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

EFFICIENT BIT APPROXIMATION DATA EMBEDDING USING REVERSIBLE DATA HIDING APPROACH

[1]Ms.M. Mohanasundari, [2]Mythili R, [3]Sethupathi V, [4]Sugumar S

[1]Assistant Professor, Department of Computer Science Engineering, Velalar College of Engineering and Technology, Erode, Tamil Nadu, India.

[2,3,4]Student, Department of Computer Science Engineering, Velalar College of Engineering and Technology, Erode, Tamil Nadu, India.

Abstract *:* A process framework called content-based image retrieval uses computer vision techniques to more effectively search through and manage huge image databases. To support effective browsing, searching, and retrieval for image collections, there is an increasing demand for devices and computer systems. This is because large digital image collections are growing because of the rapid advancements in electronic storage capacity and computing power. The security of digital information has evolved into a fundamental concern with continual advances in sight and hearing.The main focus on the efforts on altering current conventions to overcome the shortcomings of momentum security conventions. However, over the past couple of years, a few proposed encryption calculations have been shown to be unreliable, posing serious risks to important data.Using the most appropriate encryption calculation is a crucial step in providing security from such attacks, but the type of information being obtained will also determine which calculation is most appropriate in each situation.To meet the goal of protecting image content, we suggest an RDH with triple DES matrix-based transformation technique. More significantly, image retrieval and image convolution can be carried out directly on the content-protected images using the proposed framework for image content protection.

I. INTRODUCTION

Data embedding in photographs has attracted a lot of attention recently from academics and professionals across a range of fields, including computer science, engineering, and digital forensics. Data hiding in images has been successfully used in several applications to improve security, privacy, and authentication. The significance of efficient and safe data embedding in photos has grown crucial due to the widespread use of digital images in our daily lives, from social media to medical imaging.

K-Nearest Neighbor (KNN) and Least Significant Bit are examples of existing techniques for data embedding in images (LSB). LSB is a steganographic method that embeds data in the least significant bits of a picture, while KNN is a non-parametric classification algorithm that is frequently used for pattern recognition. Both KNN and LSB have drawbacks despite their popularity. For instance, KNN may be computationally expensive and memory-intensive, whereas LSB may be susceptible to intrusion.

Researchers have put up several alternative ways for data embedding in photographs to get over these restrictions. Reversible Data Hiding (RDH) is one such technique that, when the embedded data has been removed, enables the restoration of the original image without introducing any deformation. Techniques like histogram shifting, difference expansion, and prediction error expansion are frequently used to produce RDH. Triple Data Encryption Standard (DES), another suggested technique, encrypts the data before embedding it in the image, adding an extra layer of security.

The suggested method, which combines RDH and Triple DES, seeks to overcome the drawbacks of the current approaches and offer a more effective and secure way for data embedding in images. The suggested system consists of three stages: data encryption using Triple DES, data embedding using RDH, and data extraction and decryption. This technique not only strengthens security but also increases the embedded data's resistance to various attacks including compression and image processing.

It has been shown that the RDH and Triple DES combo perform better than the conventional KNN and LSB approaches. For instance, the proposed solution is less susceptible to security threats like statistical analysis and brute-force attacks. The suggested solution is also more efficient in terms of computational and storage requirements. Because of this, it is more useful for use in practical applications.

The suggested approach can be used for several purposes, including copyright protection, digital watermarking, and secure communication. The suggested technique can be used in secure communication to encrypt and embed confidential information in photos that are sent through unsecure channels. The suggested technique can be used to integrate ownership information in digital

watermarking. such as copyright or authorship, in images. In copyright protection, the proposed method can be used to embed watermarks in images to prevent unauthorized distribution and use of copyrighted material.

The suggested system has some drawbacks even if it is a step up from current practices. The suggested solution, for instance, may be subject to assaults like brute-force attacks on the encryption key. Also, because of the embedding process, the suggested solution may produce images with inferior quality. More study is required to increase the proposed system's robustness and effectiveness to address these drawbacks.

In conclusion, the subject of data embedding in images is fast developing, and fresh ideas for enhancing its efficiency and security are continually being put forth. A significant development in the field, the suggested system that combines RDH with Triple DES has the potential to be widely utilized in a variety of applications. The application of this approach might improve the general security and privacy of the data stored within photographs and contribute to the field's increasing body of knowledge.

2. LITERATURE SURVEY

2.1 AN IMAGE ENCRYPTION METHOD BASED ON ELLIPTIC CURVE ELGAMAL ENCRYPTION AND CHAOTIC SYSTEMS

This piece offers a fresh perspective on imagery. The problem of key management and distribution in symmetric picture encryption is resolved by the suggested asymmetric image encryption method, which is based on EC-ElGamal and chaotic theory. The chaotic system's initial values are generated by the SHA-512 hash, and the plain-image is jumbled using a crossover permutation based on the chaotic index sequence. The produced scrambled image is included in the ElGamal encrypted elliptic curve, which improves security and helps with key management difficulties. The cypher image is obtained by playing the DNA sequence-based diffusion combined chaos game. The suggested method is highly efficient, resistant to chosen-plaintext assaults, and secure, as shown by experimental analysis and performance comparisons, making it appropriate for secure picture communications.

Asymmetric encryption makes sure that the decryption key cannot be calculated from the encryption key and that the encryption key and the decryption key are different. Furthermore, the diffusion based on the chaos game and DNA code enhances the randomness of the pixel distribution, leading to a more secure encryption procedure. The proposed approach has undergone a thorough evaluation and been found to be highly efficient and secure. Asymmetric encryption makes it possible for several users to communicate securely, which makes it perfect for a variety of applications. Future studies will concentrate on time consumption optimisation to enhance real-time communication requirements.

The proposed encryption technique was examined in the experiment for resistance to cropping assaults. The incomplete image was decrypted after the cypher image was clipped partially and set to "0". The findings shown that even when the cypher image lost a significant amount of data in various areas or directions, the recovered images were still recognisable. This indicates how well the suggested approach defends against occlusion assaults. The proposed technique is a good contender for secure picture communications because to its efficiency, security, and durability.

To overcome key management and distribution concerns in symmetric picture encryption, this paper suggests an asymmetric image encryption approach based on EC-ElGamal and chaos theory. High security, good efficiency, and robustness against chosen-plaintext assaults are all achieved by the suggested approach. Furthermore, the technique can endure cropping assaults, proving its potency against occlusion assaults. As it permits secure communication between several users, asymmetric encryption is a fascinating field of study for a variety of applications. Future research will concentrate on time consumption optimisation to enhance real-time communication requirements. The potential for wider use of the suggested technology may be seen by the fact that it can be applied to different types of data encryption and transport.

2.2. INVISIBLE STEGANOGRAPHY VIA GENERATIVE ADVERSARIAL NETWORKS

In this work[2], convolutional neural networks (CNNs) are introduced to steganalysis and surpassed by conventional steganalysis algorithms. The improved capabilities of deep learning in the information-hiding domain have been demonstrated by these works.

Deep learning-based image steganography projects also exist, but they still face capacity, invisibility, and security issues. In order to precisely extract a secret gray image from the receiver side and conceal it in a color cover image on the sender side, we propose a novel CNN architecture called ISGAN in this paper. We create a mixed loss function that is more appropriate for steganography in order to generate more realistic stego images and reveal out more better secret images in order to better associate with the human visual system and improve invisibility. We also introduce generative adversarial networks to strengthen security by minimizing the divergence between the empirical probability distributions of stego images and natural images. Image steganography has numerous applications, including watermarking, copyright certification, the transmission of secret information, and more. A steganography algorithm's capacity, invisibility, and security can generally be measured. The capacity is measured in terms of bits-per-pixel (bpp), or the average number of bits hidden in each cover image pixel. The security and invisibility become worse as the capacity grows. Stego images must also be lossless because our steganography takes place in the spatial domain, and otherwise some parts of the secret image will be lost. There may be solutions to this issue. Since the secret image is inherently redundant, it doesn't matter if the
stego image is visually lossy. During training, some noise can be added to the stego images to mimic the loss of image caused by transmission. After that, we need to adjust our decoder network so that it can accommodate both the revealing and image enhancement processes simultaneously. We will attempt to solve this issue and boost the robustness of our model in subsequent work.

2.3 REVERSIBLE IMAGE STEGANOGRAPHY SCHEME BASED ON A U-NET STRUCTURE

In this work, the traditional steganography method has a low embedding capacity but frequently conceals secret data by mapping the data to a cover image or directly in a noisy area. In this work, we propose a novel U-Net-based image steganography scheme based on the idea of deep learning. First, a hiding network and an extraction network are included in the trained deep neural network during paired training; The sender then sends the secret image to the receiver by embedding it in another full-size image using the hiding network. Finally, the receiver correctly reconstructs the secret image and the original cover image by utilizing the extraction network. The experimental results demonstrate that the proposed method reduces the obvious visual cues issue and increases embedding

capacity by compressing and distributing the embedded secret image's information across all cover image bits. Utilizing images to conceal text messages is common. Bits per pixel (bpp) are the units used to measure the amount of hidden information. The amount of information is typically set to less than 0.4 bpp. The next step in this paper will combine image delivery with generative adversarial networks by passing image parameters to the receiver. The message length increases the bpp, which causes the cover image to change more. Through a pre-trained model, the receiver extracts the transmitted secret image. Double encryption ensures that the information is secure and that the secret message cannot be detected by the attacker during the transmission process. As the training set for the training network models used in this study, 45,000 images for training and 5,000 images for testing were gathered from ImageNet. The hyperparameter is set to 0.75, and the network's initial learning rate is set to 0.001. In order to ensure that the network parameters can be learned smoothly, the learning rate is automatically adjusted using the Adam optimization method

2.4 FEATURE - BASED SPARSE REPRESENTATION FOR IMAGE SIMILARITY ASSESSMENT

Mean-squared Error (MSE)/Peak signal-to-Matching ratio (PSNR), which has the very satisfying properties of convexity, symmetry, and differentiability, is used in this work to automatically design algorithms and evaluate similarity in a manner consistent with human evaluation. The two distorted images have drastically different visual fidelity. The correlation between MSE/PSNR and human quality judgment is not sufficient for most applications. Numerous multimedia applications rely heavily on the evaluation of image similarity. The objective of similarity assessment is to automatically and consistently assess the visual similarities between images. The image similarity assessment issue is interpreted as an information fidelity issue in this paper. To be more specific, we propose a feature-based method for quantifying the amount of information that can be extracted from a test image to determine the degree of similarity between the two images. To interpret the information in this image, we first extract the feature points and their descriptors from the image. Then, we learn the dictionary or basis for the descriptors. The image similarity assessment problem is then formulated in terms of sparse representation. By properly formulating them to sparse representation problems, we apply the feature-based sparse representation for image similarity assessment (FSRISA) technique to three well-known applications, namely image copy detection, retrieval, and recognition, to evaluate its applicability.

2.5 A TEXT RETRIEVAL APPROACH TO OBJECT MATCHING IN VIDEOS:

Algorithms for Image Quality Assessment are utilized in this work[5] to comprehend the similarity to a "reference" or "perfect" image. The image information measure measures both the amount of information that can be extracted from the distorted image from the reference image and the amount of information that is present in the reference image. The Human Visual System (HVS)/Natural scene statistics (NSS) primarily focus on assessing the similarity between a reference image and its non geometrically variational versions. The visual information fidelity measure is recommended for image quality assessment [2]. The geometric variations can be tolerated slightly by advanced methods like the Structural Similarity Index (SSIM) and Visual Information Fidelity (VIF). In both single distortion and cross distortion scenarios, the VIF method performs better than HVS-based method [5].

3.EXISTING SYSTEM

Now, we employ the algorithms KNN and LSB. When communicating on the Web, Stego-images are frequently damaged by interchannel noise or active noise attack, and it is difficult to retrieve an embedded image from a corrupted Stego-image.

The key feature of our approach is that, as opposed to k nearest neighbors, mutual nearest neighbors are used as evidence to identify anomalies and forecast the class labels of unseen instances. The benefit is that pseudo closest neighbours can be found and are not included when making predictions.

Data can be easily and frequently inserted into an image file using the least significant bit (LSB) technique. In this method, the M's bit is used to restore the LSB of a byte. The steganography of images works well with this technique. The LSB (Least Significant Bit) technique is typically used to hide data inside images.

3.1 DRAWBACKS OF EXISTING SYSTEM

- Loss of Global Weighting. Predefined fixed weights are adopted to fuse the distances of different low-level visual features. · Loss of Adaptive Weighting. adaptive weights for query images to fuse the distances of different low-level visual features.
- For our new approaches, two different ways of computing semantic signatures are compared.
- Not Visual: Query-specific visual semantic space using Reciprocal Hash Maps. For an image, a single semantic signature is computed from one SVM classifier trained by combining all types of visual features.
- The Least Significant Bit is that it is vulnerable to steganalysis and is not secure at all. To make it more secure, the least significant bit algorithm is modified to work in different way.
- Accuracy depends on the quality of the data.
- With large data, the prediction stage might be slow.
- Sensitive to the scale of the data and irrelevant features

4. PROPOSED SYSTEM

The RDH with triple DES algorithm is used by the proposed system Content-Based Image Retrieval (CBIR) to encode and index the visual contents of a picture, such as shape, texture, and spatial layout. The development of approaches for analyzing, interpreting, categorizing, and indexing image databases is the focus of current research in CBIR. The performance of image retrieval systems is being evaluated in addition to their development.

During the synthesizing process, a hidden message is embedded using the RDH approach. This provides the feature of reversibility by making it possible to retrieve the source texture throughout a message extraction method. To increase retrieval performance and accuracy, we suggested a method in this study that combines the benefits of many different techniques.

4.1 ADVANTAGES OF PROPOSED SYSTEM:

- It Represent all the descriptors of an image via sparse representation and assess the similarity between two images via sparse coding technique.
- The main advantage is, a feature descriptor is sparsely represented in terms of a Dictionary Score or transferred as a linear

combination of Dictionary Score atoms, to achieve efficient feature representation and robust image similarity assessment. · Best Results.

- High accuracy.
- High performance in search of related image reranking.

4.1 IMAGE PREPROCESSING AND FEATURE EXTRACTION

Two crucial processes in computer vision and image processing activities are feature extraction from the source picture and image preprocessing. To prepare pictures for additional analysis, such as object identification, image classification, and segmentation, these two procedures are frequently carried out in tandem. Before feature extraction, the picture data must be cleaned and improved by several activities known as image pretreatment. Resizing, cropping, noise removal, and picture normalization are a few examples of these procedures. The purpose of picture preprocessing is to eliminate any extraneous or unnecessary data that can obstruct further analysis.

Feature extraction comes after the picture has been preprocessed. Finding and extracting useful characteristics from picture data so they may be utilized for additional analysis is the process of feature extraction. Every quantifiable or perceptible aspect of the picture, such as its borders, corners, or texture patterns, might be considered a feature. When the features have been retrieved, they may be applied to a variety of tasks, including picture segmentation, object identification, and classification. As pictures are stored in matrices and are therefore easier for users to manipulate and process, Matlab is commonly used for image processing.

4.2 RDH FEATURE EXTRACTION FOR

COVER AND SECERET IMAGE:

Reversible Data Hiding (RDH) is a technique for reversibly embedding a hidden message within a picture. Finding features and constructing the area that may be utilized to hide data in the cover picture are both steps in the RDH feature extraction process for cover and secret images.

Cover Image Selection: The selection of a cover picture that is acceptable for RDH is the initial stage in the feature extraction process.

Secret Message Selection: The relevant secret message has to be chosen and then inserted after choosing the cover image. The secret message selection procedure in RDH (Reversible Data Hiding) is a crucial stage in the feature extraction process for cover and secret images.

RDH normally operates by calculating the prediction error signal between the original picture and a projected version of the image. By altering the prediction error values, this method makes space for embedding data. Many methods, including histogram shifting, difference expansion, and prediction error expansion, may be used to modify the prediction error values in order to enhance embedding capacity while maintaining picture quality.

4.3 IMAGE MINING

Data mining evaluates if data embedding in a picture is appropriate. This entails examining the statistical characteristics of the features and determining how well they can embed data while making sure that the embedded data cannot be seen. To find hidden links and patterns in the data, a variety of approaches including statistical analysis, machine learning, and pattern recognition are applied.

Image textures, colours, and forms are just a few examples of significant aspects that may be found and extracted using data mining and utilized for a variety of tasks, including picture retrieval and classification.

Using a reversible data concealing approach, the data is inserted after the most appropriate characteristics have been found. This assures that the original cover picture may be fully recovered without any distortion or loss of quality.

4.4 INDEX TABLE GENERATION

This module generates the index table. The index table allows us to access the synthetic texture and fully retrieve the source texture. The initial value of each entry in the index table is 1, indicating that the entry is empty. We must reassign values when we distribute the source patch ID in the synthetic texture. To increase the security of our steganographic process and make it more difficult for malevolent attackers to retrieve the source material, use a random seed for the distribution of patch IDs. Image 1 Original Image Index Table (a) Original Image Considering that the synthetic texture was created using 144 patches that were synthesized from nine source patches., we are able to distribute the nine IDs of the source patches in a sparse manner. Secret messages will be encoded in the excess 135 clear areas during the message.

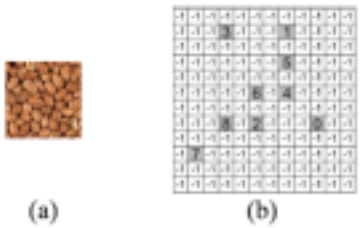

Figure 1.1 Index table Generation

4.5 COMPOSITION IMAGE GENERATION

Insert these source patches into a workbench in this module to generate a composition picture. Take a blank picture the same size as the synthetic texture to serve as our workstation. Use the source patch IDs that are saved in the index table to paste the source patches into the workbench after that. Paste the source patches straight into the workbench if there is no overlap between them throughout the pasting procedure.

Figure 1.2 Composition Image Generation

4.6 TRIPLE DES

A cryptographic method called Triple DES (Data Encryption Standard) is used to encode and decode data. Because it uses symmetric keys, the same key is utilized for both encryption and decryption. The Triple DES algorithm is a variation on the Data Encryption Standard (DES) method, which encrypts and decrypts data using the same key. TDES or 3DES are other names for triple DES. It works with 64-bit data chunks at a time. The 168-bit key length for the method is formed from three distinct 56-bit keys, known as key 1, key 2, and key 3. The plaintext message is first encrypted with key 1, then the resultant ciphertext is decrypted with key 2, and finally the result is encrypted once more with key 3. In contrast, the ciphertext message is first decrypted with key 3, encrypted with key 2, and then decrypted once again with key 1.

Preprocessing

Index table generation

Index table

Using message-oriented texture synthesis, the secret message is included in this module to produce the final stego synthetic texture. Do a rank calculation for each proposed patch. Choose the candidate patch whose rank is equal to the decimal value of the n-bit secret message. The patch that has been selected to be put into the working location has a piece of the n-bit secret message concealed inside it. The message extraction and authentication module consist of three phases.. The first sub-step establishes a candidate list using the overlapping region as its basis utilizing the present working location as a guide. The second sub-phase is the match authentication process. The final sub step involves extracting each secret message that was concealed in the stego synthetic texture patch by patch.

5.RESULT

The method used to evaluate the present technique is described. The algorithm was applied on a bit mapped (bmp) image that has the size of 300 pixels x 300 pixels with 256 colors. To evaluate the impact of the number of blocks on the correlation and entropy, three different cases were tested. The number of blocks and the block sizes for each case are shown in Each case produces three output images; (a) a ciphered image using the Blowfish algorithm, (b) a transformed image using the proposed algorithm, and (c) a ciphered image using the proposed algorithm followed by the Blowfish algorithm. For the rest of this paper, we use image A, image B, image C, and image D to denote the original image, the ciphered image using the Blowfish algorithm, the transformed image, and the ciphered image using the proposed algorithm followed by the Blowfish algorithm respectively. The respective algorithm with RDH with 3DES provides the maximum accuracy, along with the SVM. Results in the low accuracy. The resulted from applying the proposed algorithm on the different block sizes of the original image. The correlation and entropy of each one was compared with applying the corresponding algorithm alone. The results of this experiment are shown. A simple and strong method has been proposed for image security using a combination of block-based image transformation and encryption techniques. The cases showed that the correlation was decreased when the proposed algorithm was applied to them before the Blowfish algorithm. Experimental results of the proposed technique showed that an inverse relationship exists between number of blocks and correlation, and a direct relationship between number of blocks and entropy. When compared to many commonly used algorithms, the proposed algorithm resulted in the best performance; the lowest correlation and the highest entropy.

6.CONCLUSION AND FUTURE ENHANCEMENT

The project aimed to develop a Java program that utilized reversible data hiding, matrix-based image transformation, and encryption techniques to enhance the efficiency and security of image processing. The program was designed to enable 128×128 bit and 256×256-bit manipulation, reduce data loss, and decrease computing time. The outcome of the project was a working prototype that demonstrated the effectiveness of the proposed method for image security and data embedding. In bit approximation data embedding reversible data hiding (RDH) with Triple DES are powerful techniques for hiding secret data in digital media, each with their own advantages and limitations.

Future enhancements can be made by combining these techniques or developing new algorithms to increase the capacity of hidden data, improve robustness to attacks, and enhance the security and efficiency of the embedding process. Furthermore, the application of these techniques can be expanded to various domains, such as forensics, surveillance, and digital rights management, to improve the protection of sensitive information and intellectual property. As technology continues to evolve, the development and improvement of data embedding techniques will be crucial in ensuring security and privacy.

7.REFERENCES

1. Duan X, K. Jia, B. Li, D. Guo, E. Zhang, and C. Qin, "Reversible image steganography scheme based on a U-net structure,'' IEEE Access, vol. 7, pp. 9314–9323, 2019, doi: 10.1109/access.2019.2891247.
2. He, K., Zhang, X., Ren, S., & Sun, J. (2019). "Deep residual learning for image recognition". In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 580-588).
3. Liu, D., Li, B., & Wen, J. (2019). "A novel deep learning-based approach for CT image segmentation. IEEE Transactions on Medical Imaging", 38(4), 1012-1024.
4. Liu, Y., Gong, D., Shi, Y., & Yang, X. (2020). L0SM: "A low-rank and sparsity-based method for image demosaicing". IEEE Transactions on Image Processing, 29, 933-946.
5. Ren, Z., Zhong, X., Wang, Y., &Guo,J. (2020). "Edge-enhanced image deblurring using deep residual learning. IEEE transaction on image processing",29, 838-849
6. Wang, W., Xie, Z., Zhang, X., & Ma,J. (2017). "A survey of image synthesis and editing with generative adversarial networks". IEEE Transactions on Multimedia, 20(11), 2901-2918.
7. Wang, Y., Wang, L., Zhang, X., & Chen, Y. (2018). "Image quality assessment: from degradation models to perceptual metrics". IEEE Transactions on Image Processing, 27(8), 3949-3964.
8. Zeng, Y., Ye, Q., Li, J., Li, Q., & Li, Y. (2020). "Image super-resolution using deep learning: A review. IEEE Transactions on Circuits and Systems for Video Technology", 30(11), 3829-3851.