iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IV **Month of publication:** April 2022

DOI: https://doi.org/10.22214/ijraset.2022.41242

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IV Apr 2022- Available at www.ijraset.com

Multi Images Steganography using Neural Network

Gayatri Ulhas Kadam[1], Purva Ignathi Jadhav[2], Trupti Shahaji Chandanshive[3], Kajal Vilas Shinde[4], Mrs. Ashwini Bamanikar[5]
[1, 2, 3, 4, 5]*Computer Engineering, PDEA College of Engineering, Pune (India)*

Abstract: Currently, the most successful approach to steganography in empirical objects, such as digital media, is to embed the payload while minimizing a suitably defined distortion function. The design of the distortion is essentially the only task left to the stegnographer since efficient practical codes exist that embed near the payload-distortion bound. The ractitioner goal is to design the distortion to obtain a scheme with a high empirical statistical detectability.
In this paper, we propose a universal distortion design called universal wavelet relative distortion (UNIWARD) that can be applied for embedding in an arbitrary domain. The embedding distortion is computed as a sum of relative changes of coefficients in a directional filter bank decomposition of the cover image. The directionality forces the embedding changes to such parts of the cover object that are difficult to model in multiple directions, such as textures or noisy regions, while avoiding smooth regions or clean edges. We demonstrate experimentally using rich models as well as targeted attacks that steganographic methods built using UNIWARD match or outperform the current state of the art in the spatial domain, JPEG domain, and side-informed JPEG domain.

I. INTRODUCTION

Steganography is an algorithm to conceal information within an object while keeping the object containing the hidden information indistinguishable from the original one.
The main purpose of steganography is to grant access to the hidden information only to the authorized clients while keeping its content and its presence unrevealed to the others. Encryption Standard image steganography methods usually aim at hiding secret image within a cover image.
To this end, various studies including spatial domain-based methods and frequency domain-based methods have been actively conducted, and remarkable results have been achieved. The hiding network takes a cover image and a secret image as inputs then creates a container image by hiding the secret image into the cover image. The revealing network extracts a hidden secret image from the container image

A. Motivation

In this project we primarily concentrated on the data security issues when sending the data over the network using stenographic techniques. The main objectives of our project are to product security tool based on steganography techniques to hider message carried by stego-media which should not be sensible to human beings and avoid drawing suspicion to the existence of hidden message. We aim to make an effort in a similar direction, by utilizing the ideas from the aforementioned papers to encode multiple images into the single cover image. Unlike traditional methods, we use the same resolution cover and secret images and we aim to keep the changes to the encoded cover image unnoticeable to human perception and statistical analysis, while at the same time keeping the decoded images highly intelligible.

B. Problem Statement

This project addresses the security problem of transmitting the data over internet network, the main idea coming when we start asking that how can we send a message secretly to t destination? The science of steganography answers this question. Using steganography, information can be hidden in carriers such as images, audio files, text files, videos and data transmissions. In this document, we proposed some methods and algorithms of a multi-image steganography system to hide an images of a secret message. We aim to hide multiple images (2 or more) in one not-so-secret cover images. The embedded secret images must be retrievable with minimum loss. The encoded cover images must look like the original cover images.

C. Functional Requirements

1) System Feature 1

Functional requirements are the requirements that define specific behavior or function of the system.

a) *Login:* Login function will authenticate the sender if username and password are correct otherwise it will exit the system.

b) *Secret Image Message File:* In this file you will have to write secret image to hide or you can select any image file of secret message.

c) *Cover Image:* Cover Image is the image is to be selected in which secret text message can be hidden.

d) Stegno Encryption LSB implementation is performed on cover image to hide secret text message by replacing bits of cover image by the bits of message.

e) Sender In this Sender send this stego image file to intended recipient to which he does want to communicate.

f) Receiver in this receiver receives the stego image and opens in decryption option for getting hidden text message inside that image

D. System Implementation

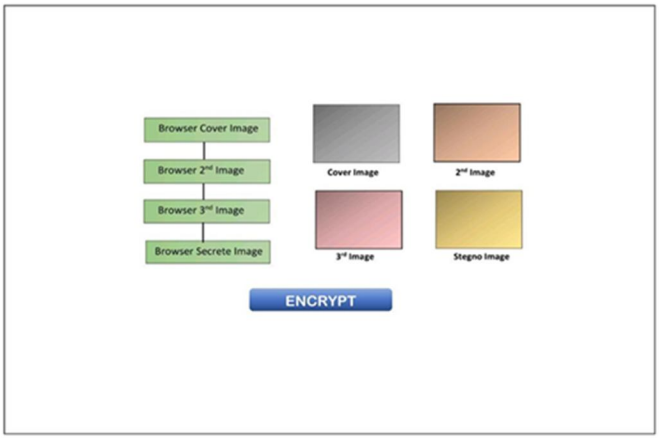
The hiding technique will consist of 4 images namely cover image, two browser images and browser secret image The technique involves two processes i.e. Encryption and Decryption

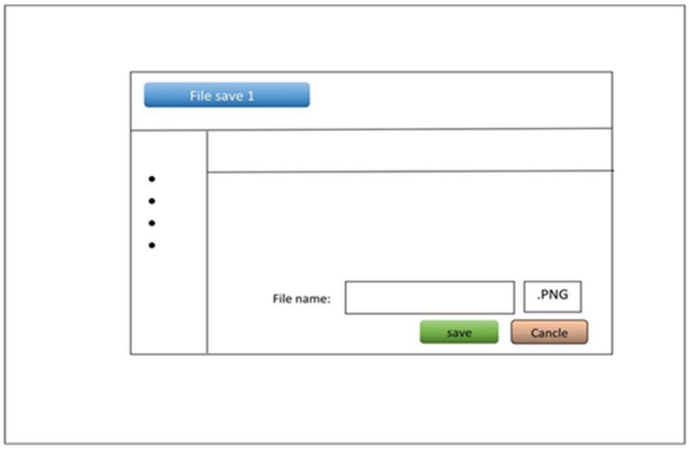
1) The Encryption Process

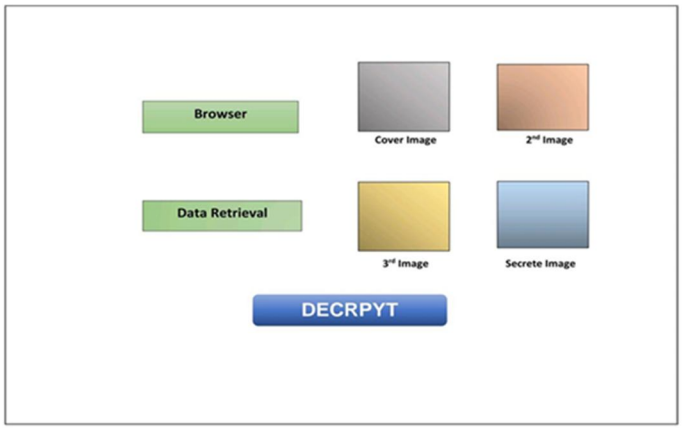
Encryption process consists the data that has to be hidden
Three images are browsed and selected so that data will be encrypted
The browser secret image will have the secret message

2) The Decryption Process

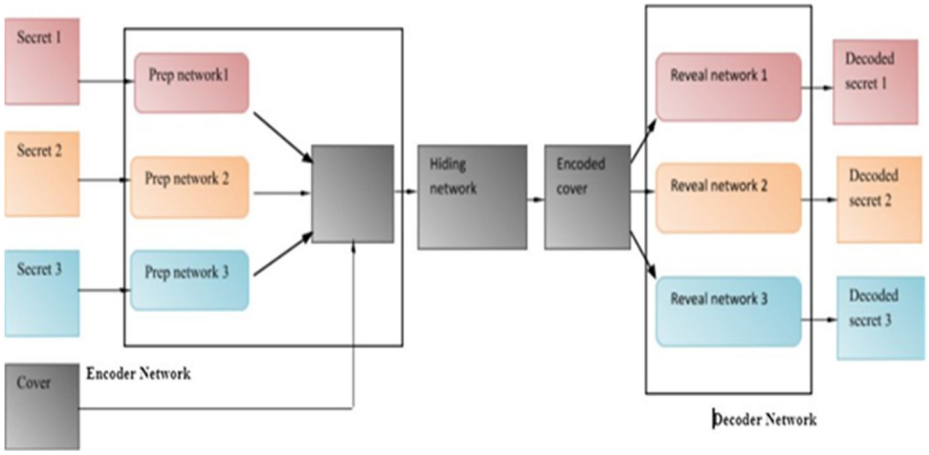
One by One images are selected and the data within the steno image is decrypted.







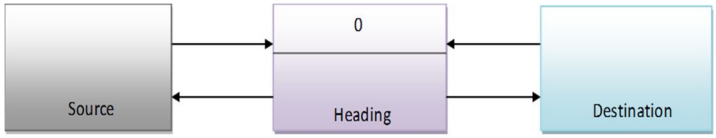
E. System Architecture



We aim to perform multi-image steganography, hiding three or more images in a single cover image. The embedded secret images must be retrievable with minimum loss. The encoded cover image must look like the original cover image. Using of Multiple Prep and Reveal Networks. In their implementation for multiple images signal steganography, suggested the use of multiple decoders to derive the decoded secret from a single encoded cover. This technique is an extension of the same idea in the image domain. It does not require scaling down the size of the image or sacrificing on the color channels of the secret images. There was another technique of using conditional decoders instead of multiple decoders but in this implementation, we have only worked on implementing multiple prep/reveal networks. Hence, we decided to build our extension based on this technique. A brief description of the encoder/decoder framework as per this technique is as follows:

1) *ENCODER:* Consists of multiple prep networks, each corresponding to separate secret image input. Prep network outputs are concatenated together with the cover image and then fed through the Hiding network.
2) *DECODER:* The decoder network comprises of multiple reveal networks, each of which is trained separately to decode its corresponding message.
3) *Prep Networks:* Each of the prep networks consists of the aggregation of 2 layers. With each of the layers made up of 3 separate Conv2D layers. The number of channels for these 3 Conv2D layers is 50, 10, and 5 respectively with the kernel sizes like 3, 4, and 5 for each layer. The stride length constantly remains 1 along both the axis. Appropriate padding is added to each Conv2D layer so as to keep output image in the same dimensions. Each Conv2d layer is followed with a Relook activation. 4. Hiding Network: The hiding network is an aggregation of 5 layers. With each of these layers made up of the 3 separate Conv2D layers. The underlying structure of the Conv2D layers in the hiding network is similar to the Conv2D layers in the Prep Network 5. Reveal Network: Each of the reveal networks shares a similar underlying architecture with the hiding network, using 5 layers of similarly formed Conv2D layers.

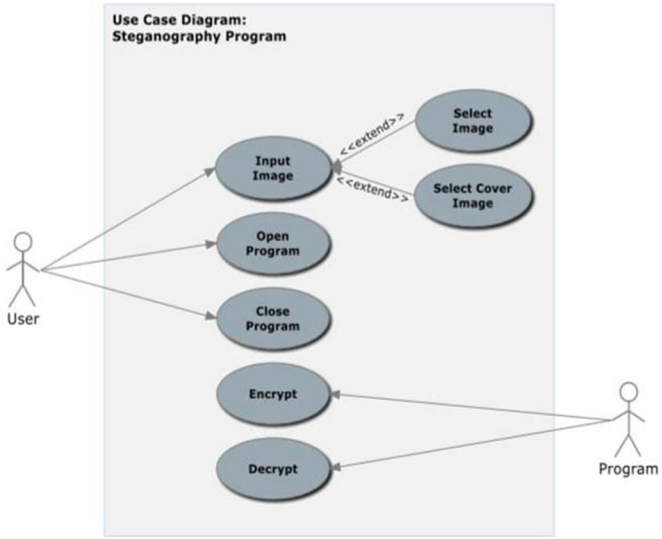
F. Data Flow Diagram



4.2 DFD diagram

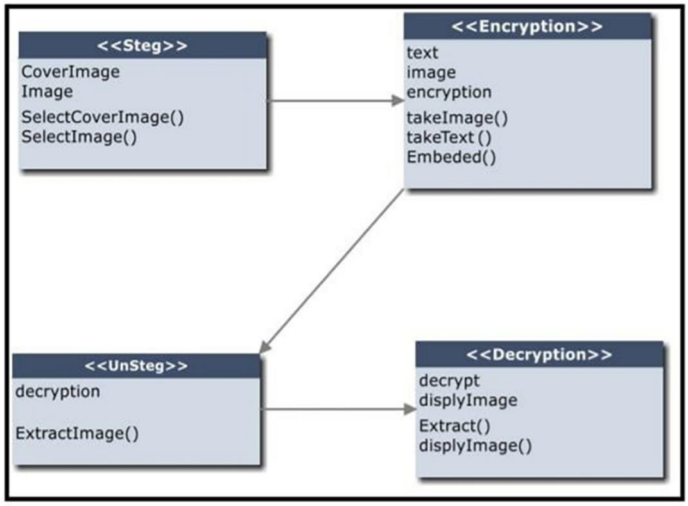
A data flow diagram (DFD) is a graphical representation of the "flow" of data through an information system, modelling its process aspects. Often they are a preliminary step used to create an overview of the system which can later be elaborated. DFDs can also be used for the visualization of data processing (structured design). A DFD shows what kinds of information will be input to and output from the system, where the data will come from and go to, and where the data will be stored. It does not show information about the timing of processes, or information about whether processes will operate in sequence or in parallel

General Use Case Diagram



G. Class Diagram

A class diagram is a picture for describing generic descriptions of possible systems. Class diagrams and collaboration diagrams are alternate representations of object models. Class diagrams contain classes and object diagrams contain objects, but it is possible to mix classes and objects when dealing with various kinds of metadata, so the separation is not rigid



II. LITERATURE SURVEY

A. Paper Name: Multi-Image Steganography Using Deep Neural Networks

Author: Abhishek Das 1 Japsimar Singh Wahi 1 Mansi Anand 2 Yugant Rana

Abstract: Steganography is the science of hiding a secret message within an ordinary public message. Over the years, steganography has been used to encode a lower resolution image into a higher resolution image by simple methods like LSB manipulation. We aim to utilize deep neural networks for the encoding and decoding of multiple secret images inside a single cover image of the same resolution.

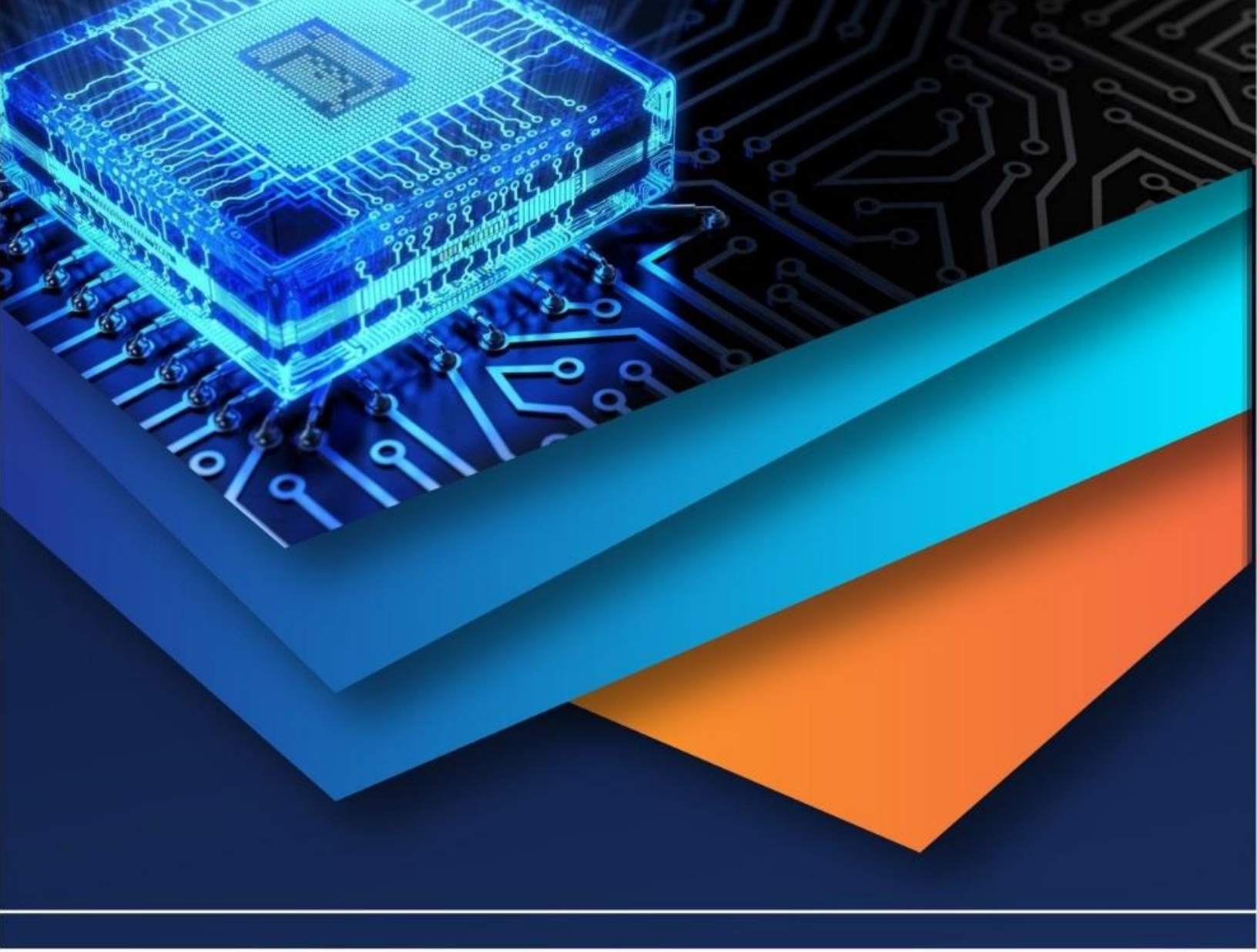
B. Paper Name: Steganalysis of Pixel-Value Differencing Steganographic Method

Author: Vajiheh Sabeti, Shadrokh Samavi, Mojtaba Mahdavi,Shahram Shirani

Abstract: In this paper a steganalysis method is presented for a steganographic routine. The steganography is based on pixel value differencing, PVD, and no attacked has been offered for it yet. By modification of an existing method, that uses 2χ measure, the PVD steganography was successfully and accurately attacked.

REFERENCES

[1] Abhishek Das 1 Japsimar Singh Wahi 1 Mansi Anand 2 Yugant Rana,"Multi-Image Steganography Using Deep Neural Networks".
[2] Vajiheh Sabeti, Shadrokh Samavi, Mojtaba Mahdavi,ShahramShirani,"Steganalysis of Pixel-Value Differencing Steganographic Method"
[3] Vojtech Holub*, Jessica Fridrich and Tomáš Denemark,"A Universal distortion function for steganography in an arbitrary domain"
[4] Vojtˇech Holub and Jessica Fridrich,":Designing Steganographic Distortion using Directional Filters ".
[5] Po-Yueh Chen* and Hung-Ju Lin,"A DWT Based Approach for Image Steganography".



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY