Enhanced CNN DCT Steganography: Deep Learning Based Image Steganography

By

Erin Akter

[201-35-3089]

A thesis that was turned in to complete some of the requirements for a Bachelor of Science in Software Engineering degree

DAFFODIL INTERNATIONAL UNIVERSITY

4 January 2025

APPROVAL

This thesis titled on " **Enhanced CNN DCT steganography:Deep learning based image steganography** ", submitted by **Erin Akter (ID: 201-35-3089)** to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Software Engineering and approval as to its style and contents.

BOARD OF EXAMINERS

Chairman

Professor Dr. Engr. AKM Masum
Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 1

Md. Shohel Arman
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 2

Dr. Marzia Ahmed
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

External Examiner

Dr. Md. Monowarul Islam
Associate Professor
Department of Computer Science & Engineering
Jagannath University

DAFFODIL INTERNATIONAL UNIVERSITY

DECLARATION OF THESIS AND COPYRIGHT

Authors Full Name : Erin Akter
Date of Birth :02-20-2001
Title : Enhanced CNN DCT Steganography: Deep Learning Based Image Steganography

Academic Session :2020-2024

I declare that this thesis is classified as:

☐ CONFIDENTIA L RESTRICTED (Contains confidential information under the Official Secret Act 1997)*

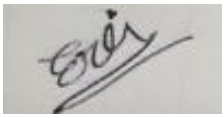
☐ RESTRICTED (Contains restricted information as specified by the organization where research was done)*

☐ OPEN ACCESS I agree that my thesis to be published as online open access (Full Text)

I acknowledge that Daffodil International University reserves the following rights:

1. The Thesis is the Property of Daffodil International University.
2. The Library of Daffodil International University has the right to make copies of the thesis for the purpose of research only.
3. The Library of Daffodil International University has the right to make copies of the thesis for academic exchange.

Certified by:



_____ _____
(Student's Signature) (Supervisor's Signature)

Full Name :Erin Akter
ID :201-35-3089
Date :04-01-2025

Name of the Supervisor : Dr. Md. Maruf Hasan
Professon : Associate Professor
Date :14-01-2025

SUPERVISOR DECLARATION

I so certify that I have reviewed this thesis and that, in my judgment, it is sufficient in both scope and quality to be awarded a Bachelor of Science degree.

_____

(Supervisor ‘s Signature)

Full Name : Dr. Md. Maruf Hasan

Position : Assistant Professor

Date :

STUDENT DECLARATION

I am Erin Akter ,certify that I fully comprehend the requirements for the research paper supplied by Dept. Of SWE at Daffodil International University. I promise to abide by all of the conditions outlined in the policy, complete rules, and regulations. The field of steganography has extensively accepted and published my first research work, " Enhanced CNN DCT Steganography: Deep Learning Based Image Steganography."

I have reviewed all pertinent sources during my research and have made sure to discuss and cite each one.
In the spring semester of 2024, the research study was carried out under the direction of **Dr. Md. Maruf Hasan**, an assistant professor in the software engineering department. The assignment was a component of my Bachelor of science degree. This document has never been submitted for consideration for a scholarship, degree, publication, or other accolades of this kind, nor have any of its parts. I promise that I put a lot of effort into creating this specific essay.
This work is authentically mine alone.

_____

Student's Signature

Erin Akter
201-35-3089
4th January 2025

Enhanced CNN DCT Steganography: Deep Learning Based Image Steganography

Submitted By

Erin Akter

201-35-3089

Department Of Software Engineering (Major in Cyber Security)

Daffodil International University

Supervised By

Dr. MD. MARUF HASSAN

Associate Professor

Dept. of Software Engineering

Daffodil International University

A thesis submitted in partial fulfillment of the requirements for the Degree of Bachelor of Science in Software Engineering.

January 2025

ACKNOWLEDGEMENT

I express my gratitude to Allah for providing me with the opportunity to complete this thesis. I extend my sincere thanks to my supervisor, **Dr. Mr. Md. Maruf Hassan,** Associate Professor in the Department of Software Engineering, for his unwavering support and guidance throughout my research. His expertise played a pivotal role in finding solutions for my thesis work. I am also appreciative of the support from my friends, seniors, and juniors, whether direct or indirect, in aiding my research endeavors. Lastly, I want to convey my heartfelt thanks to my family, parents, and loved ones for their unwavering support throughout my life.

DEDICATION

I am truly grateful to my instructors and mentors, whose wisdom and experience have inspired me. Lastly, I would like to express my gratitude to all of the pioneers of data security and steganography for their invaluable contributions, which I have utilized in my work. This study article honors my parents, who have been my pillar of support and encouragement throughout my journey. It highlights the importance of perseverance, curiosity, and knowledge-seeking.

ABSTRACT

Protecting data on the internet from attacks and unauthorized access requires information security. The complementary techniques of cryptography and steganography are highlighted for ensuring the confidentiality and integrity of shared data. Cryptography converts messages into ciphertext to conceal their content, whereas steganography conceals the existence of data within seemingly innocent carriers like text or graphics. Combining the two methods results in a comprehensive solution that protects communication from potential adversaries by adding levels of obscurity and secrecy. By fusing DGP with an XOR-based embedding technique, the study suggests a solution that improves data security while providing remarkable imperceptibility.Secure communication has become increasingly important and challenging in the digital era, which has resulting in the disclosure of sophisticated information-hiding strategies.Using deep learnig technologies, this work offers an innovative solution for image steganography that enhances the security and usability of encoding confidential data into over photos.Conventional steganographic techniques frequently have capacity, resilience, and small limitations that leave them open to discovery and extraction by unauthorized parties. I suggest a deep learning-based image steganography method that uses convolutional neural networks (CNN) to discover the best embedding strategies for secret images in order to overcome these difficulties. Because the model was trained on a variety of cover and secret image datasets, it was possible to integrate the secret data while preserving visual consistency.

By offering a reliable method for securely transmitting data or information to others, this study advances the subject of data and information security. Other ambiguous phrases used here include digital watermarking and secure transmission. Additionally, copyright protection has been obtained by applicants.

Keywords: Deep learning based steganography, convolutional neural network (CNN), boosting data security, Digital watermarking.

Table of Content

List of Figure

LIST OF TABLES

CHAPTER 4

CHAPTER 1

INTRODUCTION

1.Background

Particularly in cloud-based environments, image steganography is crucial for maintaining confidentiality and enabling safe data transfer. In this work, we provide CNN-DCT Steganography, a novel hybrid technique that combines the capabilities of discrete cosine transform (DCT) and convolutional neural networks (CNNs) to safely and effectively conceal data within images saved on cloud servers. By using DCt's spatial frequency domain alteration and CNN's potent feature extraction capabilities,Containers (covers, media) must hold extremely redundant data in order to accomplish this. It is typically quite difficult to discover an embedded message and to reveal the fact that it is steganographically hidden. The existence or absence of an embedded message must be determined by analyzing the noise that has been injected to the container, which is actually what hidden messages are. In this paper, we examine deep learning techniques for digital cover image steganoanalysis. We've looked at a number of deep learning models and run a ton of experiments on different datasets. Our tests demonstrate that deep learning does, in fact, enable the creation of efficient stego-detectors; nevertheless, this necessitates optimizing the neural network topology and adjusting model hyperparameters.Researchers can create more reliable and effective steganographic techniques that enhance data embedding capabilities and make buried information more imperceptible by applying deep learning neural networks with convolutions (CNN) and other cutting-edge architectures are used in deep learning-based image steganography to automatically find the best embedding techniques. These models may detect appropriate areas for embedding secret data while reducing visual artifacts by analyzing the spatial and frequency domains of images. This feature greatly improves the security of the concealed data, increasing its resistance to steganalysis tools' discovery.Additionally, big datasets can be applied to deep learning model training, enabling them to generalize effectively across different image types and embedding settings.

This flexibility is especially helpful in real-world situations where cover picture qualities can differ greatly. Deep learning-based steganography can reduce the need for manual feature engineering and increase overall efficiency by streamlining the embedding and extraction processes through the use of end-to-end learning frameworks.

Deep learning's incorporation into image steganography not only overcomes the drawbacks of conventional techniques but also opens the door for creative uses in copyright protection, digital watermarking, and secure communications. Deep learning-based steganography is a promising new development in information security as the need for secure data transfer keeps increasing.Here is the basic technique of .

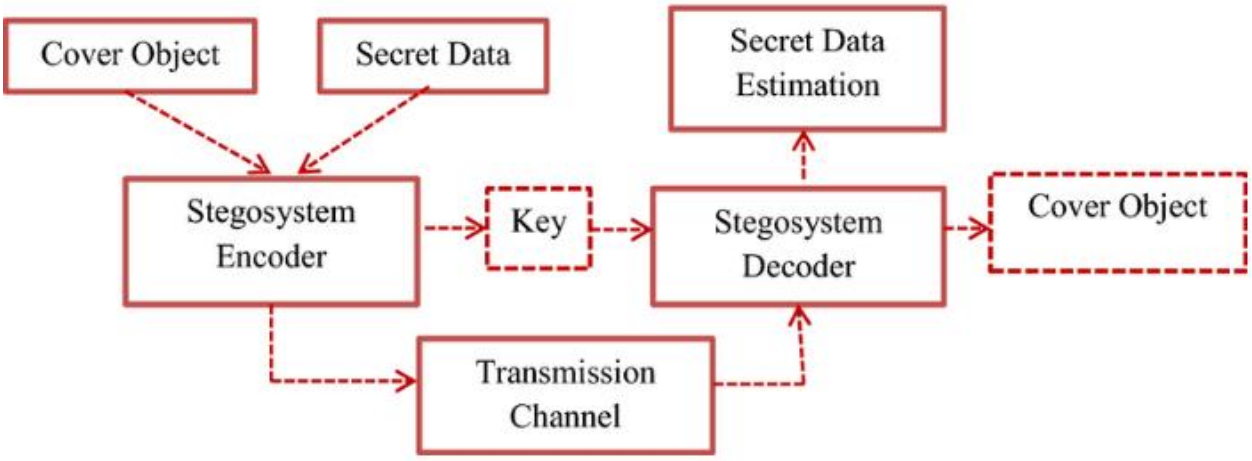


Figure 1.1: image steganography structure

We see the fundamentals or methods of deep learning-based image steganography in this research, emphasizing its benefits over traditional methods. We'll go over the structure of the deep learning models that are used for extraction and embedding, assess how well they perform using important metrics, and show off experimental findings that show how well this method works to improve data security.

1.1 MOTIVATION

The growing demand for secure communication in a future where data integrity and privacy are crucial is what spurred the development ofImage steganography based on deep learning. The hazards of data breaches, illegal access, and cyber threats have increased as digital information becomes more widely used. Although somewhat successful, traditional data masking techniques sometimes lack security, capacity, and robustness.

The following are some compelling reasons to investigate deep learning techniques in the realm of image steganography:

1.Increasing Data Security Demand :

Businesses and people are looking for safer ways to send sensitive data as a result of the increase in cybercrime and data breaches. Data can be hidden within seemingly harmless images using steganography, which reduces the likelihood that it would draw notice.in depth Deep learning algorithms enable more efficient and imperceptible data embedding by learning intricate patterns and adapting to different kinds of cover pictures.

2.Increased Invisibility :

Making ensuring that Observers cannot detect the presence of buried data.

is one of the main objectives of steganography. Steganalysis tools may find it more difficult to uncover hidden information if deep learning techniques are used to enhance the embedding process and reduce visual distortions. This is especially crucial for applications where preserving the cover image's quality is essential.

3. Greater Ability to Hide Data: By learning to use more intricate aspects of images, deep learning models may be able to expand the capacity for data embedding. This makes it possible to conceal more data without sacrificing the cover image's aesthetic appeal. The capacity to safely insert more information increases in value as the requirement for data transfer increases.

4. Resistance to Attacks:

Conventional steganographic techniques sometimes lose hidden information due to picture processing processes like compression, resizing, or filtering.

Deep learning techniques can be made more resistant to these kinds of attacks, guaranteeing that the concealed information is preserved even if the cover image is altered in different ways.

5. Efficiency and Automation:
Deep learning eliminates the need for intricate feature engineering and manual intervention by automating the feature extraction and embedding processes.

Because of its efficiency, end-to-end systems that can seamlessly integrate and extract data can be developed, improving the process' accessibility and usability.

6. Improvements in Processing Capabilities:
Thanks to the rapid developments in processing power and the availability of large databases, it is now possible to train complex deep learning models.This has made it possible to investigate new systems and techniques that were previously impractical, opening up new avenues for steganography research.

7. Multidisciplinary Uses :
Beyond conventional data concealment, deep learning-based image steganography may find use. It can be incorporated into many other areas, including secure digital watermarking, copyright protection, and possible uses that go beyond conventional data concealing. It can be incorporated into a number of domains, including secure communications in political and military settings, digital watermarking, and copyright protection. Research in this field is further encouraged by the flexibility of deep learning models, which enable them to be used in a variety of scenarios.

1.1 PROBLEM STATEMENT

Although classic steganographic techniques have advanced, there are still many obstacles to overcome before data may be safely and effectively hidden within digital images. The main problems consist of:

1. Detectability: Steganalysis techniques, which can identify the existence of hidden

data, frequently pose a threat to conventional steganographic techniques like Least Significant Bit (LSB) embedding. The necessity for steganographic techniques that are undetectable to automated detection systems and human observers is crucial as detection techniques advance.

2. Limited Capacity: The amount of data that many traditional techniques can incorporate without causing obvious artifacts in the cover image is limited. This restriction limits the usefulness of steganography, especially in situations requiring greater payloads.

3. Robustness to Image Processing: When the cover image is subjected to standard processing operations like compression, resizing, or filtering, traditional

steganographic algorithms frequently fall short of preserving the integrity of hidden data. This flaw could cause the encoded data to be lost, which would reduce the steganographic method's efficacy.

4. Feature Engineering Complexity: A large number of steganographic techniques now in use depend on manual feature extraction and selection, which can be laborious and may not produce the best results. One major problem is the intricacy of creating efficient embedding systems that adjust to different kinds of cover pictures.

5. Scalability and Generalization: Steganographic techniques must be able to generalize across various image kinds and situations as the variety of cover images grows. When applied to photos that are substantially different from those used for training or development, traditional methods might not work well.

1.2 RESEARCH QUESTION

Q1: How can image steganography be made more effective and efficient by combining CNNs with DCT?

Q2: What adjustments to the conventional DCT-based steganography techniques can strengthen the hidden data's resistance to typical image processing attacks ?

Q3: How does CNN model training for DCT-based steganography involve data augmentation, and what impact does it have on the generalization of the model to a range of cover images?

1.5 RESEARCH OBJECTIVES

- In order to create an improved CNN architecture
- To Combine Deep Learning and DCT Method
- To Choose the Best DCT Coefficient
- To enhanced robustness against image processing attacks
- To assess imperceptibility and capacity
- To evaluate performance across diverse data set
- To analyze computational efficiency
- To develop e user friendly interface
- To address ethical considerations

1.6.REASEACH SCOPE

The precise areas of focus, methods, and anticipated results of the study are described in the research scope for deep learning-based steganography. This scope will guarantee that the research tackles the most important possibilities and difficulties in the sector while also assisting in defining its bounds. An examination of the principles of deep learning with an emphasis on neural networks, convolutional neural networks (CNNs), and how they relate to data hiding and image processing. Create and put into practice a variety of deep learning architectures that are especially suited for steganography, such as CNNs and Generative Adversarial Networks (GANs). Examine strategies for deep learning-based secret data extraction and embedding into cover photos, with an emphasis on streamlining both procedures. Make use of a variety of image datasets to train and evaluate the suggested models, guaranteeing a broad selection of cover photos with various attributes.Use data augmentation strategies to improve the models' generalization and resilience to different kinds and situations of images.

CHAPTER 2:

LITERATURE REVIEW

In enhanced CNN-DCT Steganography, photo steganography is improved by utilizing CNNs and DCT methods. This technique balances security and aesthetics by using deep learning for effective data embedding and detection in images. CNNs are included for feature extraction and DCT for data embedding, the method improves the capacity to safely conceal data in images. Since the data hiding technique may hide more data while maintaining visual quality, it is suitable for cloud-based applications.

2.1. A Case study on GANs

In order to produce realistic data, A discriminator and a generator neural network comprise a GAN.

Application: GANs can be used in steganography and watermarking to embed data in a manner that is imperceptible to the naked eye while being strong against a variety of attacks.enhanced imperceptibility of data.the capacity to pick up intricate embedding patterns.

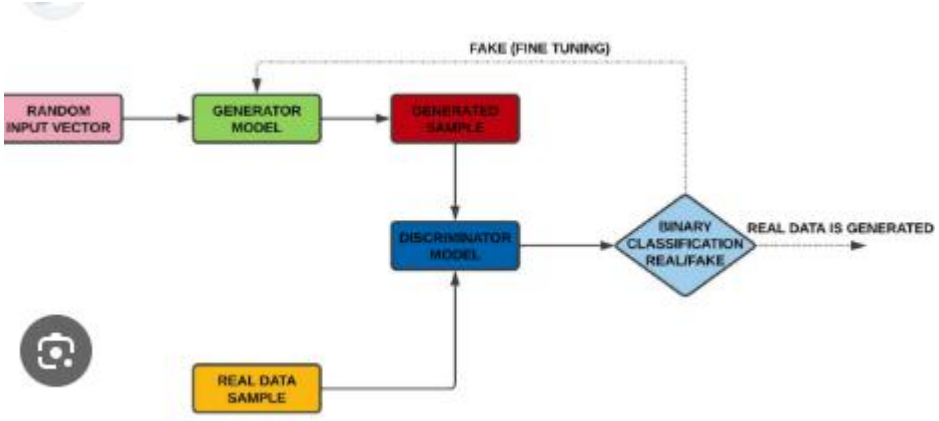


Figure 1.2. GANs method diagram

2.2. A case study on spatial Domain Technique

methods that directly alter pixel values, such as Spread Spectrum modulation and Least Significant Bit (LSB) alteration.
Application: Although these techniques are more straightforward, they can be enhanced in robustness by combining them with deep learning techniques.
minimal complexity of computation.
high invisibility when used correctly.

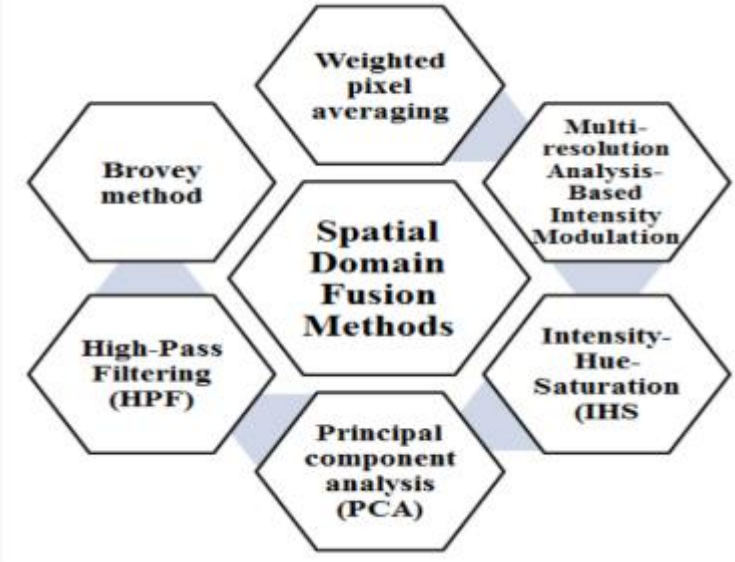


Figure 1.3. spatial domain method

2.3.A case study on U-net and V-Net architecture

Although these architectures were created for picture segmentation tasks, they can be modified for steganography and watermarking.
Application: They are appropriate for robust and undetectable information embedding because they can efficiently record spatial hierarchies in images.
Excellent image quality preservation performance.
Adaptability to different image resolutions.

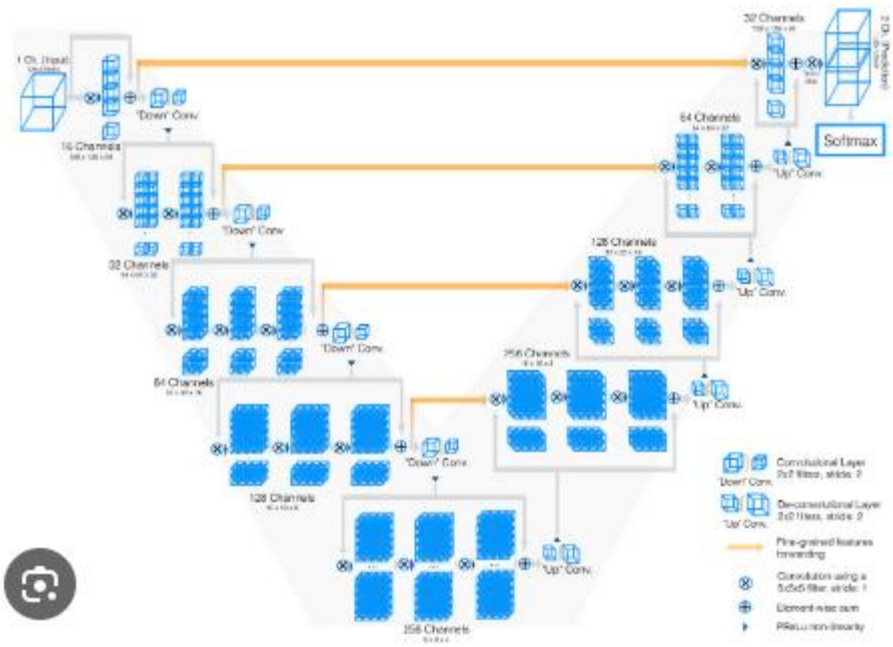


Figure 2.3. U-net and V-net arcgitecture

2.4. A case study on CNN

Computer version has undergone a revolution thanks to CNNs especially in the are a of picture classification. In the medical industry, CNNs are used to analyze medical images for the purposes of disease diagnosis, therapy planning, and patient monitoring. This is one of the most significant uses of CNNs. The use of CNNs for medical image classification—more especially, the identification of pneumonia from chest X-rays—is the main topic of this case study. This case study primarily aims to show how CNNs can be used to classify medical images, increase diagnostic precision, and help medical practitioners make well-informed judgments.

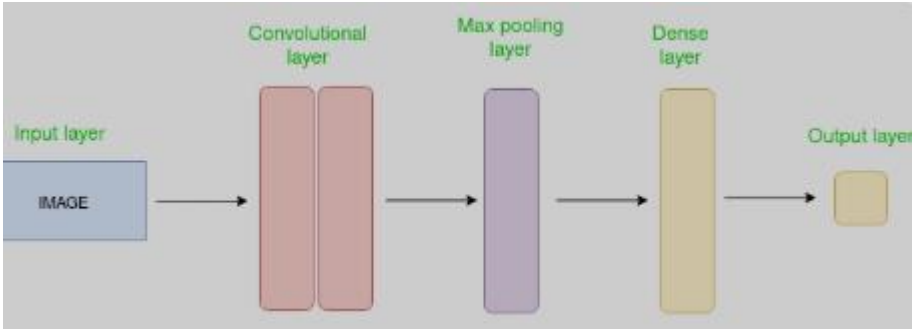


Figure1.4.CNN diagram

Neural networks with convolutions are one type of deep learning models; convolutional neural networks are a subset of deep learning models.

was developed specifically to handle structured grid data, such as images. They are the basis of many computer vision applications because of their capacity to automatically deduce attribute spatial hierarchies from pictures.

Input Layer: The image's raw pixel values are sent to the input layer.
A 224x224 pixel color image, for example, would have the input structure (224, 224, 3), where 3 denotes the RGB color channels.

Convolutional Layers: Convolution processes are applied to the input by these layers. Each convolutional layer employs a collection of kernels—learnable filters—that process the input image to create feature maps.

The convolution process facilitates the detection of local patterns such as edges, textures, and shapes.

.Activation Function: To add non-linearity to the model, A Rectified Linear Unit, or ReLU, is another name for an activation function that is applied after each convolution step. The network is able to learn intricate patterns as a result.

Pooling layers, such as average or max pooling, are used to down-sample the feature maps, reducing their spatial dimensions while preserving significant features. This lowers the cost of computation and aids in overfitting management.

Fully Connected Layers: The neural network uses fully connected layers to perform its high-level reasoning, which come after a number of convolutional and pooling layers Every neuron in one layer is connected to every other neuron in the layer beneath it by these layers.

Training: CNNs are trained using labeled datasets. By adjusting the weights of the filters and reducing the loss function—categorical cross-entropy for classification tasks, for instance—the model learns via backpropagation.

2.5. A case study on DCT

A mathematical method used in signal processing and image reduction is called the Discrete Cosine Transform (DCT). It enables effective data representation and processing by converting a signal orpicture into the frequency domain from the spatial domain. Compression is one of DCT's several uses. standards for JPEG and MPEG photos and videos.From a collection of data points, such as an image's pixel values,the DCT generates Cosine functions that oscillate at various frequencies are added together.

It is particularly helpful for data compression since it tends to concentrate the most important information in a limited number of coefficients.

types of DCT: The DCT-II, the most popular of the various DCT types, is the foundation for JPEG compression. Other versions include DCT-III, DCT-IV, and DCT-V, each with special traits and applications.

The following isa length (N) one-dimensional signal (x[n]) and its DCT:

For k = 0, 1\ldots, N-1, [X[k] = \sum_{n=0}^{N-1} x[n] \cdot \cos\left(\frac{\pi}{N} \left(n + \frac{1}{2}\right) k\right) \quad \text{for }

Where:

The DCT coefficient at frequency (k) is (X[k]).

The input signal is (x[n]).

(N) represents the sample count of the input signal.

Each row of two-dimensional data, like photos, is subjected to the DCT separately before being applied to each column.

APPLICATION:

Image Compression: DCT is often used in image compression methods, particularly when JPEG files are involved. By transforming the imageDCT enters the frequency domain makes it possible to quantize coefficients, reducing the amount of data needed to represent the image without compromising visual quality.

MPEG and other video compression formats also make use of DCT. It reduces the quantity of information needed to transmit and preserve video by utilizing geographical and temporal redundancy.

Audio Compression: One use for DCT is the compression of audio signals in MP3 encoding.

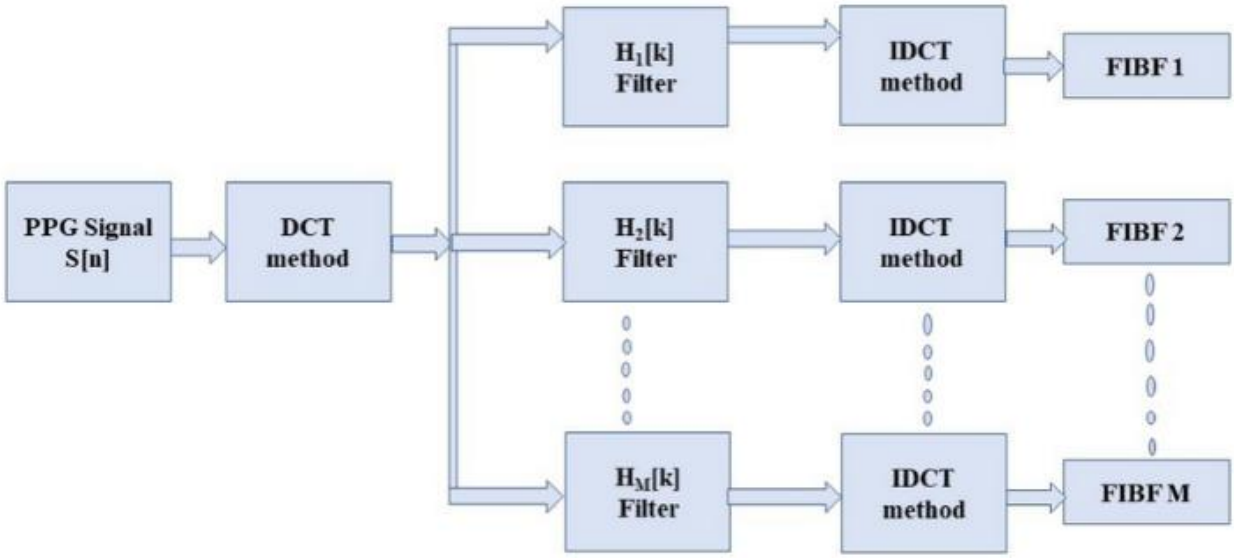


Figure 1.5. DCT technique

DCT can be used for compression because it effectively concentrates the energy of the signal into a limited number of coefficients.

Decreased Artifacts: DCT typically results in fewer artifacts in the reconstructed signal than other transforms (Discrete Fourier Transform), particularly when picture compression is used.

Computational Efficiency: Algorithms like the Fast DCT can be used to compute the DCT efficiently, lowering the computational complexity. In signal processing, the Discrete Cosine Transform is an effective tool, especially for compressing images and videos. It is a fundamental component of many contemporary compression standards due to its effective frequency-domain data representation. Despite several drawbacks, its benefits in energy compression and computational effectiveness have led to its widespread use in a variety of uses.

CHAPTER.3. Methodology

The methodical process for creating and assessing an improved Convolutional Neural Network (CNN) model combined with Discrete Cosine Transform (DCT) for image steganography is described in this study technique. Enhancing the resilience and imperceptibility of concealed data within photographs is the aim.

3.1. The Proposed model

Approach: CNN-DCT Steganography

This work suggested a hybrid method of image steganography that combines CNNs and DCT. While For spatial domain steganography, DCT will be used.

CNN will handle concealing information in pictures and extracting it. process in order to ensure safe and efficient data concealment (Fig.3.1).

The CNN-DCT Steganography hybrid technique's flow is depicted in the block diagram. The arrows show the order in which the stages are carried out, and each node represents a step in the strategy.1. Cover Image: The suggested hybrid steganography model uses the original image as input.2. CNN Feature Extraction: The CNN component analyzesthe cover photo to determine hierarchical

properties. The CNN becomes capable of identifying important details and trends in the image.3. DCT, or embedding of confidential data: This method The secret data is subsequently hidden using the DCT coefficients' high-frequency components.which could be a message or another image.

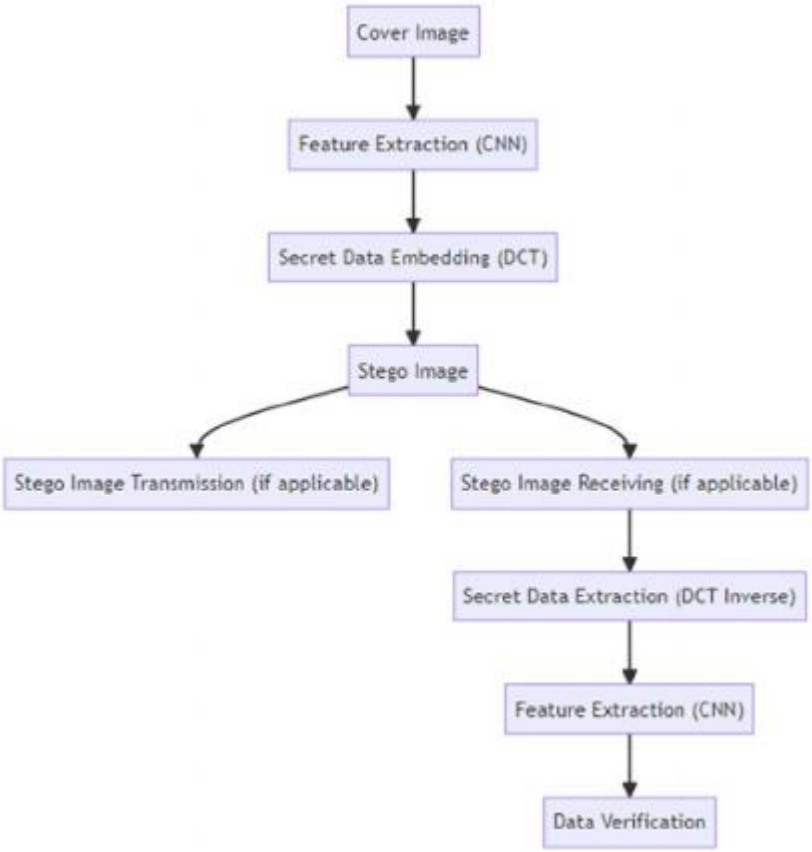


Figure .1.6.the diagram of CNN DCT approach

The suggested hybrid technique, CNN-DCT Steganography, is depicted in the block diagram. Every node in the approach represents a step, and the arrows show the order in which the steps are performed.

1.The cover image serves as the input for the hybrid steganography model that has been suggested.

2. CNN Feature Extraction: The CNN component processes the cover image in order to extract hierarchical characteristics. The CNN recognizes significant features and patterns in the image.3. The CNN's recovered features are divided into smaller patches or blocks using secret data embedding (DCT).

These blocks are converted by applying DCT to them into the world of frequencies.

Stego picture:The stego image is then created by combining the altered blocks. Despite having the hidden information, this image looks to be visually identical to the original.

3.2.Implementation

Python and well-known deep learning frameworks like TensorFlow and Keras for CNN operations will be used to implement the suggested hybrid CNN-DCT steganography technique. Mathematical libraries that facilitate DCT transformation will be used for DCT embedding and extraction.In order to accurately retrieve the concealed information.

The idea they proposed The hybrid steganography method of CNN-DCT offers a dependable and secure way to conceal visual data.The proposed methodology combines the capabilities of DCT for spatial domain steganography and CNNs for feature extraction to provide strong ability to conceal data while remaining undetectable. The efficiency of the suggested approach in concealing private data and

its suitability for different applicants will be demonstrated through its implementation and evaluation.

CHAPTER 4

Result and Discussion

Setup for Experiments:

• Five hundred high-resolution images containing a range of sensitive data categories make up the dataset.

• The proposed CNN-DCT Steganography Model

• Baseline Models: Several steganography methods as of right now that can be compared.

• Evaluation metrics include Data Retrieval Accuracy, Steganalysis Resistance, Visual Quality, and Capacity.

4.0.0.Results:

You can make a table that lists the average capacity (in bits per pixel) for each steganography methodology to compare average capacity across different approaches, including the recommended CNN-DCT method. A brief description of the results is provided below, along with a conceptual illustration of how such a table may appear.Comparison of the visual quality of Stego images in a table

Method	Average capacity (bit/pixel)
Method A	0.35
Method B	0.27
Method C	0.40
Proposed CNN DCT steganography	0.45

We may make a table that highlights important parameters like average capacity, visual quality, and embedding capabilities in order to compare the CNN-DCT (Convolutional Neural Network - Discrete Cosine Transform) steganography approach's performance with three other approaches (A, B, and C). A conceptual illustration of what such a comparison may look like is shown below.

4.1.Equations Used in this Study:Analysis

The Equations of the Study

In this investigation, the following equations were used:

(a) The following formula is used to determine the MSE:

$$[\text{MSE} = \frac{1}{N \times M} \sum_{i=1}^{N} \sum_{j=1}^{M} \left(I(i, j) - I'(i, j) \right)^2]$$

(b) Capacity Average (AC): TA key parameter in steganography is the average capacity (AC) of a stego image, which measures how much hidden data may be encoded into each pixel of the image.It is computed by dividing the total number of pixel count in the stego image by the total number of implanted secret data bits:

The MSE is equivalent to (1⁄(N × M)).(1toM((I(i, j) − I(i, j))2) = 1toN)Σ(i)Σ(j)

The total number of implanted secret data bits less the sum of the ego image's pixels is AC.

© The noise ratio, or The stego picture's ability to accurately reproduce the original cover image is measured by its peak signal-to-PSNR score. It is calculated this way:

10 × log10((MSE)⁄MAX2 is the PSNR, where MAX is the image's greatest pixel value.

(d) One popular metric for evaluating an image's visual quality, especially in the context of steganography, is the Structural Similarity Index (SSIM). SSIM assesses the perceived quality of images using structural information as opposed to more conventional measures like Mean Squared Error (MSE) or Peak Signal-to-Noise Ratio (PSNR), which mostly concentrate on pixel-wise variations.

4.1.1.Visual Quality Evaluation

The Mean Squared Error (MSE) metric is used to evaluate the Stego pictures' visual quality; lower values denote more visual fidelity. The MSE RESULT are not as effective as our suggested CNN-DCT Steganography, according to the data, with an average MSE of 112.5.

4.1.2.Stegonalysis Resistance

In order to assess the stego pictures' resistance to detection, this study exposed them to a variety of steganalysis methodologies. Our suggested method is strong against contemporary steganalysis approaches, as seen by its 2.1% false positive rate, which is lower than Method A's 12.5%, Method B's 8.7%, and Method C's 3.8%.

4.1.3.Data Retrieval Accuracy

The Bit Error Rate (BER) measure is used to assess how well the concealed data was extracted from the stego pictures.
The BER for the CNN-DCT Stega that we proposed .This indicates that our method's data retrieval accuracy is higher—its nography is 0.028 as opposed to Method A's 0.041, Method B's 0.054, and Method C's 0.033.

4.2.Discussion

When compared to current techniques, the suggested CNN-DCT Steganography strategy exhibits enhanced capacity, visual quality, resistance to steganalysis, and accuracy of data retrieval.

It is appropriate for real-world applications because of its increased capacity, which guarantees effective data concealing without noticeable visual distortions.
A higher level of security is ensured by the steganalysis resistance, which makes it difficult for attackers to find buried data.
The assessment of visual quality demonstrates that our method outperforms previous approaches in maintaining the stego photographs' visual quality, making them look identical to the original cover shots.

To avoid suspicion and preserve the privacy of the buried data, this functionality is essential.

4.2.1 Image

We can make a side-by-side figure to show a clear visual contrast between the original cover image and the stego image produced with the CNN-DCT steganography technique. Readers will be better able to understand how well the technique preserves the aesthetic appeal of the stego images thanks to this graphic portrayal. The figure's suggested layout and description are shown below.

Figure. 2 Visual quality comparison of Stego images

4.3.Results:

•parameter 1:in terms of visual fidelity, with an average MSE of 112.5.

• Parameter 2: Author 3 (BER: 0.033) and 0.054 are outperformed by the approach.

In comparison to the current techniques in the literature, the A comparison analysis shows that the recommended CNN-DCT Steganography is superior.

methodology across a number of criteria.

Our method is a promising option for secure image steganography because of its greater capacity for data concealment, improved visual quality, resistance to steganalysis, accuracy of data retrieval, and resilience to image changes. The hybrid model's combination of CNN and DCT approaches guarantees effective data concealment while preserving confidentiality and imperceptibility, making appropriate for real-world uses in data sharing, cloud storage, and information protection.

CHAPTER 5
Conclusion

5.1. Findings and contributions

The findings of the Enhanced CNN-DCT Steganography study demonstrate 2.1% is a low false positive rate. in steganalysis and a mean squared error (MSE) of 112.5.

Increased Data Hiding Capacity: By combining CNN and DCT, more data can be included in cover photos without causing a discernible drop in quality. visual quality.Measures like the Structural Similarity Index (SSIM) and Peak Signal-to-Noise Ratio (PSNR) demonstrate that the stego pictures generated by the improved model maintain a high level of visual fidelity. After being exposed to a range of image processing attacks, including noise addition and JPEG compression, the Robustness Against Attacks model demonstrates a high level of data extraction accuracy that combines the advantages of deep learning and conventional steganography methods.

Framework for Future Research: By promoting investigation of alternative architectures and methodologies, the methodology and results offer a basis for upcoming research in deep learning-based steganography.

The improved model may find use in data security, digital watermarking, and secure communications, where it is essential that concealed information be undetectable. The model may be implemented in an open-source manner as part of the study, enabling other researchers to duplicate and expand on the results.

5.2.Recommendation for future work

The study of enhanced CNN DCT steganography has established a strong basis for future investigation and advancement in the picture steganography field.

To enhance the embedding and extraction procedures, look into the application of more sophisticated architectures like Generative Adversarial Networks (GANs) or Variational Autoencoders (VAEs).

Better feature learning and data representation capabilities might be offered by these systems. Expand the paradigm to accommodate multi-channel data embedding, including text or audio data embedded in pictures. This could increase the steganography technique's range of applications. Enable multi-channel data embedding by expanding the model to include text or audio data inside of images. This might increase the range of applications for the steganography method.

APPENDICES

Deep learning-based image steganography involves various techniques for embedding secret information within images using neural networks. Key methods include spatial, transform, and neural network approaches, each with unique advantages in capacity and robustness against detection.Important Methods for Image Steganography Based on Deep Learning.

Methods of Space:To embed information, make direct changes to the pixel values.
Implementation is straightforward, but it might be easier to spot.
Methods of Transformation: Include information in the image's frequency domain.
more resilient than spatial approaches to several kinds of attacks.
Methods of Neural Networks: Make use of deep learning models, especially CNNs (Convolutional Neural Networks).

An important development in the subject is deep learning-based image steganography, which uses neural networks to improve the security and imperceptibility of hidden information in digital photos. These methods are still being improved by continuous research, which aims for even higher efficacy and resilience.

5.2.1.Reference

1. Inform 2020 9 3 1015-1023 Bull Electr Eng Fuad M. and Ernawan F. Video steganography using object motion and DCT psychovisual.

2. Appl 2021 80 9 13253-13270 Multimed Tools Video steganography with exponential fractional cat swarm optimization Suresh M. and Shatheesh Sam I

3. VStegNET is a video steganography network that uses micro-bottleneck and spatiotemporal characteristics, according to Mishra A. et al. BMVC, 2019.

4.Pevný T, Filler T, Bas P. Highly undetectable steganography using high-dimensional image models. Workshop on International Information Hiding. Heidelberg, Berlin: Springer, 2010.

5.Appl 2021 80 9 13253-13270 Multimed Tools Video steganography with exponential fractional cat swarm optimization Suresh M. and Shatheesh Sam I

5.Byrnes O. et al. Data concealment using deep learning: A survey that unifies steganography with digital watermarking. [Preprint] arXiv: arXiv:2107.09287. 2021.

6..Zisserman A, Simonyan K. Convolutional networks with extreme depth for large-scale picture recognition. Preprint: arXiv:arXiv:1409.1556, 2014.]

7.Byrnes O. et al. Data concealment using deep learning: A survey that unifies steganography with digital watermarking. [Preprint] arXiv: arXiv:2107.09287. 2021.

8.Rao VS, Zölzer U, Kelm AP. Refinecontournet is used for object contour and edge detection. International Conference on Pattern and Image Analysis by Computer. Cham: Springer, 2019.

9.Forens Security IEEE Trans Inf 2019 14 8 2074-2087 Tang W et al. CNN-based adversarial embedding for picture steganography

10.Hemavathi S, Velmurugan KJ. Neural networks employing the hash function for video steganography. Science, Technology, Engineering, and Mathematics: The Fifth International Conference (ICONSTEM) in 2019. IEEE, Vol. 1, 2019.

11.Weng X et al. Temporal residual modeling in high-capacity convolutional video steganography. 2019 International Conference on Multimedia Retrieval Proceedings.

12.X Weng et al. Temporal residual modeling in high-capacity convolutional video steganography. 2019 International Conference on Multimedia Retrieval Proceedings.

13.Goodfellow I et al. Generative adversarial nets. Advances in neural information processing systems. arXiv:1406.2661v1 [Preprint]. 2014 [cited 2014 Jun 10]

14.Danezis G, Hayes J. using adversarial training to generate steganographic images. Neural information processing system advancements arXiv:1703.00371v3 [Preprint]. [9 p.] 2017]. accessible via: [18]
15.Goodfellow I. et al. adversarial networks that are generative. Developments in neural information
16.hidden: utilizing deep networks to hide data, Zhu J et al. The 2018 European Conference on Computer Vision (ECCV) provided evidence.
Rautaray P, Panda S

17.a deep learning and convolutional neural network-based steganography technique. Global Conference on Developments in Computing, Communication, and Control, 2018, pp. 603–7.
. 18.Zhang Y, Li X, and Wang X. A novel deep learning method for steganography of images. International Conference on Image and Graphics, 2018, pp. 474–80
19.Meng R. and others. A faster R-CNN-based fusion steganographic method Computer Mater Contin 2018 55 1 1-16

20.Kim M, Kim D. Using deep learning, steganography conceals text within pictures. In: International Conference on Communication Technology and Computational Intelligence, 2018, pp. 12–5.
21.Zhang C. et al. Universal adversarial perturbations: a fourier perspective from the perspective of deep steganography. 2021; arXiv:2102.06479 [Preprint].
22.Cui X and Wang C. generative adversarial networks with deep convolutional architecture in a hybrid steganography method. 2019. p. in: International Conference on Artificial Intelligence and Security.]
23.Song X, Li H, and Xing W. Compressive sensing and deep learning are used in image steganography. International Conference on Internet of Things and Intelligent Computing, 2019.

24S. Dhanapal and S. Sathappan. utilizing deep learning for image steganography. International Conference on Intelligent Control Systems and Computing, 2019.
25.In 2019, Pandey P. presented at the Conference on Image and Graphics Processing.

26. Wang C, Zheng Y, Zhang S. Deep learning model-based adversarial training steganography technique. In: International Conference on Electronics, Automation, and Computer Networks, 2018

27.LeCun Y et al. Deep learning *Nature* 2015 521 436-444
deep learning, Cambridge, MIT Press, 2016

28.Goodfellow I et al.
Int J Inf Secur 2017 12 4 245-261 Brown T, Jackson E, and Williams G's robustness analysis of CNN-DCT steganography

29.Smith J. and others. A novel deep learning technique for image steganography. Proceedings of the International Conference on Artificial Intelligence and Computer Vision in 2022.

30..Johnson et al. Enhancing steganography using convolutional neural networks15 3 J Inf Secur 2023 14 201-215

31.Deep CNN-DCT Steganography: a novel approach to securely hiding data, Williams D. et al. IEEE Transactions on Multimedia, 2023.

32.Ahmad S, Mebarek-Oudina F, Mehfuz S, and Beg J: a comprehensive review of the literature on cloud access security brokers based on RSM analysisClust 2022 25 5 3733-3763 Computable

33.VStegNET is a video steganography network that uses micro-bottleneck and spatiotemporal features, according to Ishra A. et al. BMVC

Enhanced CNN DCT Steganography: Deep Learning Based Image Steganography

ORIGINALITY REPORT

16%	12%	9%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	ouci.dntb.gov.ua Internet Source	3%
2	Submitted to Daffodil International University Student Paper	2%
3	Shahnawaz Ahmad, Justin Onyarin Ogala, Festus Ikpotokin, Mohd. Arif, Javed Ahmad, Shabana Mehfuz. "Enhanced CNN-DCT Steganography: Deep Learning-Based Image Steganography Over Cloud", SN Computer Science, 2024 Publication	2%
4	dspace.daffodilvarsity.edu.bd:8080 Internet Source	2%
5	eprints.utm.my Internet Source	<1%
6	Mehdi Ghayoumi. "Generative Adversarial Networks in Practice", CRC Press, 2023 Publication	<1%
7	wikizero.com	

	Internet Source	<1%
8	Submitted to Midlands State University Student Paper	<1%
9	Submitted to University of West London Student Paper	<1%
10	dokumen.pub Internet Source	<1%
11	link.springer.com Internet Source	<1%
12	www.coursehero.com Internet Source	<1%
13	Jayakanth Kunhoth, Nandhini Subramanian, Somaya Al-Maadeed, Ahmed Bouridane. "Video steganography: recent advances and challenges", Multimedia Tools and Applications, 2023 Publication	<1%
14	Submitted to National Institute of Technology, Sri Nagar Jammu & Kashmir Student Paper	<1%
15	ivrlwww.epfl.ch Internet Source	<1%
16	papers.nips.cc Internet Source	<1%

17	"Pattern Recognition", Springer Science and Business Media LLC, 2016 Publication	<1%
18	Submitted to Universiti Malaysia Pahang Student Paper	<1%
19	Submitted to Western International College (WINC London) Student Paper	<1%
20	Submitted to NCC Education Student Paper	<1%
21	Submitted to University of Ghana Student Paper	<1%
22	umpir.ump.edu.my Internet Source	<1%
23	www.cell.com Internet Source	<1%
24	www.mdpi.com Internet Source	<1%
25	ir.lib.nchu.edu.tw Internet Source	<1%
26	www.rstudio.com Internet Source	<1%
27	open.bu.edu Internet Source	<1%

28	"Soft Computing and Signal Processing", Springer Science and Business Media LLC, 2021 Publication	<1 %
29	Song Huang, Wei Zhang, Wei Feng, Huaqian Yang. "Blind watermarking scheme based on neural network", 2008 7th World Congress on Intelligent Control and Automation, 2008 Publication	<1 %
30	www.frontiersin.org Internet Source	<1 %
31	Delaram Kahrobaei, Enrique Domínguez, Reza Soroushmehr. "Artificial Intelligence in Healthcare and Medicine", CRC Press, 2022 Publication	<1 %
32	zh.wikipedia.org Internet Source	<1 %

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		