JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

MULTI-IMAGE STEGANOGRAPHY USING DEEP NEURAL NETWORKS

[1]Gayatri Ulhas Kadam, [2]Purva Iganti Jadhav, [3]Trupti Shahaji Chandanshive, [4]Kajal Vilas Shinde, [5]Ashwini Bhamnikar

[1]Student, [2]Student, [3]Student, [4]Student, [5]Teacher
Computer Engineering,
PDEA's 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 steganographer since efficient practical codes exist that pscheme 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.

Introduction: Stegano graphy 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. Various kinds of carriers such as physical objects, texts, sounds, and network packets have been utilized to safely conceal and deliver confidential data. Among them, a digital image is one of the widely used carriers in recent digital steganographic algorithms Various kinds of carriers such as physical objects, texts, sounds, and network packets have been utilized to safely conceal and deliver confidential data. Among them, a digital image is one of the widely used carriers in recent digital steganographic algorithms (i.e., image steganography). Advanced 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 [1,2] and frequency domain-based methods [3–7] have been actively conducted, and remarkable results have been achieved. Although there has been tremendous progress in image steganography, there is still a limitation in hiding a large amount of data. Recently, several studies have tried to hide fullsize secret images inside a cover image using Advanced Encryption Standard[8–10]. These methods are completely different from the conventional image steganography approaches. the Advanced Encryption Standard-based steganography method usually consists of a hiding network and a revealing network. 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.

Motivation

Motivation comes from the recent works, like that of (Baluja, 2017), (Hayes Danezis, 2017), and (Zhu et al., 2018). These papers suggest the use of deep neural networks to model the data-hiding pipeline. These methods have significantly improved the efficiency in terms of maintaining the secrecy and quality of the encoded messages. Recently, similar work in terms of audio signal steganography, like (Kreuk et al., 2019), has shown that deep neural networks can be used to encode multiple audio messages onto a single cover message.

Objective

The objective of Multi-Image Steganography is to hide a secret image within a cover-media in such a way that others cannot discern the presence of the hidden image. Technically in simple words steganography means hiding one piece of data within another.

Problem Statement

Image steganography refers to hiding information i.e. text, images or audio files in another image or video files. The current project aims to use steganography for an image with another image using spatial domain technique. This hidden information can be retrieved only through proper decoding technique.

Software Requirement Specifications:

Functional Requirements:

System feature

- **Database:** The Personal details of sender and receiver also account details of sender and receiver stored in database.
- **User:** User do the registration on the system for transaction, also user has account details of their own accounts and receiver accounts. user do the money transaction and then system keep the details of the sender and receiver.
- **System:** Pre-processing on the dataset. also apply machine learning to train the machine. and detect the accounts details which will connected with the credit card fraud.

External interface requirements:

User interfaces

User of the system will be provided with Graphical User Interface, there is no command line interface for the functions of the product.

Hardware interfaces

Since the application must run over the Internet, all the hardware shall require to connect Internet will be hardware interface for the system. As for e.g. WAN – LAN, Ethernet Cross-Cable.

Software interfaces

PYTHON : Python is a high-level, interpreted, interactive and object-oriented scripting language. Python is designed to be highly readable. It uses English keywords frequently where as other languages use punctuation, and it has fewer syntactical constructions than other languages. • Python is Interpreted Python is processed at runtime by the interpreter. You do not need to compile your program before executing it. This is similar to PERL and PHP.

- Python is Interactive You can actually sit at a Python prompt and interact with the interpreter directly to write your programs.
- Python is Object-Oriented Python supports Object-Oriented style or technique of programming that encapsulates code within objects.
- Python is a Beginner's Language Python is a great language for the beginnerlevel programmers and supports the development of a wide range of applications from simple text processing to WWW browsers to games.**Pyharm :** Pycharm are usually developed in the python language.

Spyder: Spyder is an open-source cross-platform integrated development environment (IDE) for scientific programming in the Python language. Spyder integrates with a number of prominent packages in the scientific Python stack, including NumPy, SciPy, Matplotlib, pandas, IPython, SymPy and Cython, as well as other open-source

software.It is released under the MIT license. Initially created and developed by Pierre Raybaut in 2009, since 2012 Spyder has been maintained and continuously improved by a team of scientific Python developers and the community. Spyder is extensible with first-party and third-party plugins, includes support for interactive tools for data inspection and embeds Python-specific code quality assurance and introspection instruments, such as Pyflakes, Pylint and Rope. It is available cross-platform through Anaconda, on Windows, on macOS through MacPorts, and on major Linux distributions such as Arch Linux, Debian, Fedora, Gentoo Linux, openSUSE and Ubuntu. Spyder uses Qt for its GUI and is designed to use either of the PyQt or PySide Python bindings.QtPy, a thin abstraction layer developed by the Spyder project and later adopted by multiple other packages, provides the flexibility to use either backend.

Communication interfaces

The system can use the HTTP protocol for communication over the Internet and for the intranet communication will be through TCP/IP protocol suite.

System Requirements

Database Requirements

SQLITE: DB Browser for SQLite (DB4S) is a high quality, visual, open source tool to create, design, and edit database files compatible with SQLite. DB4S is for users and developers who want to create, search, and edit databases. DB4S uses a familiar spreadsheet-like interface, and complicated SQL commands do not have to be learned. Controls and wizards are available for users to: Create and compact database files Create, define, modify and delete tables Create, define, and delete indexes Browse, edit, add, and delete records Search records Import and export records as text Import and export tables from/to CSV files Import and export databases from/to SQL dump files Issue SQL queries and inspect the results Examine a log of all SQL commands issued by the application Plot simple graphs based on table or query data.

Software Requirements(Platform Choice)

- Operating system : Windows 7 or more.
- Coding Language : python
- IDE : syder

Hardware Requirements

- System : Intel I3 Processor and above.
- Hard Disk : 20 GB
- Ram : 4GB
- Mobile Sensors : Accelerometer, Gyroscope

Overview of Project Modules:

Pandas: Pandas is an open-source library that is made mainly for working with relational or labeled data both easily and intuitively. It provides various data structures and operations for manipulating numerical data and time series. This library is built on top of the NumPy library.

NumPy: NumPy is a Python library used for working with arrays. It also has functions for working in domain of linear algebra, fourier transform, and matrices.

import cv2: All packages contain Haar cascade files. cv2.data.haarcascades can be used as a shortcut to the data folder.

Pillow: Pillow is the friendly PIL fork by Alex Clark and Contributors. PIL is the Python Imaging Library by Fredrik Lundh and Contributors.

Tools And Technologies used

HARDWARE REQUIREMENTS:

- System Processors : Core2Duo
- Speed : 2.4 GHz
- Hard Disk : 150 GB

SOFTWARE REQUIREMENTS:

- Operating system : 32bit Windows 7 and on words
- Coding Language : Python
- IDE : Pycharm, Syder
- Database : Sqlite

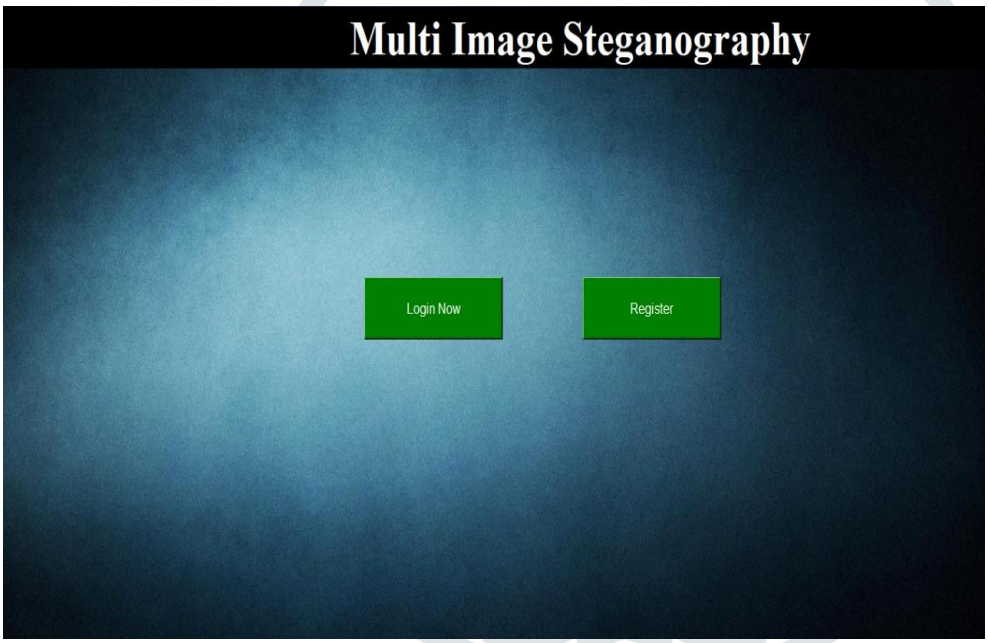
Algorithm

Advanced Encryption Standard algorithm:

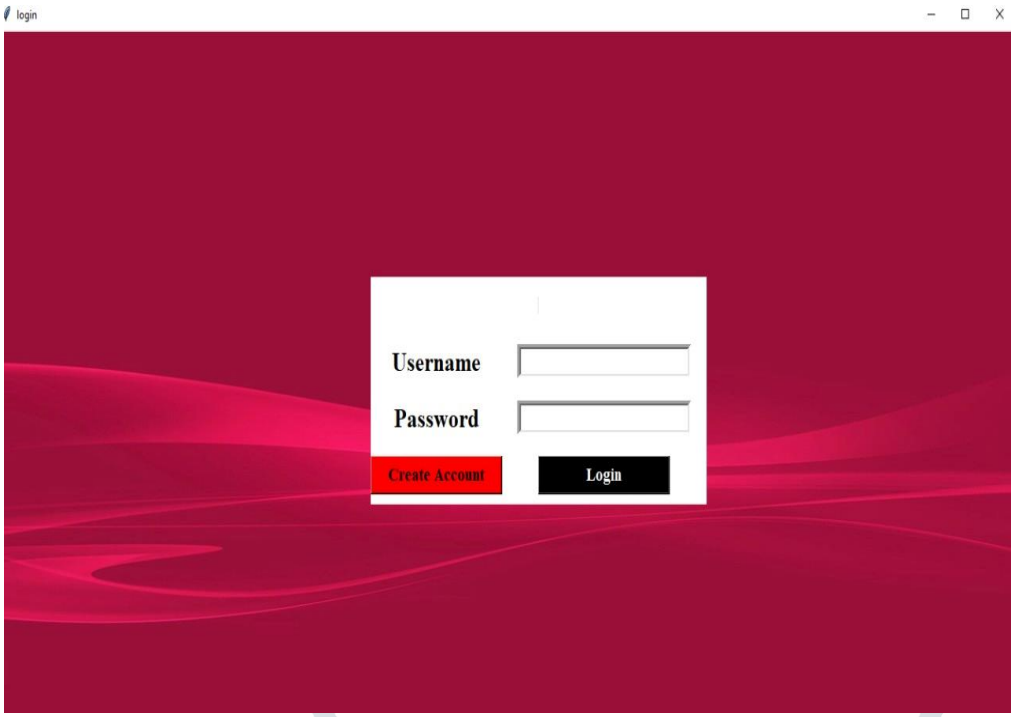
AES is an Advanced Encryption Standard algorithm. It is a type of symmetric, block cipher encryption and decryption algorithm. It works with key size 128, 192, and 256 bits. It uses a valid and similar secret key for both encryption and decryption. In AES, the block cipher is used. It means that the data to be encrypted is converted into blocks for encryption. The original data value is encrypted using different bits of padding such as 128, 192, or 256 bits.

Implementation

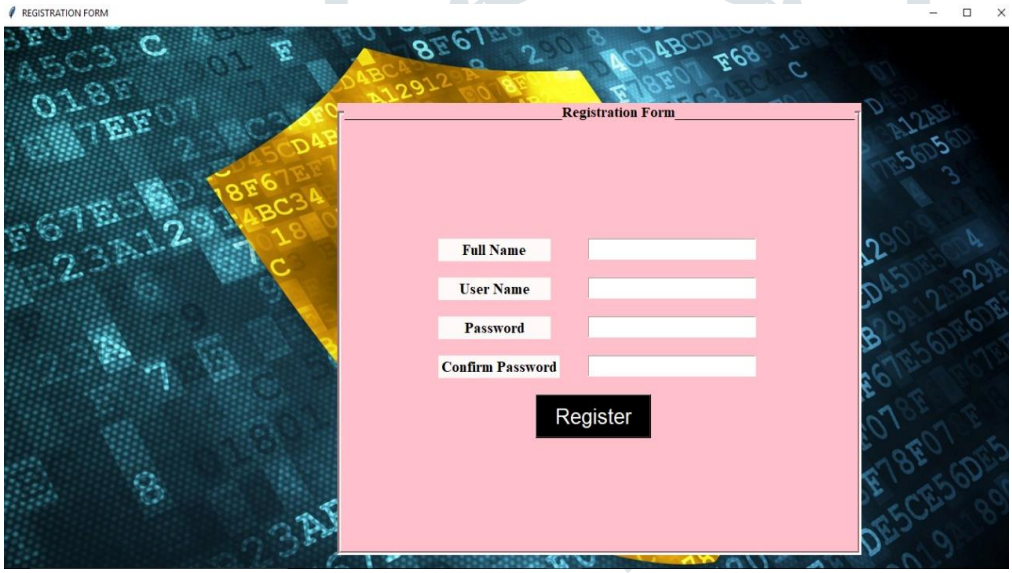
1) Login/Registration



2) Login

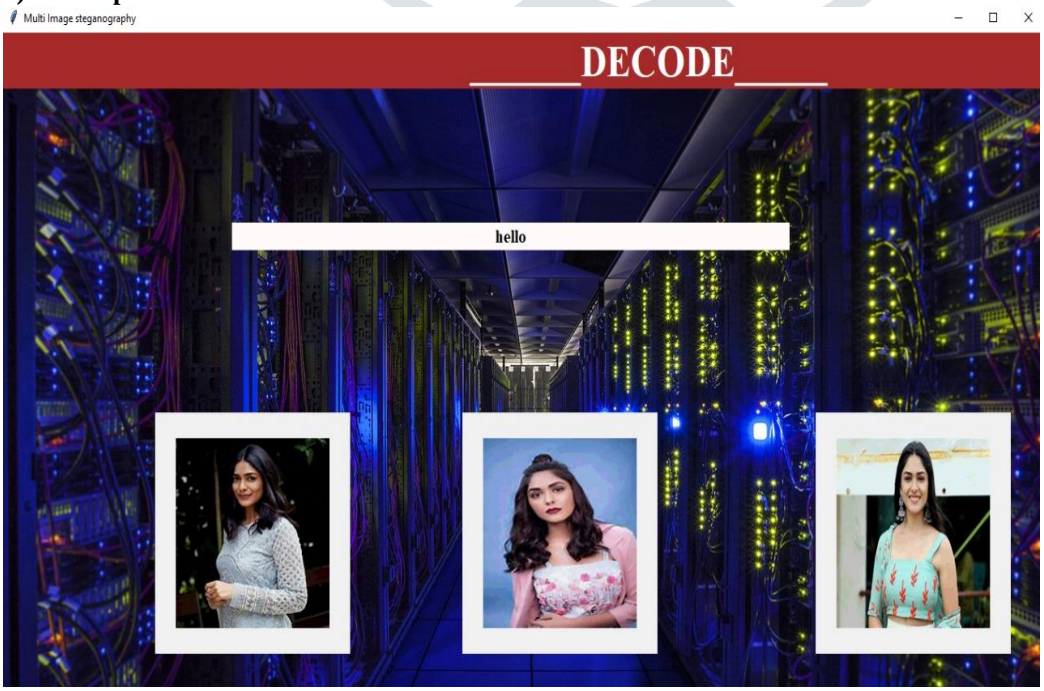


3) Registration Form



4) GUI

5) Decription



Modes AES Algorithm-

1.ECB (Electronic Code Book):

It is the simplest mode among all. It divides the plaintext message into blocks of size 128 bits. Then these blocks are encrypted using the same key and algorithm. Hence, it generates the same cipher text for the same block every time. It is considered a weakness and therefore it is suggested not to use ECB for encryption.

2.CBC (Cipher Block Chaining):

CBC uses an Initialization Vector (IV) to improve the encryption. In CBC, the encryption is performed by XOR operation between the plaintext and IV. Then the cipher text is generated. It then uses the encryption result to XOR with the plain text until the last block.

3.CFB (Cipher FeedBack):

CFB can be used as a stream cipher. It encrypts the initialization vector (IV) first and then XOR with the plaintext to generate the cipher text. Then it encrypts the cipher text with the next plaintext block. In this mode, decryption can be performed in a parallel manner but encryption cannot be performed in a parallel manner.

4.OFB (Output FeedBack):

OFB can also be used as a stream cipher. It does not need padding data. First, the IV is encrypted and then the encryption result is XOR with the plaintext to generate the cipher text. Here, the IV cannot be encrypted or decrypted in a parallel manner.

5.CTR (Counter):6. GCM (Galois/Counter Mode):

In CTR mode the encryption process is similar to OFB mode, the only difference is that it encrypts the counter value instead of IV.It has two advantages, encryption or decryption can be performed in a parallel manner and the noise of one block does not affect another block.

6.GCM (Galois/Counter Mode):

GCM mode is an extended version of CTR mode. It was introduced by NIST. The GCM mode provides the cipher text as well as authentication tag after the encryption process.

Conclusion and Future Work

The concept of the private key to the multi-image steganography, which hides multiple secret images within a single cover image. Our steganography model takes stack of secret images and a cover image as inputs then produces a container image and private keys for each secret image. In order to extract a secret image from the container image, the corresponding private key is required. The proposed model provides a hidden image only when a proper private key is provided, and does not disclose information about other hidden images. Through extensive experiments, we verified the effectiveness of our method under various conditions (i.e., random key and noisy key).

References

1.Abhishek Das 1 Japsimar Singh Wahi 1 Mansi Anand 2 Yugant Rana,"MultiImage 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 Toma´˘s Denemark,"A Universal distortion function for steganography in an arbitrary domain"

4.Vojt˘ech Holub and Jessica Fridrich,":Designing Steganographic Distortion using Directional Filters ".

5.Po-Yueh Chen* and Hung-Ju Lin,"A DWT Based Approach for ImageSteganography