ADDING WATERMARK TO MULTIPLE IMAGES USING OPENCV AND PYTHON

K.VENKATESH, MASABATHULA.TARAKA RAMANJANEYULU

Assistant Professor MCA, DEPT, Dantuluri Narayana Raju College, Bhimavaram-534202, Andhra Pradesh
Email id : kornalavenkatesh@gamail.com

PG student of MSC(CS) D.N.R. COLLEGE, P.G. COURSES (AUTONOMOUS), BHIMAVARAM-534202.
Email id : tarakamasabathula@gmail.com

ABSTRACT

Add Watermark to Multiple Images with OpenCV and Python it provides a step-by-step guide on adding watermarks to multiple images using OpenCV and Python. This abstract provides an overview and summarizing its objectives, the tools used, and the key steps involved in the process.

This project begins by importing the necessary libraries, including OpenCV and NumPy. Images are loaded and processed using OpenCV, and the watermark is prepared as either an image or text. The watermark is then overlaid onto the target images with appropriate positioning, opacity, and scaling. The final watermarked images are saved to the desired location.

The implementation of this project is an invaluable tool for photographers, content creators, and businesses aiming to protect their visual assets, establish branding, or provide additional context to their images. Additionally, the use of OpenCV ensures that the watermarking process is efficient, reliable, and customizable to meet specific requirements.

Overall, this project showcases a practical and effective approach to adding watermarks to multiple images using OpenCV in Python, addressing the need for image protection and branding in the digital age..

1 INTRODUCTION

The recent growth in computer networks, and more specifically, the World Wide Web, has allowed multimedia data such as images to be easily distributed over the Internet. However, many publishers may be reluctant to show their work on the Internet due to a lack of security. Images can be easily duplicated and distributed without the owner's consent. Digital watermarks have been proposed as a way to tackle this issue. A digital watermark is an invisible signature embedded inside an image to show authenticity and ownership. An effective digital watermark should be perceptually invisible to prevent obstruction of the original image. It should be statistically invisible to prevent detection, and it should also be robust to many image manipulations, such as filtering, additive noise, and compression.

Several watermarking techniques have been proposed. Some methods embed the watermark in the spatial domain of the image [1,2]. Other watermarking techniques use transform methods, such as the FFT [3], DCT [4,5], or the Wavelet transform [6] to embed the watermark. Recent developments have also seen the use of the Human Visual System to improve watermark performance [7,8].

With the exception of [9], most watermarking methods do not employ error-correction. This project report proposes a new watermarking scheme using convolutional codes and compares its performance to a method without coding. Performance is based upon its robustness to common image attacks such as additive noise, JPEG compression, and image resizing. Section 2 gives a description of the proposed watermarking method, and Section 3 shows the results. Section 4 explains the potential applications of watermarking, and Section 5 gives a conclusion to this project report.

1.1 THE DIGITAL WATERMARK

Digital watermarking is a technology for embedding various types of information in digital content. In general, information for protecting copyrights and proving the validity of data is embedded as a watermark.

A digital watermark is a digital signal or pattern inserted into digital content. The digital content could be a still image, an

audio clip, a video clip, a text document, or some form of digital data that the

creator or owner would like to protect. The main purpose of the watermark is to identify who the owner of the digital data is, but it can also identify the intended recipient.

Why do we need to embed such information in digital content using digital watermark technology? The Internet boom is one of the reasons. It has become easy to connect to the Internet from home computers and obtain or provide various information using the World Wide Web (WWW).

All the information handled on the Internet is provided as digital content. Such digital content can be easily copied in a way that makes the new file indistinguishable from the original. Then the content can be reproduced in large quantities.
For example, if paper bank notes or stock certificates could be easily copied and used, trust in their authenticity would greatly be reduced, resulting in a big loss. To prevent this, currencies and stock certificates contain watermarks. These watermarks are one of the methods for preventing counterfeit and illegal use.

Digital watermarks apply a similar method to digital content. Watermarked content can prove its origin, thereby protecting copyright. A watermark also discourages piracy by silently and psychologically deterring criminals from making illegal copies.

1.2 Principle of digital watermarks

A watermark on a bank note has a different transparency than the rest of the note when a light is shined on it. However, this method is useless in the digital world.Currently there are various techniques for embedding digital watermarks. Basically, they all digitally write desired information directly onto images or audio data in such a manner that the images or audio data are not damaged. Embedding a watermark should not result in a significant increase or reduction in the original data.
Digital watermarks are added to images or audio data in such a way that they are invisible or inaudible Ñ unidentifiable by human eye or ear. Furthermore, they can be embedded in content with a variety of file formats. Digital watermarking is the content protection method for the multimedia era.

1.3 Materials suitable for watermarking

Digital watermarking is applicable to any type of digital content, including still images, animation, and audio data. It is easy to embed watermarks in material that has a comparatively high redundancy level ("wasted"), such as color still images, animation, and audio data; however, it is difficult to embed watermarks in material with a low redundancy level, such as black-and-white still images.

To solve this problem, we developed a technique for embedding digital watermarks in black-and-white still images and a software application that can effectively embed and detect digital watermarks.

2. LITERATURE SURVEY AND RELATED WORK

2.1 Watermarks can be visible or invisible:

1.Visible watermarks are designed to be easily perceived by a viewer (or listener). They clearly identify the owner of the digital data, but should not detract from the content of the data.

2.Invisible watermarks are designed to be imperceptible under normal viewing (or listening) conditions; more of the current research focuses on this type of watermark than the visible type.
Both of these types of watermarks are useful in deterring theft, but they achieve this in different ways. Visible watermarks give an immediate indication of who the owner of the digital work is, and data watermarked with visible watermarks are not

of as much usefulness to a potential pirate (because the watermark is visible). Invisible watermarks, on the other hand, increase the likelihood of prosecution after the theft has occurred. These watermarks should therefore not be detectable to thieves, otherwise they would try to remove it; however, they should be easily detectable by the owners.

A further classification of watermarks is into fragile, semi-fragile or robust:

1.A fragile watermark is embedded in digital data to for the purpose of detecting any changes that have been made to the content of the data. They achieve this because they are distorted, or "broken", easily. Fragile watermarks are applicable in image authentication systems.

2. Semi-fragile watermarks detect any changes above a user-specified threshold.

3. Robust watermarks are designed to survive "moderate to severe signal processing attacks".

Watermarks for images can further be classified into spatial or spectrum watermarks, depending on how they are constructed:

1.Spatial watermarks are created in the spatial domain of the image and are embedded directly into the pixels of the image. These usually produce images of high quality but are not robust to the common image alterations.

2.Spectral (or transform-based) watermarks are incorporated into the image's transform coefficients. The inverse-transformed coefficients form the watermarked data.

Perceptual watermarks are invisible watermarks constructed from techniques that use models of the human visual system to adapt the strength of the watermark to the image content. The most effective of these watermarks are known as image-adaptive watermarks.

Finally, blind watermarking techniques are techniques that are able to detect the watermark in a watermarked digital item without use of the original digital item.

2.2 Features of a Good Watermark

The following are features of a good watermark:

1.It should be difficult or impossible to remove a digital watermark without noticeably degrading the watermarked content. This is to ensure that the copyright information cannot be removed.

2.The watermark should be robust. This means that it should remain in the content after various types of manipulations, both intentional (known as attacks on the watermark) and unintentional (alterations that the digital data item would undergo regardless of whether it contains a watermark or not). These are described below. If the watermark is a fragile watermark, however, it should not remain in the digital data after attacks on it but should be able to survive certain other alterations (as in the case of images, where it should be able to survive the common image alteration of cropping).

3.The watermark should be perceptually invisible, or transparent. That is, it should be imperceptible (if it is of the invisible type). Embedding the watermark signal in the digital data produces alterations, and these should not degrade the perceived quality of the data. Larger alterations are more robust, and are easier to detect with certainty, but result in greater degradation of the data.

4.It should be easy for the owner or a proper authority to readily detect the watermark. "Such Decodbility without requiring the original, unwatermarked [digital document or] image would be necessary for efficient recovery of property and subsequent prosecution".

Further properties that enhance the effectiveness of a watermarking technique, but which are not requirements are

5.Hybrid watermarking refers to the embedding of a number of different watermarks in the same digital carrier signal.

Hybrid watermarking allows intellectual property rights (IPR) protection, data authentication and data item tracing all in one go.

6.Watermark key: it is beneficial to have a key associated with each watermark that can be used in the production, embedding, and detection of the watermark. It should be a private key, because then if the algorithms to produce, embed and detect the watermark are publicly known, without the key, it is difficult to know what the watermark signal is. The key indicates the owner of the data.

In 1997, a counterfeiting scheme was demonstrated for a class of invertible, feature-based, frequency domain, invisible watermarking algorithms. This counterfeiting scheme could be used to subvert ownership claims because the recovery of the digital signature from a watermarked image requires a comparison with an original. The counterfeiting scheme works by first creating a counterfeit watermarked copy from the genuine watermarked copy by effectively inverting the genuine watermark. This inversion creates a counterfeit of the original image which satisfies two properties: (a) a comparison of the decoded versions of both the original and counterfeit original yields the owner's (authorized) signature, and (b) a comparison of decoded versions of both the original and counterfeit original yield the forged (inverted) signature. This, the technique of establishing legitimate ownership recovering the signature watermark by comparing a watermarked image with the original image breaks down. It can be shown that both the legitimate signature and counterfeiter's signature inhere in both the watermarked and counterfeit watermarked copies. Thus, while it may be demonstrated that at least one recipient has a counterfeit watermarked copy, it cannot be determined which it is.

This research suggests that not all watermarking techniques will be useful in resolving ownership disputes in courts of law. There will likely be non-commercial applications, or those with limited vulnerability to theft, where "good enough watermarking" will suffice. More sensitive applications may require non-invert able or non-extracting watermarking techniques. These issues are under consideration at this writing.

3 EXISTING SYSTEM

Watermarking is the process that embeds data called a watermark or digital signature or tag or label into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object. The object may be an image or audio or video. A simple example of a digital watermark would be a visible “seal” placed over an image to identify the copyright. However, the watermark might contain additional information including the identity of the purchaser of a particular copy of the material. In general, any watermarking scheme (algorithm) consists of three parts: [19] • The watermark • The encoder (marking insertion algorithm) • The decoder and comparator (verification or extraction or detection algorithm) Each owner has a unique watermark or an owner can also put different watermarks in different objects the marking algorithm incorporates the watermark into the object. The verification algorithm authenticates the object determining both the owner and the integrity of the object.

4 PROPOSED WORK AND ALGORITHM

DCT is a transform domain-based watermarking scheme that ensures the imperceptibility of the watermarked image and also provides robustness under various attacks and noise addition [11]. We have added two images into a single host image by DCT fashion. Our algorithm has a total of six steps. Among these steps, four of them are key generation, pre-processing, watermark encryption, and embedding steps that are executed on the sender side. Another two steps are watermark extraction and decryption that are executed on the receiver side. In the key generation step, a random binary matrix of size [32 × 32] is generated. Pre-process means to resize the host image as [512 × 512] and grayscale and watermark images as binary [32 × 32]. For embedding the watermark images into the host image, the original host image is converted to the frequency domain by DCT. After then, the DCT bands are selected and modified. Then, the watermark embedding operation is done by the embedding algorithm, and the watermarked image is generated. The above procedure of watermark embedding is shown in Figure 2. The watermark embedding algorithm is described by Algorithm 1. The watermark

extraction and decryption steps are performed in a reverse procedure.

METHODOLOGIES

MODULES

Building a campus placement prediction system involves several modules and steps. Here are some key modules to consider:

Data Collection: Gather historical data related to campus placements. This may include information about students, their qualifications, the companies that visited the campus, job offers made, and other relevant details.

Data Preprocessing: Clean and preprocess the data to handle missing values, outliers, and ensure data quality. This step is crucial for accurate predictions.

Feature Engineering: Create relevant features from the data that can help in making predictions. This may involve transforming and selecting the most informative features.

Data Visualization: Visualize the data to gain insights and understand patterns. Visualization can also help in feature selection and model evaluation.

Model Selection: Choose appropriate machine learning or deep learning algorithms for the prediction task. Common choices include logistic regression, decision trees, random forests, support vector machines, and neural networks.

Model Training: Train the selected model on the pre-processed data. This involves splitting the data into training and testing sets and fine-tuning hyperparameters.

Model Evaluation: Assess the model's performance using evaluation metrics such as accuracy, precision, recall, F1-score, and ROC-AUC, depending on the nature of the problem (binary classification, multi-class classification, etc.).

RESULTS AND DISCUSSION

Fig 1: Without watermark

Fig 2: With watermark

Fig 3: Output Image

6.CONCLUSION AND FUTURE SCOPE

The multiple image watermarking techniques have gained attention in today's world as they provide stronger security than singular watermarking techniques. In this paper, the multiple image watermarking system is designed with DCT to increase the imperceptibility and security for image authentication. The random binary matrix encrypts the watermark images and provides the enhanced security for the system. This multiple image watermarking technique requires insignificant amount of time for each test case like singular watermarking to simulate the system. But, the system provides a little bit of computational complexity. Here, PSNR > 30 dB for each test case indicates the better quality of the watermarked image. The future work can be extended by simulating the results under several single and combined attacks. Also, the performance of the proposed method will be compared with existing current state-of-the-art methods and expanded for other multimedia elements.

7 REFERENCES

1. Begum, M. and Uddin, M.S. (2020) Digital Image Watermarking Techniques: A Review. Information, 11, 110.
2. https://doi.org/10.3390/info1102011
3. Begum, M. and Uddin, M.S. (2020) Analysis of Digital Image Watermarking Techniques through Hybrid Methods. Advances in Multimedia, 2020, Article ID: 7912690.
4. https://doi.org/10.1155/2020/7912690
5. Agarwal, N., Singh, A.K. and Singh, P.K. (2019) Survey of Robust and Imperceptible Watermarking. Multimedia Tools and Applications, 78, 8603-8633.
6. https://doi.org/10.1007/s11042-018-7128-5
7. Sridhar, B. and Arun, C. (2012) On Secure Multiple Image Watermarking Techniques using DWT. Proceeding Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12), Coimbatore, 26-28 July 2012, 1-4.
8. https://doi.org/10.1109/ICCCNT.2012.6395871
9. Mohananthini, N. and Yamuna, G., (2015) Multiple Image Watermarking Technique based on Hybrid DWT, SVD and Artificial

Neural Network. International Journal of Applied Engineering Research, 10, 7275-7297.
10. Preet, C. and Aggarwal, R.K. (2017) Multiple Image Watermarking Using LWT, DCT and Arnold Transformation. International Conference on Trends in Electronics and Informatics (ICEI), Tirunelveli, 11-12 May 2017, 158-162.
11. https://doi.org/10.1109/ICOEI.2017.8300908
12. Ananth, C., Karthikeyan, M. and Mohananthini, N. (2018) DWT-SVD based Multiple Image Watermarking Process on Cloud Computing. International Journal of Research Granthaalayah, 6, 88-96.
13. https://doi.org/10.29121/granthaalayah.v6.i6.2018.1339
14. Kumar, C., Singh, A.K., Kumar, P., Singh, R. and Singh, S. (2018) SPIHT-Based Multiple Image Watermarking in NSCT Domain. Concurrency and Computation: Practice and Experience, e4912, 1-9.
15. https://doi.org/10.1002/cpe.4912