International Journal of Engineering &Technology, 7 (1.7) (2018) 100-104

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Secret data sharing using steganography and image processing

R. Bhuvanya [1] *, K. Vijayalakshmi [1], S. Uma [1], A. Suresh [2]

[1] *Assistant Professor, Department of Computer Science and Engineering, School of Computing, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai-62, TamilNadu, India*
[2] *Professor & Head, Department of Computer Science and Engineering, Nehru Institute of Engineering and Technology, T.M.Palayam, Coimbatore-641105, TamilNadu, India*
**Corresponding author E-mail: bhuvanya@veltechuniv.edu.in*

Abstract

Steganography is a technique that helps to hide the secret data inside the digitally covered image. The message to be hidden can be a text,image, speech, video. The proposed method aims to combine the technique of steganography and Image Processing. Cover image helps to carry the secret data in an embedded form which is referred as stego image. This work proposes a new implementation process called clustering modification directions (CMDs). To implement this methodology, several sub images will be created by decomposing the cover image using additive distortion functions. To enhance the security, password protection is also applied for the hidden information to be retrieved.

Keywords: *Stegnography; Image Processing; Clustering Modification Directions.*

1. Introduction

Steganography technique allows the secret data transmission in images, audio and video. To hide the secret data in digital image various techniques are available. In the existing system of HUGO (Highly Undetectable Stego) the cost of each pixel is calculated by taking weighted sum of difference between the feature vectors taken from the cover image and their equivalent parts from a prospective stego image.
In the technique of WOW (Wavelet Obtained Weights) high costs will be assigned to pixels which are more predictable and low costs to less predictable pixels. S-UNIWARD and WOW shows the similar performance and works better than HUGO. HILL (High pass and low pass) works better than WOW by utilizing one high pass and two low pass filters.
Embedded data concentrated in textured areas will perform better than applying WOW and S-UNIWARD technique.
Fundamental Steps in Image Processing

- Image acquisition: To obtain digital image through processing and compression.
- Image preprocessing: Process of obtaining the improved image through various techniques.
- Image segmentation: Helps to partition the input image into sub image.
- Image representation: Conversion of input data to a form suitable for computer processing.

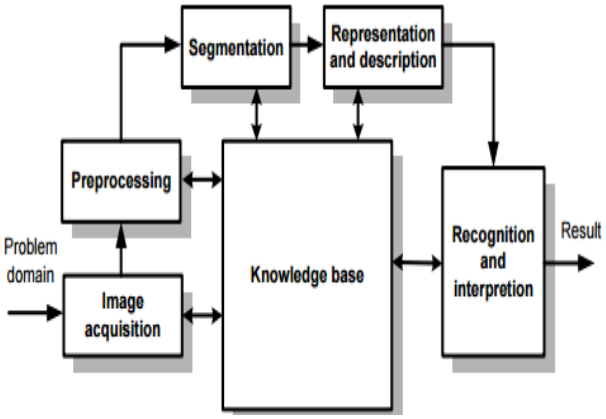


Fig. 1.1: Image Processing Steps.

2. Related work

2.1. Steganography using reversible texture synthesis

S. Hemalatha et.al [1] proposed a novel methodology for hiding the secret image through a reversible composition blend. A surface union resize a little composition picture which may include another composition with a neighborhood appearance. Rather than taking a current picture to wrap message this process covers the source surface picture, and installs mystery messages. Though this approach offers unmistakable preferences small drawback found is that the texture synthesis process resizes a smaller texture image which in turn produces a new texture image with a similar appearance and random size.

2.2. Digital image steganography using a novel uniform distortion function with all possible DCT magnitudes

G. Swain et. al [2] proved the improper utilization of DC and zero AC coefficients might occupy extra square in JPEG steganography, and the productivity will get reduced due to the JPEG pressure. This paper suggests certain DC and zero AC coefficients can be consolidated to further information installing without destroying, and security execution can be expanded. The installed twisting is processed as an aggregate of relative changes of coefficients. But the drawback found is that the usage of stego key made the detection process difficult.

2.3. Ensemble classifiers for steganalysis of digital media

B. Li et.al [6] presented a well-known machine learning device "Gathering Classifiers" that is especially suited for steganalytic techniques. It scales a great deal with respect to the number of samples and the element dimensionality with the execution equivalent to SVM. This work essentially reduces training many-sided quality and allows the steganalyst people to work with rich spread models. Group classification is depicted here as an effective designer apparatus that permits quick development of steganography identifiers with extraordinarily enhanced discovery over a variety of embedding methods. As a conclusion the drawback found is here that the complexity of support vector machine slows down the development cycle even for the problems of moderate size.

2.4. Efficient and secure biometric image stegnography using discrete wavelet transform

V. Holub et. al [9] adopted a new strategy of steganography for embedding a secret data in the skin portion of the image as it is not sensitive to Human Visual System. This method follows the strategy of hiding the data in the skin tone region instead of embedding anywhere in the image. Initially the skin will be detected in the cover images and the hiding of text will be done through Discrete Wavelet Transform (DWT).The reason behind the choice of DWT is, it works better than Discrete Cosine Transform while it comes for compression. The above mentioned method will provide more robustness than any other existing methods.

2.5. Jpeg error analysis and its applications to digital image forensics

G. Liu et. al [10] criticized JPEG is a standout amongst the most broadly utilized picture groups. In this paper, author examined JPEG blunder examination with the investigation of picture legal sciences. The principle blunders of JPEG incorporate quantization, adjusting, and truncation blunders. Through hypothetically breaking down the impacts of these blunders on single and twofold JPEG pressure, proposed three novel plans for picture crime scene investigation including recognizing whether a bitmap picture has already been JPEG packed, assessing the quantization ventures of a JPEG picture, furthermore, identifying the quantization table of a JPEG picture. Broad test results demonstrate that this new techniques altogether beat existing systems particularly for the pictures of little sizes. And the new technique can dependably identify JPEG picture squares which are as little as 8 pixels and packed with quality elements as high as 98. But the drawback here is that Image forgery, like any other illegal and pernicious activity, could cause serious harm to society.

3. Implementation

A novel approach is introduced to hide the secret data in digital images, in some of the images pre processing techniques are applied to get the clear image and to extract the desired feature from the particular digital image. Once the feature is extracted then the selection of trained data will be done. And the process of image processing is depicted in the below figure 3.1.

Various image enhancements and image processing techniques used are discussed.

Enhancement

- Histogram equalization-Helps to redistributes the intensities of the image (usually 256 gray-scale levels).
- Unsharp masking-Smoothed image will be subtracted from the original image to enhance the intensity.

Convolution

Convolution process is 3×3 masks operate on pixels. Here the high pass filter is used to emphasize regions where the low pass filter helps to smoothens images, blurs regions.

Math processes

Math processes programs perform a variety of functions.

- Add images-Two images can be added through pixel by pixel.
- Subtract images-Second image will be subtracted from the first image based on pixel by pixel.
- Exponential or logarithm-Process helps to take log of pixel intensity.

Noise filters

- Noise filters eliminates the external disturbance in the image.
- Mean, median and Gaussian filtering can be applied to remove the noise and to destroy the lines, other fine details of the image.

Trend removal

Trend removal programs remove intensity trends which vary slowly over the image. It can be done by either choosing row or column based on the direction with minimal abrupt changes.

Edge detection

Edge detection programs helps to find boundaries in an image. Process of image segmentation, extraction of data can be achieved through the edge detection.

Image analysis

Extraction of useful information from the digital image will be achieved through image analysis.

Image segmentation

Multiple segments of the digital image will be achieved that typically used to locate boundaries such as lines, curves etc. The result obtained may be the set of segments or contours derived from the particular image. Here the process of assigning a label to every pixel will be carried out. Labels will be shared by the pixel which possesses similar characteristics.

The proposed method aims to combine the technique of Steganography and cryptography. Cryptography may scramble the message and there is a possibility that it can't be understood by the user. Where the Steganography hide the message so there is no knowledge of the existence of the message inside the digital image. When speaking about the comparison, it is made between portions of the plaintext and cipher text in cryptography. Whereas in steganography the comparison is done between the cover-media, the stego-media, and some possible portions of the message.

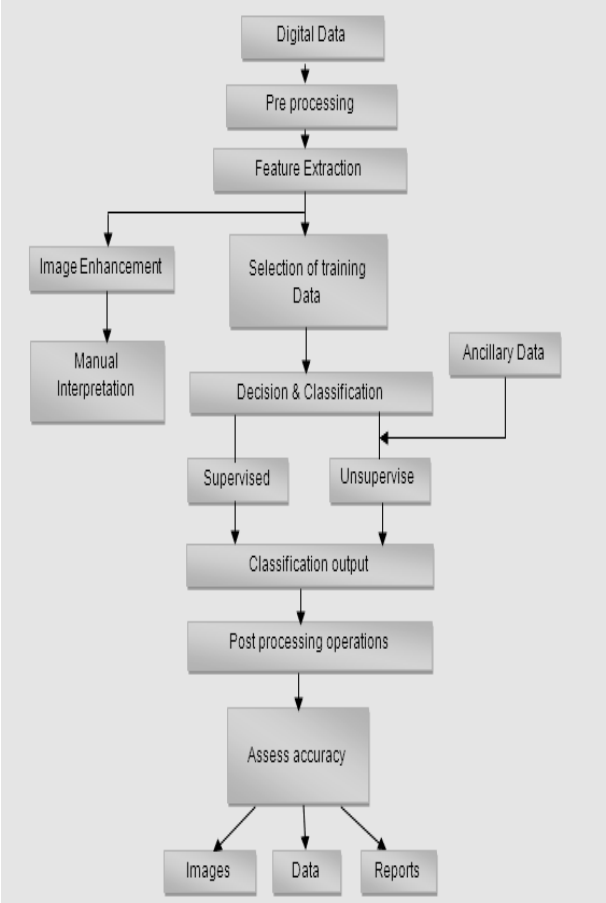


Fig. 3.1: Process Involved in Digital Image Processing.

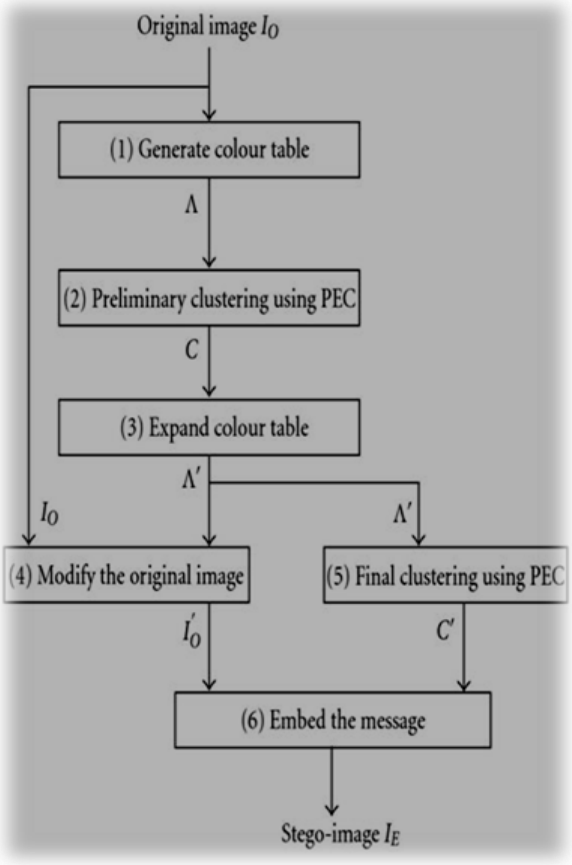


Fig. 3.2: Clustering Modification Direction.

Techniques Used

- Image Acquisition
- Clustering Modification Direction
- Text Embedding
- Decomposition
- Hill Steganalyzer

Image Acquisition

Initial stage of image processing sequence which follows the process of processing, compression and storing of image in a digital form. And it is the process of extracting the image from some source preferably it is hardware. One of the ultimate goal of this process is to have a source of input image that should be operated within the controlled guidelines. If it is in the necessary situation it helps to perfectly reproduce the image under the same conditions.

Clustering Modification Direction

Carrying out clustering on an image helps to yield different sets of useful data. Progressive exponential clustering (PEC) is one of the new clustering algorithm applied to increase the capacity of data to be embedded by avoiding redundancy. Another technique of cluster expansion algorithm also helps to increase the capacity of embedding data by not compromising imperceptibilty. Following figure illustrates the process involved in Clustering Modification Direction (CMD).

Text Embedding

Text embedding methods visualize the representation of text. Low dimensional representation is one among the method applicable to many different task but not restricted for any single task. This work introduced the concept of semi supervised representation learning for embedding the text data. Levels of labeled information are represented through a large scale heterogeneous network where the text can be embedded through an efficient algorithm. Low dimensional embedding helps to preserve the closeness of words. In order to encrypt the text RC4, Alternative step, shrinking generator can be used. The process of text hiding is depicted in the figure 3.4.

Decomposition

To strengthen the performance of the image and to optimize the quality of stego image singular value decomposition and integer wavelet transform is proposed. Acquired results are compared with discrete cosine transform (DCT), redundant discrete wavelet transforms (RDWT) and correlation coefficient metrics for checking the performance. Experimental results proved that the proposed method provides more robustness in JPEG compression and filtering techniques.

Hill steganalyzer

Dimensional SRM (spatial rich model) features and the ensemble classifiers are equipped with hill steganalyzer which checks the performance of noise pattern. Average value taken from the false positive rate and false negative rate is termed as the classification error.

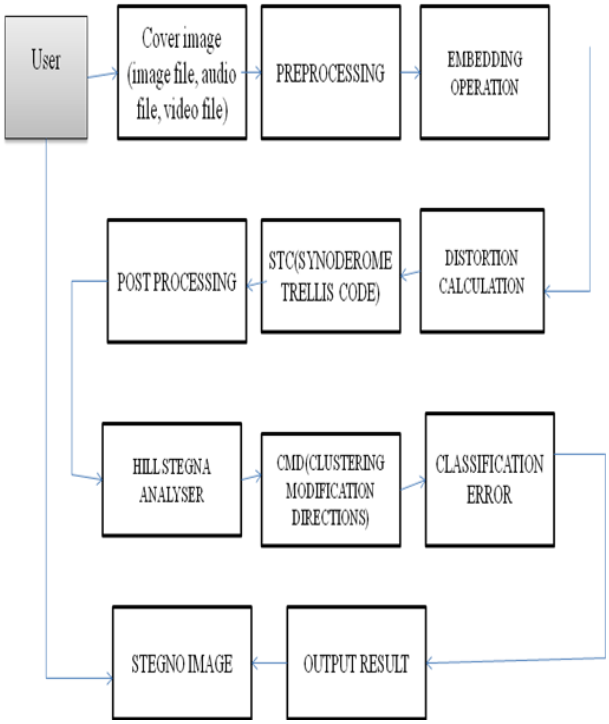
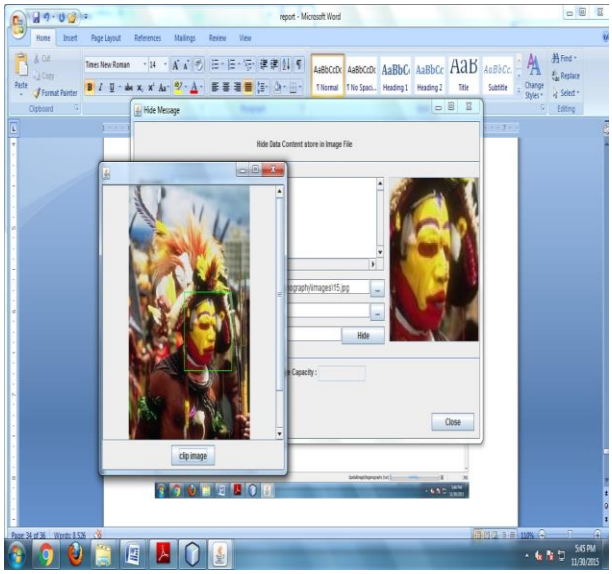
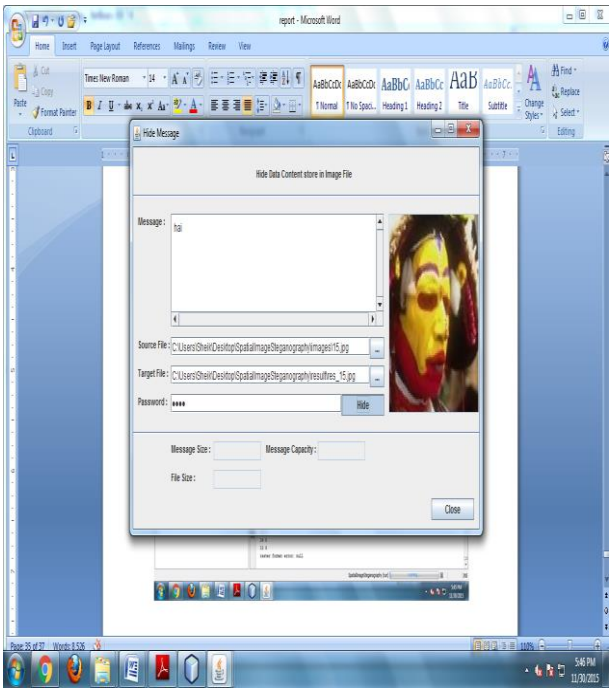


Fig. 3.3: Process of Text Hiding.

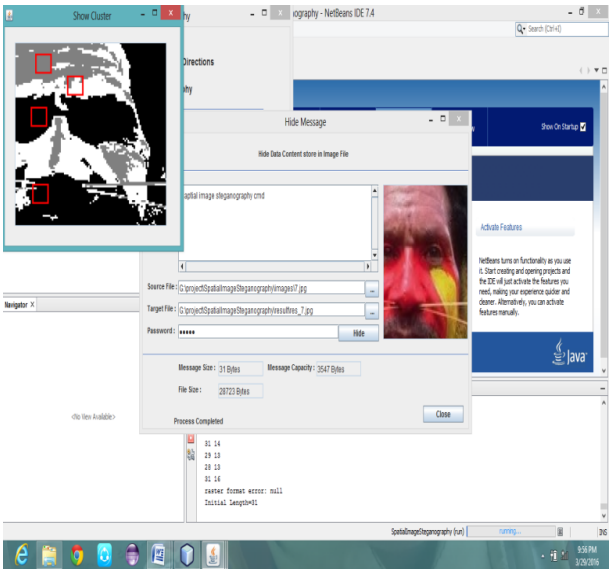
4. Results and discussion



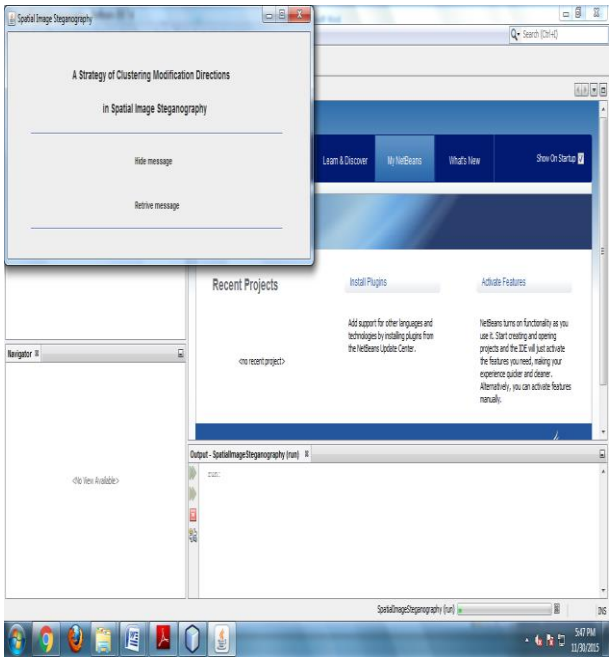
4.1. Extraction of feature from the selected image



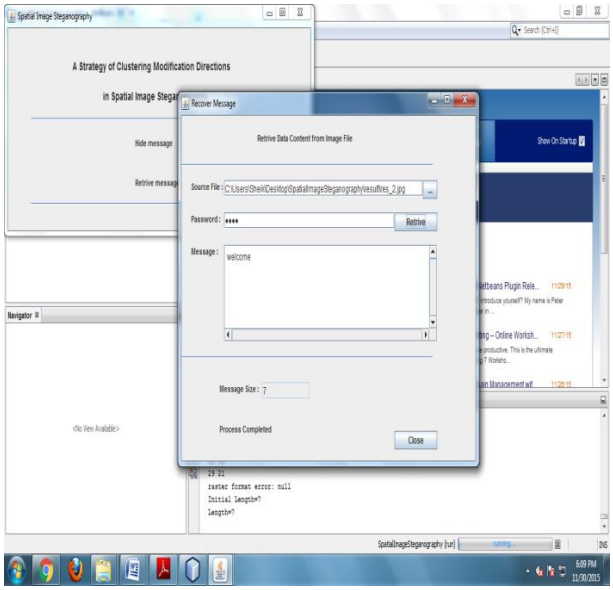
4.2. Password protection added



4.3 Hiding of text inside the image



4.4. Process of retrieving images



4.5. Retrieved message

5. Conclusion

This work adopts the strategy of steganography along with the image processing which embeds the secret data in an image. Since the secret data is embedded in various segments of image it is not as easy to predict the image with the particular component. Though the opponent retrieves the particular component of the image, password protection mode is enabled which doesn't allow them to retrieve the embedded data. Thus the probability of protection is enhanced using Clustering modification direction and Text Embedding.

Acknowledgement

Finally I would like to thank my colleagues, friends and family members for encouraging me to finish this work.

References

[1] S.Hemalatha, D. Acharya, A.Renuka and P. Kamath," A Secure and High Capacity Image Steganography Technique", Signal & Image Processing: An International Journal (SIPIJ) Vol.4, No.1, 2015.

[2] G. Swain and S.K. Lenka," Steganography using two sided, three sided, and four sided side match methods", CSI Transaction on ICT,Springer-Verlag, pp.127- 133, 2015.

[3] G. Liu, W. Liu, Y. Dai, and S. Lian, "Adaptive steganography based on syndrome-trellis codes and local complexity," in Proc. 4th IEEE Int. Conf. Multimedia Inf. Netw. Secur., Nanjing, China, Nov. 2014, pp. 323–327.

[4] V. Holub and J. Fridrich, "Digital image steganography using universal distortion," in Proc. 1st ACM Workshop Inf. Hiding Multimedia Secur., Montpellier, France, Jun. 2013, pp. 59–68. https://doi.org/10.1145/2482513.2482514.

[5] T. Denemark, J. Fridrich, and V. Holub, "Further study on the security of S-UNIWARD," Proc. SPIE, Electron. Imag., Media Watermarking, Secure Forensics, vol. 9028, pp. 902805-1–902805-13, Feb. 2013.

[6] B. Li, M. Wang, J. Huang, and X. Li, "A new cost function for spatial image steganography," in Proc. IEEE Int. Conf. Image Process., Paris https://doi.org/10.1109/ICIP.2014.7025854.

[7] "Adaptive steganalysis against WOW embedding algorithm," in Proc. 2nd ACM Workshop Inf. Hiding Multimedia Secur., Salzburg, Austria, Jun. 2012, pp. 91–96.

[8] T. Denemark, V. Sedighi, V. Holub, R. Cogranne, and J. Fridrich, Selection-channel-aware rich model for steganalysis of digital images," in Proc. IEEE Int. Workshop Inf. Forensic Secur., Atlanta, GA, USA, Dec. 2011, pp. 48–53.

[9] V.Holub, "Content adaptive steganography—Design and detection," Ph.D. dissertation, Dept. Elect. Comput. Eng., Binghamton Univ., Binghamton, NY, USA, 2011.

[10] G. Liu, W. Liu, Y. Dai, and S. Lian, "Adaptive steganography based on syndrome-trellis codes and local complexity," in Proc. 4th IEEE Int. Conf. Multimedia Inf. Netw. Secur., Nanjing, China, Nov. 2010.