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

Technology of Hiding and Protecting the Secret Image Based on Neural Network: A Review

Miss. Mrunalini Balkrushana Shinde, Dr. Bijendra Gupta

Department of Computer Engineering

Siddhant College Of Engineering, Pune

Abstract

Transmission of secret remote sensing or military photos has become more difficult due to the advancement of new media technology. Studying the technique for securing these secret photographs is a new and difficult endeavour. In this paper, a novel two-channel deep hiding network (TDHN) is designed based on the powerful spatial feature extraction capability of the convolutional neural network by introducing advanced ideas such as skip connection, feature fusion, and so on, and the two channels are used to simultaneously input the cover image and the secret image. There are two sections to this network: the concealment network and the extraction network. The sender employs the hiding network to conceal a secret image within a standard cover image, resulting in a hybrid image known as the hidden image. To extract and recreate the secret image from the hidden image, the receiver employs the extraction network. Meanwhile, two measures called MSE and SSIM are used to create a novel loss function. The TDHN optimised by the loss function may generate a high-quality concealed image and extracted image, according to the results. Between the concealed picture and the original cover image, the SSIM value is around 0.99, and between the extracted image and the original secret image, it's around 0.98. It has been proven through testing on various datasets that the developed and optimized TDHN has great generalisation potential, and so has significant theoretical and engineering utility.

Keywords

Dataembedding ,Convolutional neural network, steganography technology, object localization,Object

Classification,remote sensing images.

Introduction

Many developments have been made in the field of digital media over the lastdecade, and there has been a lot of anxiety about steganography for digital media. Steganography is a unique way of information concealment. It embeds messages into a host medium in order to hide secret messages from eavesdroppers. A typical steganographic application involves covert communications between two parties whose existence is unknown to a potential attacker and whose success is contingent on detecting their existence. In general, relevant digital media such as digital images, text, audio, video, and 3D models are employed as the host medium in steganography. With the growing popularity and use of digital photographs, a great number of image steganographic algorithms have been investigated.In the field of remote sensing, there is currently little demand for accurate localisation. Detection rather than localisation is the focus of the vast majority of research (the two processes have been confused by some people). Detecting objects in remote sensing photos is significantly more difficult than in natural images due to the more complicated background information they carry. Remote sensing photographs provide information about the texture, shape, and structure of things on the ground, and they can be used to identify them precisely. They do, however, create information redundancy issues in addition to giving adequate information for object detection. Object detection in remote sensing photographs is also a difficult problem due to noise interference, weather, illumination intensity, and other factors.This research proposes a novel two-channel deep hiding network (TDHN), which is divided into two parts: the hidden network and the extraction network, based on the deep CNN. The first hiding network can fully extract the high-dimensional features of the cover image and the secret image, then highly integrate the information of these two images to embed the secret image into the cover image and produce a hidden image embedded with secret information that looks visually similar to the original cover image; the second extraction network can automatically extract feature information from the hidden image embedded with secret information.In this paper, we propose a new TDHN is being developed to protect classified remote sensing and military picture data. This network can learn the high-dimensional feature information of images automatically using data, and achieve end-to-end mapping between the original cover image and hidden image, as well as between the hidden image and extracted image. Multi-level features are integrated into the model structure of TDHN, and skip connection, residual connection, feature fusion, feature dimension reduction, and multi-scale feature extraction are introduced to optimise the structure and performance of TDHN. To iteratively optimise the parameters of the model, an innovative loss function is developed by introducing metrics to measure the similarity of image content and metrics to measure the similarity of image structure. Finally, the refined model achieves an excellent image concealment effect.

Literature Survey

In this paper [1], the major aim was to review several ways of combining steganographic and cryptographic techniques to achieve a hybrid system. Moreover, some of the differences between cryptographic and steganographic techniques were presented as well.

In this paper [2], three common cryptographic algorithms two in symmetric cryptography DES, AES and one in asymmetric cryptography RSA are compared. In this one can simply understand the background history of the algorithm in review and the key functional cipher operation of the algorithm. Accordingly summarizes of strength and weakness of each algorithm under the review is highlighted.

In this paper [3], a method is proposed to protect data transferring by three hybrid encryption techniques: symmetric AES algorithm used to encrypt files, asymmetric RSA used to encrypt AES password and HMAC to encrypt symmetric password and/or data. MAC is used to protect the encrypted key or the data.

In this paper [4], efficient pairing free CP-ABE access control scheme using elliptic curve cryptography has been used for data sharing in sub optimal multimedia applications. Data can be accessed only by specific users that are authenticated by the data owner. Pairing based computation is replaced with scalar product on elliptic curves that reduces the resource and memory requirements for users. The features of both cryptography and steganography are combined by embedding crypto text into an image that enhanced data security, privacy and ownership.

In this paper [5], Text encryption has been done using combined elliptic curve cryptography algorithm with Hill cipher which reduces the computation overhead. DCT is applied to the secret image and 40% of these DCT coefficients has been embedded into the base image. The LSB method has been used to embed the encrypted data and the DCT coefficients into the image.

In this paper [6], a watermarking algorithm of colour image is proposed based on Discrete Wavelet Transform, Discrete Cosine Transform and Singular Value Decomposition (DWT-DCT-SVD). First convert host colour image from RGB colour space to YUV colour space. Then a layer of discrete wavelet transform is applied to the luminance component Y, and divided the low frequency and into blocks by using discrete cosine transform, and conducted SVD with every block. Finally embed watermark to the cover image.

In this paper [7], a new method is proposed to provide security to 24 bit color images, by integrating Steganography and Cryptography. In this method, randomized LSB based method is used to hide an image in another image. The resulting stego image is then encrypted using chaotic theory. This new integrated method ensures the enhancement in the data hiding capacity, the security of the image and lossless recovery of the secret data. It also provides the concept of 3 level security: Steganography, Cryptography, and Transmission by splitting.

In this paper [8], comparison between steganography techniques between texts and Images when hiding secret message in texts and images is done. In this several techniques are uses in domain of steganography.

In this paper [9], a novel approach to visual cryptography with the additional capability of authentication based on steganography for hiding digital signature of the secret image was proposed. A new steganography method is used for hiding secret bits in the different blocks of the shares. The method makes no change in the sub-pixels of the shares for hiding binary „0‟, but a change is done for hiding binary „1‟ by flipping a white (black) sub-pixel in one of the blocks of black (white) share The hidden signature can be recovered in the presence of all shares and verified by comparing with the reconstructed digital signature in case of doubt.

In this paper [10], an encoding technique that uses the combination of cryptography and steganography is proposed. Two levels of data encryption is done and then the encrypted data is hidden inside the image. The image in which the cipher text is embedded is used for further purposes.

In this paper [11], hybrid cryptography has been applied using AES and RSA. In this hybrid cryptography, the symmetric key used for message encryption is also encrypted, which ensures a better security. An additional feature of this paper is to create a digital signature by encrypting the hash value of message. At the receiving side this digital signature is used for integrity checking. Then the encrypted message, encrypted symmetric key and encrypted digest are combined together to form a complete message. This complete message again has been secured using the steganography method, LSB.

In this paper [12], cryptography and steganography together are used to ensure two levels of security to the data. The purpose of this paper is to develop new methodology using XOR operation for encrypting the data and embedding the encrypted data into the image pseudo randomly using user chosen key

Motivation

The TDHN proposed in this research is capable of fully automatic concealment and extraction from start to finish. TDHN's model also has great generalisation and migration capabilities, as well as a broad range of engineering applications. We 20-fold increase the leftover image between the hidden image and the original cover image in this section. We can't locate any secret information in the enhanced residual image; just the shape of the cover image can be seen, confirming the great performance and strong security of our proposed TDHN.

The Existing System

In existing system, a reversible image data concealing approach that can recover the cover picture from the stego image without distortion after the concealed data has been extracted. Histogram shifting is a favoured technique among existing ways to reversible image data concealing because it allows for control over pixel alteration, limiting embedding distortion, and it only requires a modest size location map, lowering overhead.Traditional steganography methods often have two major flaws. The first flaw is that, in most studies, the amount of hidden information is limited, and the size of the information to be hidden is small in comparison to the size of the cover image, implying that the cover image's relative capability is relatively limited. To limit the amount of information being passed through specific frequency domain channels.

Proposed System

The suggested TDHN model was tested on a new dataset called AID, which was gathered from Google Earth utilising several remote sensing imaging sensors, and the photos in the dataset came from various nations and seasons. As a result, this dataset contains a lot of inter-class variance and is completely different in terms of picture structure and form from the NWPU-RESISC45 dataset, which is a big challenge for the TDHN model. The TDHN proposed in this research is capable of fully automatic concealment and extraction from start to finish. TDHN's model also has great generalisation and migration capabilities, as well as a broad range of engineering applications.

System Architecture

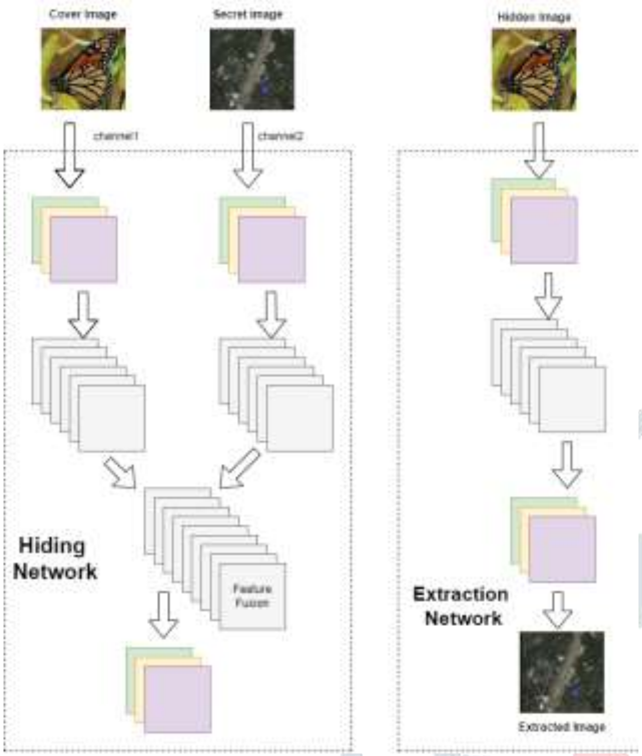

Fig. System Architecture

Conclusion

In this study, a novel end-to-end TDHN is built based on CNN's strong feature extraction ability, and the TDHN's structure is improved using tune skills such as skip connection, feature dimension reduction, feature fusion, and so on. The simulation results demonstrate that our proposed TDHN has a big concealing capacity and sound hiding performance due to the architecture and loss function innovation. Our approach has a relative hiding capacity of 1 bytes/pixel, which is significantly higher than the state-of-the-art method.Hide and safeguard secret or critical military remote sensing photos is a difficult and important undertaking. We want to incorporate GANs into our framework in the future to lessen our reliance on data-driven models. For the HVPS, there is a lot of duplicated information in the hidden image, and the HVPS primarily concentrates on the secret image's vital information. After that, we'll use attention theory to simplify and refine the model, as well as further optimise and increase the hiding performance.

References

[1] Mustafa Sabah Taha, Mohd Shafry Mohd Rahim, Sameer abdulsattar lafta, Mohammed Mahdi Hashim, Hassanain Mahdi Alzuabidi, “Combination of Steganography and Cryptography: A short Survey”, 2nd International Conference on Sustainable Engineering Techniques (ICSET 2019).

[2] Aljaafari Hamza and Basant Kumar, “A Review Paper on DES, AES, RSA Encryption Standards”, Proceedings of the SMART–2020, IEEE Conference ID: 50582 9th International Conference on System Modeling & Advancement in Research Trends, 4th– 5th, December, 2020 Faculty of Engineering & Computing Sciences.

[3] Eman Salim Ibrahim Harba, “Secure Data Encryption Through a Combination of AES, RSA and HMAC”, Engineering, Technology & Applied Science Research Vol. 7, No. 4, 2017.

[4] V. Reshma, S. Joseph Gladwin and C. Thiruvenkatesan, “Pairing-Free CP-ABE based Cryptography Combined with Steganography for Multimedia Applications”, International Conference on Communication and Signal Processing, April 4-6, 2019, India.

[5] S. Joseph Gladwin, Pasumarthi Lakshmi Gowthami, “Combined Cryptography and Steganography for Enhanced Security in Suboptimal Images”, 2020 International Conference on Artificial Intelligence and Signal Processing (AISP).

[6] C. N. Yang, D. S. Wang, “Property Analysis of XOR-Based Visual Cryptography,” IEEE Transactions on Circuits & Systems for Video Technology, vol. 24, no. 12 pp. 189-197, 2014.

[7] Radha S. Phadte, Rachel Dhanaraj, “Enhanced Blend of Image Steganography and Cryptography”, IEEE 2017 International Conference on Computing Methodologies and Communication (ICCMC).

[8] Maisa'a Abid Ali Khodher, Teaba Wala Aldeen Khairi, “Review: A comparison Steganography Between Texts and Images” , FISCAS 2020.

[9] Kh. Manglem Singh, Sukumar Nandi2 , S. Birendra Singh1, L. ShyamSundar Singh1, “Stealth Steganography in Visual Cryptography for Half Tone Images”, International Conference on Computer and Communication Engineering 2008.

[10] Nidhi Menon, Vaithiyanathan V, “Triple Layer Data Hiding Mechanism using Cryptography and Steganography”, 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT-2018), MAY 18th & 19th 2018.

[11] Chitra Biswas, Udayan Das Gupta, Md. Mokammel Haque, “An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography”, 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), 7-9 February, 2019.

[12] Krishna Chaitanya Nunna, Ramakalavathi Marapareddy, “Secure Data Transfer Through Internet Using Cryptography and Image Steganography”, IEEE SoutheastCon 2020.