+\bar{y}^2)} \quad (1.5)$$

The first component Q1 is the correlation coefficient between x and y, which measures the degree of linear correlation between x and y. The second component Q2 measures how much the x and y are close in luminance. The third component Q3 measures the similarities between the contrasts of the images.

Structural Similarity Index Metric (SSIM):

The SSIM is an objective image quality metric and superior to traditional measures such as MSE and PSNR. The PSNR estimates the perceived errors, whereas the SSIM considers image degradation as a perceived change in the structural information. The structural information is the idea that the pixels have strong inter-dependencies especially when they are spatially close. These dependencies take important information about the structure of the objects from the image. Similar to UIQI, the SSIM also has three components corresponding to luminance, contrast, and structural (or correlation) distortions.
The SSIM is given by

$$SSIM = \frac{(2\times\bar{x}\times\bar{y}+C1)(2\times\sigma_{xy}+C2)}{(\sigma_x{}^2+\sigma_y{}^2+C2)\times(\bar{x}^2+\bar{y}^2+C1)} \quad \textbf{(1.6)}$$

where C1 = (k1L)2, and C2 = (k2L)2 are the two constants used to avoid null denominator. L is the dynamic range of the pixel values (typically this is 2number of bits per pixel -1). By default, k1 = 0.01 and k2 = 0.03.

IV. IMPLEMENTATION AND RESULTS

To prove the effect of proposed system, the experiments used MATLAB tool. The experiments are performed on an Intel Dual Core with a RAM capacity 2GB. The algorithms are implemented in Matlab Tool are run under Windows 7. The technique is tested with four cover images:

Lena, Baboon, Peppers, and Nature with size 256 x 256. These are the standard color images used in most of the color image steganography techniques. Customized secret text and images are considered: the images like Football and Moon with size 128 x 128. The images Moon and Earth are hidden in the Peppers and the images Football and Earth are concealed in the Baboon. Different sets of secret images are considered for four different cover images to show the performance of the technique. The cover images are shown in Figure 4.0. The images shown in Figure 4.0 are used to hide secret data. The stego images are shown in Figure 3.0respectively.

(a) Lena (b) Baboon (c) Peppers
Figure .3. Cover images (HSA)

PSNR Comparison
This section gives performance comparison of existing techniques such as LSB,IP, Pixel Value Differencing (PVD) and Pixel Indicator (PI) methods. The PSNR comparison is made with three images such as Lena, Baboon, and peppers.

Table .1. PSNR Value Comparison Table

Host Image 512x512	LSB	IP	PVD	PI	Proposed HAS
Lena	44.250	50.802	44.901	74.585	95.3
Baboon	45.000	50.764	44.966	75.057	96.1
Peppers	43.000	50.797	44.897	74.712	96.1

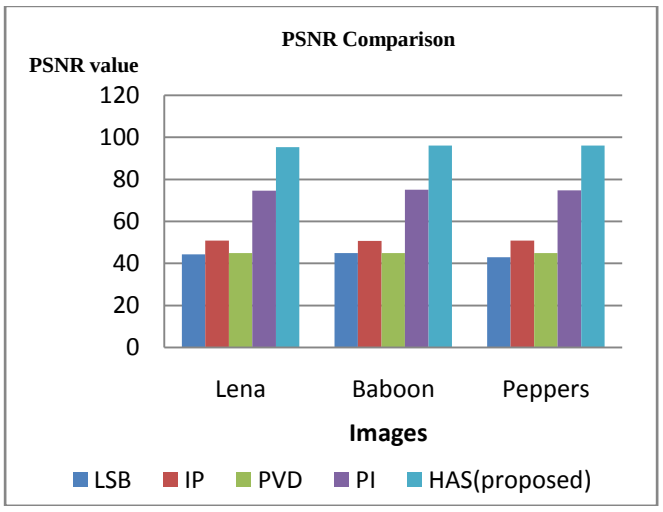

Figure .4. PSNR value comparison

To give the comparisons of the final assessment of the HSA algorithm, comparisons were achieved with other wavelet domain algorithms. Since the main novelty of the approach resides in the way the existing techniques are exploited to hide the secret message where it tested on the various images. Several kinds of attacks were carried out, and for each of them the maximum attack strength the secret message can survive was measured. The algorithm of IWT appeared to meet the highest security and robustness of the proposed system.

V. CONCLUSION

The tremendous improvement in information hiding techniques has drawn a lot of attention now a day, and becomes a dynamic topic in both private and government sectors. In order to protect the system integrity and prevent the exploitation of digital media

from the criminal activities that have malicious intent. Steganography and steganalysis techniques are proposed. The proposed work examined and performed a hybrid steganography approach (HSA) for effective data hiding and analysis; This combines the Integer Wavelet Transform (IWT) and improved SVD. The strict way to choose the secret message such as text, ciphertext, text-image and biometrics data to be embedded into the media content are followed in the proposed system. The proposed system uses HSA technique which is employed for the data embedding, without changes the content of the media. Then the steganalysis using non-linear prediction algorithms have been further studied so as to perform the extraction without information loss for the purpose of security and robustness. The proposed system is evaluated with several quality oriented parameters. This also evaluated various attacks on Stego image such as compression, cropping, filtering, and noisy transmission.

VI. REFERENCES

[1].Simmons, Gustavus J. "The prisoners' problem and the subliminal channel." In *Advances in Cryptology*, pp. 51-67. Springer US, 1984.

[2]. Mohammeda, Arifullah, Kin-Ying Wonga, Paritala Vikrama, Kishore K. Chiruvellab, and Arifullah Mohammed. "Phytochemical Screening and Antimicrobial Potentials of Borreria sps (Rubiaceae)." (2014).

[3]. Hussain, Mehdi, and Mureed Hussain. "A survey of image steganography techniques." (2013).

[4]. Dhand, Geetika. "Information Hiding Techniques." In *proceeding of the national conference: INDIAcom-2008*.

[5]. Swanson, Mitchell D., Bin Zhu, and Ahmed H. Tewfik. "Robust data hiding for images." In *Digital Signal Processing Workshop Proceedings, 1996., IEEE*, pp. 37-40. IEEE, 1996

[6]. Robinson, Jonathan, and Vojislav Kecman. "Combining support vector machine learning with the discrete cosine transform in image compression." *IEEE Transactions on Neural Networks* 14, no. 4 (2003): 950-958.

[7]. Chan, Chi-Kwong, and Lee-Ming Cheng. "Hiding data in images by simple LSB substitution." *Pattern recognition* 37, no. 3 (2004): 469-474.

[8]. Chan, Chi-Kwong, and Lee-Ming Cheng. "Hiding data in images by simple LSB substitution." *Pattern recognition* 37, no. 3 (2004): 469-474.

[9]. Yang, Cheng-Hsing. "Inverted pattern approach to improve image quality of information hiding by LSB substitution *Pattern Recognition* 41, no. 8 (2008): 2674-2683.

[10]. Sancheti, Ankita. "Pixel Value Differencing Image Steganography Using Secret Key." *International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN* (2012): 2278-3075.

[11]. Amirtharajan, R., D. Adharsh, V. Vignesh, and R. John Bosco Balaguru. "PVD blend with pixel indicator-OPAP composite for high fidelity steganography." *International Journal of Computer Applications* 7, no. 9 (2010): 31-37.

[12]. Potdar, Vidyasagar M., and Elizabeth Chang. "Grey level modification steganography for secret communication." In *Industrial Informatics, 2004. INDIN'04. 2004 2nd IEEE International Conference on*, pp. 223-228. IEEE, 2004.