An Improved Data Hiding Technique based on the Combination of Compression Steganography and RSA Cryptography

SUSHANT CHAMOLI , Department of Comp. Sc. & Info. Tech., Graphic Era Hill University, Dehradun, Uttarakhand, India 248002,

Abstract

Image compression and encryption are crucial components of information security since it is safer to use compressed data than uncompressed data and can be handled more easily due to its smaller size. Therefore, efficient, safe, and connectable data is produced using effective data compression technology. Lossy and lossless compressions are the two main categories of compression algorithm approaches. Any type of data format, including text, audio, video, and picture files, may leverage these technologies. To further security, this data will be encrypted using the LSB algorithm, after which it will be hidden from prying eyes.

DOI Number: 10.48047/nq.2019.17.03.2019 NeuroQuantology 2019; 17(03):188-193

1. INTRODUCTION

A two-dimensional discrete cosine transform (2D-DCT) system with quantization and zigzag layout is demonstrated in this technique. This method serves as the basis and primary channel for the JPEG photo compression scheme. Compression and decompression are used to separate the entire process in the computation by utilising the 2D-DCT characteristic. The pixel size was decreased based on the quantization and zigzag processes, even if the picture data remained unchanged. The quantization procedure is conducted using the division operation. This process thereby reduces data loss during decompression. Added knowledge about the behaviour of local variation under JPEG compression are provided by the theoretical research presented in this work. It may also be used for a number of image processing and analysis tasks, such as image filtering, image quality assessment, and picture enhancement. Improved vector quantization is applied in this project, which is conducted in MATLAB. Pictures may be compressed and use the compression ratio, MSE, and PSNR.

Picture compression uses data compression to encrypt the original image using a minimal number of bits. Reducing picture redundancy and storing or transmitting data in an effective manner are the goals of image compression. The fundamental objective of such a system is to minimise the amount of storage required, and the decoded picture that is presented on the monitor attainable proximity feasible to the original image. Encoding communications (or information) in the realm of cryptography, this process is known as encryption, making information so that only those with the right access may read it. Although it doesn't stop hacking, encryption makes it less likely that the data will be read by the hacker. The message or data, which is known as plaintext in an encryption system, is encrypted using an encryption algorithm to produce unintelligible ciphertext (ibid.). Typically, a key for encryption is used, which defines how the message should be encoded. Any opponent who has access to the ciphertext should be unable to decipher the original message in any way. However, an authorised person can decode the ciphertext applying a decryption technique, which often necessitates a secret decryption key that attackers are unable to get. An encryption technique often requires a key-generation mechanism to generate keys at random for technical reasons.

Encryption can safeguard message secrecy on its own, but other measures, such as the validation of a message authentication code (MAC) or a digital

signature, are still required to safeguard a message's integrity and validity. Standards and cryptographic hardware and software are readily accessible, however utilising encryption to guarantee security may be a difficult task. Attacks can be effective if a single design or implementation error occurs. Without really disabling the encryption, an attacker may occasionally be able to access unencrypted data. for instance, TEMPEST, a Trojan horse, or traffic analysis.To prevent manipulation, digital signature and encryption must be used at the moment the message is created (that is, on the same device it was generated on). Otherwise, it might possibly be compromised by any node between the sender and the encryption agent. It should be understood that adding encryption at the time of creation only increases security provided the encryption device has not been tampered with.

The analysis of JPEG compression's impact on local variation is the primary topic of this article. In order to predict local variance, we must create a theoretical equation using the alternating-current (AC) coefficients of the block-DCT as a model, which are assumed to follow a Laplacian distribution. The fluctuation in local variance brought on by JPEG compression is next examined based on the derivation.In order to validate our derivation and analysis, simulation and experiments are finally carried out. A common way to gauge how smooth a picture is by looking at its local variance in intensity. For instance, it is frequently used in image processing and analysis to determine the visual saliency or to modify the intensity of the filtering. As far as we can tell, however, no analytical work examining the impact of JPEG compression on local picture variance has been published. When dealing with a noisy data collection, the suggested feature extraction strategy performs consistently well. When compared to FFT-based methods, the DCT approach is frequently simpler to get excellent performance for general lengths N.

2. LITERATURE SURVEY

In many surveillance situations, when there is consistently a great distance between the camera and the objects (people) of interest, face image resolution augmentation is typically desirable. Face photos have a more regular structure than the generic images outlined above, making them easier to manipulate. In fact, we can work with input photographs of lesser quality for face super-resolution. To recover details, the fundamental strategy is to first utilise the face prior to magnify the input to a respectable medium resolution. Next, the local sparsity prior model is used.To be more specific, there are two phases to the solution: 1) Global model: restore a face with a medium-high resolution picture using the reconstruction constraint; however, the sole available option sought in the face subspace; and 2) Local model: recover the image's finer features using the local sparse model. They produce photos with super-resolution for both generic and face photographs in comparison to earlier suggested work. To save a picture in the dictionary using this way would take up too much RAM [1].

Before any picture compression, the K-SVD training method is an offline technique. A set of K-SVD dictionaries are created during training, and these dictionaries are then regarded as fixed during the picture compression step. Over a set of instances known as the learning set, a single dictionary is educated for each 15-15 patch. The training is conducted as described in the preceding section, with the parameters being described in Section 4. The mean patch image of the learning set's examples is computed and subtracted from each example before the training process for that patch begins. The processes used in the encoder for image compression are shown below, and they are then used in the decoder in reverse order. When compared to other compression techniques, they yield superior results because to the K-SVD dictionary learning process and sparse and redundant representations. However, fingerprint image analysis is difficult with this approach [2].

An image compression method can make use of a dictionary learned using the RLS-DLA methodology. Create the vector set from non-overlapping picture patches or, if the dictionary is learnt in the wavelet domain, from wavelet coefficient patches. Applying sparse approximation of X and the dictionary D, determine the sparse matrix W.the zero-bin is double the size of the other bins due to the author's usage of a uniform quantizer with thresholding. The quantize W matrix is encoded using entropy. The non-zero items of W are first put into one sequence (columnwise) and the position information, or the number of zeros before each non-zero entry, is put into another series. In both the pixel domain and the 9/7 wavelet domain, the goal of this work was to investigate the compression potential of sparse approximations using dictionaries learned by RLS-DLA. They examine the compression capacity of dictionaries learned using RLS-DLA-based sparse approximations in the pixel domain as well as the 9/7 wavelet domain. The suggested compression method, which makes use of learned dictionaries—preferably those acquired via RLSDLA—performs admirably. This technique yields results that are comparable to JPEG2000 but just barely poorer [3].

Due to the fact that the majority of feasible sparsity measures are not convex, sparse approximation issues are computationally difficult. Greedy approaches attempt to solve the approximation issue globally by making a series of locally optimum decisions. The Image is compressed once it has been encrypted. The data was supplemented by a key sequence that had the same length as the data sequence. A stream cypher was used to encrypt the information.A Gaussian sequence that was unrelated to the data held the secret. The encrypted data is compressed by our encoder at a rate of 1 bit/sample. The length of the generated binary sequence is twice that of the real-valued data sequence. Carrier images and SCAN patterns produced by SCAN technique are both used in hybrid image encryption. After combining the original picture and carrier image, the scan process is used to either image to produce a severely deformed encrypted image. It is possible to create new physical sampling systems that capture discrete, low-rate, incoherent samples of the analogue signal directly. It's possible to not know or have access to the sparse basis on which the signal should be represented [4].

It has been demonstrated that FISTA converges to function values as O(1/k2), where k is the number of iterations. Alternative algorithms being developed by other researchers may improve ISTA's performance. Similar to FISTA, these techniques calculate the subsequent iteration based on not just the previous iteration but also on two or earlier computed iterations. Finally, we note that FISTA already had the values produced by ISTA and MTWIST at iterations 275 and 468, respectively, when compared to their values at iteration 10,000. Similar to FISTA's suggested procedure, these approaches calculate the subsequent iteration based on not just the previous iteration but also one or more earlier computed iterations.FISTA maintains the computational simplicity of ISTA while having a global rate of convergence that is demonstrably far higher. However, the data obtained via the regularisation toolbox's function blur [5].

3. PROPOSED SYSTEM

The analysis of JPEG compression's impact on local variation is the primary topic of this article. In order to predict local variance, we must create a theoretical equation using the alternating-current (AC) coefficients of the block-DCT as a model, which are assumed to follow a Laplacian distribution. In the suggested study, a hybrid data compression technique enhances the amount of input data that is encrypted using the RSA (Rivest-Shamir-Adleman) cryptographic procedure in order to raise security level, furthermore, it may be utilized for implementing both lossy plus lossless compacting Steganography methods.

By reducing the amount of data sent each time, this strategy can help with quick transmission over a sluggish internet connection or take up little room on various storage devices.

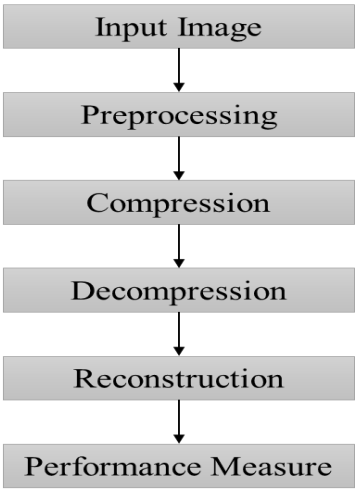

Fig 1: System Architecture

The fluctuation in local variance brought on by JPEG compression is next examined based on the derivation. In order to validate our derivation and analysis, simulation and experiments are finally carried out. A common way to gauge how smooth a picture is by looking at its local variance in intensity. For instance, it is frequently used in image processing and analysis to determine the visual saliency or to modify the intensity of the filtering. As far as we can tell, however, no analytical work examining the impact of JPEG compression on local picture variance has been published. A hypothetical investigation of the fluctuation in local variance brought on by JPEG compression is offered in this work.

In a JPEG picture, the anticipated intensity variation for 8 8 non-overlapping blocks is first determined.The discrete cosine transform coefficient distributions of the original image's Laplacian parameters also the JPEG compression's quantization step sizes serve as the basis for the expectation. Second, several intriguing characteristics that define how the local variance behaves when subjected to various JPEG compression levels are addressed. Finally, to validate our derivation and explanation, both simulation and experiments are run. The theoretical research offered in this study offers some fresh perspectives on how local variation behaves when JPEG compression is applied. Additionally, it might be utilised in a few aspects of image

processing as well as analysis, including picture enhancement, image quality evaluation, and image filtering.

The three colours of the image are split into several 88 blocks as the following stage after the conversion of colour coordinates. We really discard data during the quantization process. Lossless processing is used in the DCT. The IDCT can accurately retrieve the data, albeit this isn't totally accurate as no physical implementation can calculate with absolute precision in practise. The 88 DCT matrix's coefficients are split by a matching quantization value during quantization. The DC coefficient and the 63 AC coefficients are handled individually following quantization. The average value of the 64 initial picture samples is gauged by the DC coefficient.

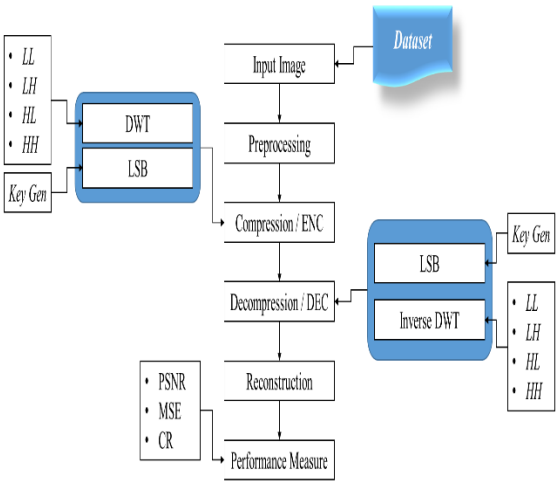

Fig 2: System Flow Diagram

The DC coefficient of an adjacent 88 block is typically highly correlated, hence, the quantized DC coefficient is represented as the divergence from the DC term of the preceding block. As a considerable portion of the overall picture energy is typically found in DC coefficients, this specific approach is beneficial. Although JPEG and other DCT-based picture compression algorithms have given excellent quality, there is still significant room for improvement. The new DWT-based image compression methods, such JPEG 2000, consequently gained popularity. Since the DWT is an application of subband coding, we first go over the theory of subband coding. In essence, decompressing a JPEG picture is the same as running the compression stages backwards and in the wrong sequence.

The Huffman tables and Huffman tokens in the picture are first extracted from the image and then decompressed. As the first item required to decompress a block, it then decompresses the DCT values for each block. The remaining 63 values in each block are then decompressed by JPEG, which inserts the proper number of zeros as necessary. The final step in undoing phase four is to reconstruct the 8 × 8 blocks that were initially utilised to compress the image by decoding the zigzag sequence. High compression ratios were achieved using the JPEG algorithm, which was developed to compress photographic pictures.

Additionally, it gives users the option to select either extremely tiny or high-quality output photos. The majority of JPEG variations adapt the fundamental ideas of the algorithm to deal with more particular issues. When dealing with a noisy data set, the suggested feature extraction approach exhibits strong performance.

4. RESULTS

Since compressed data is more secure than uncompressed data and can be handled more easily with less resources, image compression and encryption are crucial components of information security. The result is efficient, safe, and connectable data thanks to effective data compression technologies. The project's final output, an 8x8 Compressed DCT image, was assessed in each scenario using the MATLAB environment on Windows XP. The blocking effect is a significant problem and a point of contention for the DCT. Images in DCT are divided into blocks of 8x8 or 16x16 pixels or bigger. These blocks provide a challenge since they become visible at higher compression ratios when the image is reduced. People refer to this as the blocking effect. Only 4 coefficients are retained in the final image after 8x8 block compression. This piece of art effectively utilises the blocking effect.

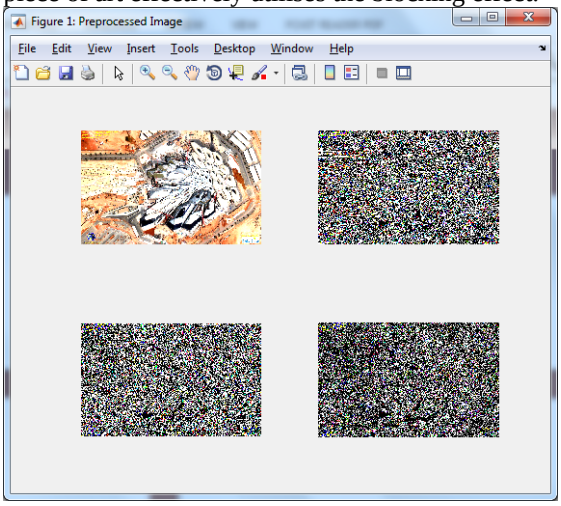

Fig 3: Pre-Processed Image

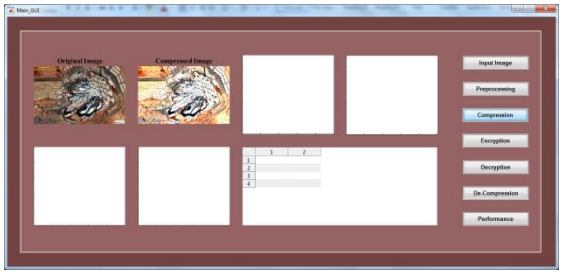

Fig 4: Image Compression

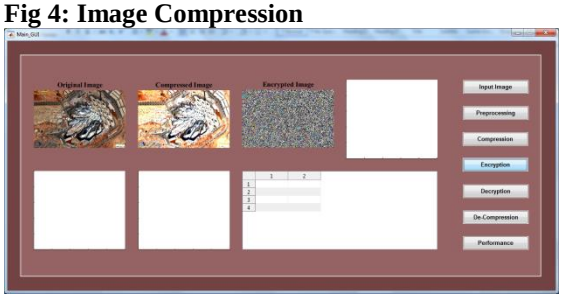

Fig 5: Image Encryption

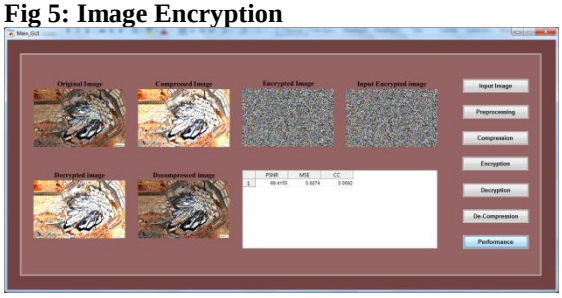

Fig 6: Performance Analysis

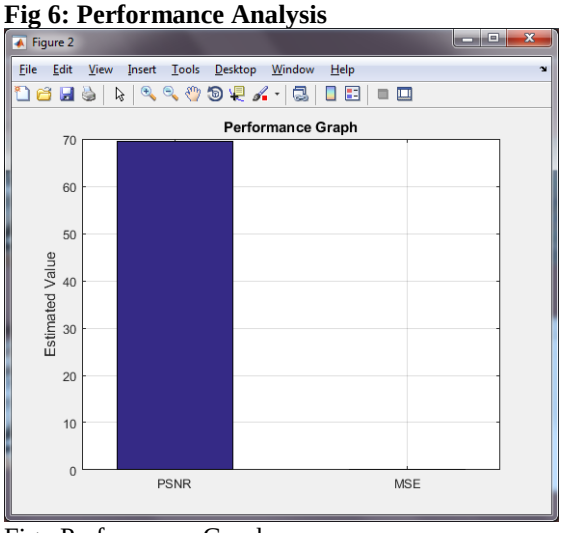

Fig : Performance Graph

5. CONCLUSION

This article demonstrates how the JPEG image compression was effectively implemented. Utilizing MATLAB software, the system is created. The end product of this project, an 8x8 Compressed DCT picture, was evaluated in every scenario under the MATLAB environment on Windows XP. The blocking effect is a major issue and a source of criticism for the DCT. Blocks of 8x8 or 16x16 pixels or larger are used to divide pictures in DCT. These blocks provide a difficulty in that they become noticeable at greater compression ratios when the image is lowered. The blocking effect is what people refer to as this. With 8x8 block compression, only 4 coefficients are kept in the final picture. This artwork makes a strong use of the blocking effect.

6. FUTURE ENHANCEMENT

The two lossless data compression methods LZ77 and LZ78 are employed to compress the image in future work.

REFERENCE

[1] L. Guan, S. W. Perry, and H.-S. Wong, *Adaptive Image Processing: A Computational Intelligence Perspective*. Boca Raton, FL, USA: CRC Press, 2001.

[2] F. Catté, P.-L. Lions, J.-M. Morel, and T. Coll, "Image selective smoothing and edge detection by nonlinear diffusion," *SIAM J. Numer. Anal.*, vol. 29, no. 1, pp. 182–193, 1992.

[3] J. A. Stark, "Adaptive image contrast enhancement using generalizations of histogram equalization," *IEEE Trans. Image Process.*, vol. 9, no. 5, pp. 889–896, May 2000.

[4] Y. Zhang, X. Ji, H. Wang, and Q. Dai, "Stereo interleaving video coding with content adaptive image subsampling," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 23, no. 7, pp. 1097–1108, Jul. 2013.

[5] C. Liu, A. Zhou, Q. Zhang, and G. Zhang, "Adaptive image segmentation by using mean-shift and evolutionary optimisation," *IET Image Process.*, vol. 8, no. 6, pp. 327–333, 2014.

[6] Jeysudha, A., Muthukutty, L., Krishnan, A., & Shivadekar, S. (2017). Real Time Video Copy Detection using Hadoop. International Journal of Computer Applications, 162(9), 42-45.

[7] N. Sharma and U. Batra, "Performance analysis of compression algorithms for information security: A review", ICST Trans. Scalable Inf. Syst., vol. 7, no. 27, Jul. 2018.

[8] R. Ferzli and L. J. Karam, "A no-reference objective image sharpness metric based on the notion of just noticeable blur (JNB)," *IEEE Trans. Image Process.*, vol. 18, no. 4, pp. 717–728, Apr. 2009.

[9] Shivadekar, Samit, S. R. Abraham, and S. Khalid. "Document validation and verification system." Int. J. Adv. Res. Comput. Eng. Technol.(IJARCET) 5.3 (2016).

[10] G. Yammine, E. Wige, and A. Kaup, "A no-reference blocking artifacts visibility estimator in images," in *Proc. Int. Conf. Image Process. (ICIP)*, Sep. 2010, pp. 2497–2500.

[11] K.-H. Thung, R. Paramesran, and C.-L. Lim, "Content-based image quality metric using similarity measure of moment vectors," *Pattern Recognit.*, vol. 45, no. 6, pp. 2193–2204, 2012.
[12] L. Li, H. Zhu, G. Yang, and J. Qian, "Referenceless measure of blocking artifacts by Tchebichef kernel analysis," *IEEE Signal Process. Lett.*, vol. 21, no. 1, pp. 122–125, Jan. 2014.
[13] Vinit Khetani, Jennifer Nicholas , Anuja Bongirwar , Abhay Yeole."Securing Web Accounts Using Graphical Password Authentication through Watermarking". International Journal of Computer Trends and Technology (IJCTT) V9(6):269-274, March 2014. ISSN:2231-2803.
[14] K. Lee, D. S. Kim, and T. Kim, "Regression-based prediction for blocking artifact reduction in JPEG-compressed images," *IEEE Trans. Image Process.*, vol. 14, no. 1, pp. 36–48, Jan. 2005.
[15] E. Nadernejad, N. Burini, and S. Forchhammer, "Adaptive deblocking and deringing of H.264/AVC video sequences," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP)*, May 2013, pp. 2508–2512.
[16] B. Gatos, I. Pratikakis, and S. J. Perantonis, "Adaptive degraded document image binarization," *Pattern Recognit.*, vol. 39, no. 3, pp. 317–327, 2006.