Steganography in Multimedia

Subalakshmi Shanthosi S

SSN College of Engineering

29-03-2019

Presentation Outline

Steganography

- Steganography is the process of hiding a secret message within a larger one in such a way that someone can not know the presence or contents of the hidden message.
- Aim - To develop a generative system which is capable of hiding the secret message into the different Multimedia files without any ease of decryption.

Challenges in Steganography For Multimedia.

- To make sure that the steganography doesnt affect the image quality.
- Secret data should be undetectable without secret knowledge, typically the key.
- Presence of multiple data without interferring with one another.
- The secret data should survive attacks that dont degrade the perceived quality of the work.
- The proposed procedure is simple and easy to implement.
- Practical,Personal and militaristic applications for both point-to-point and point-to multi-point communications.

Presentation Outline

Image Hiding by Non-Uniform Generalised LSB and Dynamic Programming[1].

- Adaptive LSB technique to reduce the destortion while replacing the pixel values with data bits.
- Methods used:
  - Modified LSB(Least Significant Bit) Technique.
  - Modified LSB Technique with AES authentication mechanism.
  - Steganography approach based on LSB in digital image.
  - IMStego-Java based Tool with reduced PSNR in conventional LSB approach.
- Different Spatial and Transform techniques are realised.
- Literature review demonstrating the popular steganographic techniques.

Digital Image Steganography Using Modified LSB and AES Cryptography[2].

- This method ensures enhanced security of digital images.
- Steps involved:
  - The secret message is transformed to cipher text by AES cryptography.
  - The cipher text is hidden inside the image using the modified LSB method.
- Methods:Replacing LSB of cover image with the bits of the concealed message and manipulating the LSB plane of the cover image.
- Limitation :
  - Less secure:Easy to decrypt secret message.
  - Less performance.
- Modified LSB shows improved performance based on PSNR,SSIM metrics.
- Future work:Performance Improvement based on storage or computatational time.

Boundary-based Image Forgery Detection by Fast Shallow CNN[3].

- Network (SCNN) capable of distinguishing the boundaries of forged regions from original edges in low resolution images SCNN is designed to utilize the information of chroma and saturation.
- Methods:Based on SCNN:
  - Sliding Windows Detection (SWD).
  - Fast SCNN.
- Methodology:
  - SWD: We start by picking a certain window of an image.
  - Window is feed into SCNN and compute a confidence score to predict whether it is tampered.
  - Confidence score and probablity map is maintained.
  - Then the window slides over and outputs another confidence score.
  - After sliding the window through the entire image, a complete probability map is constructed.

Boundary-based Image Forgery Detection by Fast Shallow CNN[3]

- Fast SCNN :
  - Takes entire image as the input
  - Produces feature maps by processing the entire image with Conv layers.
  - Extract feature vectors with dimension from feature maps and feed them into fully-connected layers.
  - The parameters of Fast SCNN are all trained by SCNN on the patch dataset.
- Limitation :
  - Less secure:Easy to decrypt secret message.
  - Less performance.
- Modified LSB shows improved performance based on PSNR,SSIM metrics.
- Future work:Performance Improvement based on storage or computatational time.

Steganalysis of RGB Images Using Merged Statistical Features of Color Channels[4]

- The steganalysis process is based on supervised machine learning, utilizing the Support Vector Machine (SVM) binary classifiers implementation in MATLAB.
- Proposed Model:
  - Based on merging features of single color channels into a multi-channel feature set, without consideration to the correlation between color channels.
  - Accuracy of model is evaluated with uncompressed RGB clean image and stego image.
  - Feature Selection - Statistical Textural Features:
    - Single Channel - Statistical and Traditional Feature Set.
    - Multi Channel - Consists of GLCM features. Contrast,Correlation,Energy and Homogeneity, as well as other textural features such as Entropy in the study of textural features of images, and have been used in many steganalysis research works.

Steganalysis of RGB Images Using Merged Statistical Features of Color Channels[4].

- Dataset : The selected cover image type is uncompressed RGB-BMP, in three channels, without the alpha channel.
- Two independent datasets are used, for double validation:
  - The first validation dataset consists of 1500 clean images in TIFF format with alpha channel, that were downloaded from the Natural Resources Conservation (NRC) image dataset.
  - The CALTECHs birds images dataset [14], which is in a compressed color JPEG format .A set of 1500 CALTECH images were converted to BMP format and resized to 512 X 512 pixels.

Steganalysis of RGB Images Using Merged Statistical Features of Color Channels[4].

- Experimental Work:
  - Embedding : Secret messages are embedded using Spatial Steganography.
    - Each Channel in each pixel were Embedded with 2 bits or 4 bits by replacing the least significant bits .For single channel embedding, only the NRC cover images were used, in which the Blue color channel of each pixel was embedded using 2-bpc.
    - The processes of embedding have produced five stego datasets: NRC-LSB2, NRC-LSB4, CALTECH-LSB2, CALTECHLSB4, and NRC-2LSB-Blue.
  - Features Extraction: Using build in functions of MATLAB.
  - Classification using SVM Classifier.
  - Evaluation metrics :True Negative(TN),True Positive(TP), False Negative(FN) , False Positive(FP) and Detection Accuracy(DA).

Steganalysis of RGB Images Using Merged Statistical Features of Color Channels[4].

- Limitation:
  - Does not apply to compressed images with lossey compression.
  - Performance and Storage consideration for Multi channel.
  - Capacity of hiding data is low.
- Future Work : The proposed steganalysis model can be evaluated. using
  - Lower embedding rates.
  - Different media types : audio and video.
  - Flexibility to work with transform domain.

Large-Scale JPEG Image Steganalysis Using Hybrid Deep-Learning Framework[5].

- Deep Learning in Image Steganalysis is still in its initial stage-A generic hybrid deep-learning framework for JPEG steganalysis incorporating the domain knowledge behind rich steganalytic models.
- Stages in JPEG Steganalysis:
  - The first stage is hand-crafted, corresponding to the convolution phase followed by for rich model :
    - Quantization phase.
    - Truncation phase.
  - The second stage is a compound deep-neural network containing multiple deep subnets, in which the model parameters are learned in the training procedure.

Large-Scale JPEG Image Steganalysis Using Hybrid Deep-Learning Framework[5].

- Proposed Model:
  - Preliminaries:
    - The principal part of CNN is a cascade of alternating convolutional layers, regulation layers (eg. BN layers) and pooling layers.
- Working :
  - Each neuron unit receives inputs from a previous layer, performs a dot product with weights and optionally follows it with a nonlinear point-wise activation function .
  - CNNs can be trained using backpropagation.
- Quantisation and Truncation in Steganalysis:
  - Convolution with series of kernal to derive varied noise residuals.
  - Quantisation.
  - Truncation.
  - Aggregation.

Large-Scale JPEG Image Steganalysis Using Hybrid Deep-Learning Framework[5]

- Hybrid Deep Learning Approach :
  - Takes Decompressed JPEG images and performes Convolution and Quantisation,Truncation.
  - The second stage is a compound deep CNN network in which the model parameters are learned in the training procedure.
- Future Work :
  - Incorporation of Adversarial Machine Learning into current hybrid framework.
  - Exploration of the application of hybrid framework in the field of multimedia forensics.

Presentation Outline

- **Image Steganography Review paper [1]**, International Journal of Advanced Research in Computer and Communication Engineering(IJARCCE) , Mohammed A Saleh ,DOI.

- **Image Steganography Based on Modified LSB Substitution Method and Data Mapping[2]** , International Journal of Computer Science and Network Security(IJCSNS) , Pranab Kumar Dhar, Abdul Kaium and Tetsuya Shimamura , DOI [

- **Boundary-based Image Forgery Detection by Fast Shallow CNN[3]** , 2018 24th International Conference on Pattern Recognition (ICPR) , Zhongping Zhang , Yixuan Zhang , Zheng Zhou , Jiebo Luo , DOI [

- **Steganalysis of RGB Images Using Merged Statistical Features of Color Channels[4]** , 2018 11th International Conference on Developments in eSystems Engineering (DeSE) , Zaid I. Rasool , Mudhafar M. Al-Jarrah ,Saad Amin , DOI.

- **Large-Scale JPEG Image Steganalysis Using Hybrid Deep-Learning Framework[5]** , IEEE Transactions on Information Forensics and Security , Jishen Zeng , Shunquan Tan , Bin Li , Jiwu Huang , DOI.