JOINT IMAGE COMPRESSION AND ENCRYPTION SCHEMES

Punitha.V[1], Pooja.M[2], Monisha.S[3],Thagasin.M[4],Yogapriya.S[5]

[1] Professor, Department of Information Technology, Saranathan College of Engineering, Trichy,Tamilnadu,India

[2,3,4,5] Department of Information Technology, Saranathan College of Engineering, Trichy,Tamilnadu,India

punitha-it@saranathan.ac.in, poojait82001@gmail.com, monishayashan@gmail.com, thagasinaafsheen@gmail.com, lathapriya017@gmail.com

Abstract: The benefits of combining image encryption and compression algorithms have been demonstrated in the protection of compressed images. A trade-off between encryption power and compression ability must be addressed in order to provide the protection. We raster scan a given plain- image into non-overlapping 8 x 8 blocks,then use the AES encryption algorithm to encrypt it. JPEG's encryption procedures take place throughout the transformation, quantization, and zigzag scan stages.

Keywords:Compression, Encryption, Discrete Cosine Transform, Quantization, Zigzag Scan

I.INTRODUCTION

Networks and multimedia technologies are fast evolving these days, and they are now widely employed in all aspects of life. Sharing raw size digital media files necessitates a significant amount of storage space and network traffic due to the widespread availability and use of high-resolution multimedia devices and services. As a result, researchers are focusing their efforts on improving image compression algorithms for massive data files while keeping the highest possible quality. Due to the rapid increase in hacking attempts and personal privacy concerns, security and privacy have become an important and hard part of protecting multimedia assets from unwanted access.[6][7]

As a result, data compression and encryption has become a popular research topic. As a result, JICE (joint image compression and encryption) is necessary to achieve both compression and encryption goals at the same time. The joint technique is problematic due to the discrepancy between compression and encryption. JICE is a useful tool for providing security and saving space when it comes to photos.[8][9][10]

II. OBJECTIVE

In Conventional Methods, image compression and encryption are two different processes. As a result, an adversary's attack can be more easily organised. However, combining these two methods increases the output confidence. As a result, opponents will face greater challenges, and plans will be safer.

The goal of picture encryption and compression is to produce a high-quality hidden image in order to keep information private and to decrease image data irrelevance and redundancy in order to store or transfer data efficiently.

The primary goal of the Joint Image Compression and Encryption Scheme is

improve the compression ratio and the encryption time complexity.

III. LITERATURE SURVEY

In [1], Mohammed Rasheed suggested an image reduction and encryption approach based on the Hexa-Coding algorithm and a modified JPEG technology. The compression process begins by partitioning a picture into 8x8 blocks, then applying the DCT (Discrete Cosine Transform) to each block separately before applying uniform quantization. Additionally, the number of blocks is lowered by removing inconsequential values, and leftover coefficients are compressed using Arithmetic coding. Finally, the compressed data is encoded with Hexa-encoding to further reduce compression size and enable encryption.

For joint picture compression and encryption, Pratibha Chaudhary employed a novel column-wise scanning and optimization approach.[2]. It works with various image sizes and dimensions, including 256X256, 512X512, and 1024X1024 pixels. The compression algorithm used is similar to JPEG compression, however instead of zigzag scanning, column-wise scanning and optimization is used. The Huffman coding of JPEG compression is replaced with Arithmetic coding in entropy phase coding.

In[3],Xinsheng Li proposed a revolutionary joint picture compression and encryption approach dubbed QSBLA, which combines a quantum chaotic system, sparse Bayesian learning (SBL), and a bit- level 3D Arnold cat map. The QSBLA comprises of six stages in total. To generate chaotic sequences for later compression and encryption, a quantum chaotic system is used first. Second, SBL is used to compress images as one type of compressive sensing. Third, the compressed image is subjected to a diffusion procedure. The compressed and diluted image is then divided into numerous bit-level cubes in the fourth step. Fifth, each bit-level cube is permuted using 3D Arnold cat maps. Finally, all of the bit-level cubes are combined and converted into a 2D pixel-level image, yielding a compressed and encrypted image. Extensive tests on 8 publically accessible photos show that the proposed QSBLA outperforms or is comparable to several state-of-the-art techniques on several measurement indices, indicating that the QSBLA is promising for joint image compression and encryption.

A unique approach for compressing encrypted photos with auxiliary data was proposed by Xinpeng Zang in [4].The content owner encrypts the original uncompressed photos and generates auxiliary data for data compression and image reconstruction. The channel provider who does not have access to the original content can then compress the encrypted data using a quantization method with optimal parameters derived from auxiliary data and compression ratio-distortioncriteria, and send the compressed data, which includes an encrypted sub-image, quantized data, quantization parameters, and another piece of auxiliary data. The principal image content can be reconstructed at the receiver using compressed encrypted data and the secret key. The suggested scheme's ratio-distortion performance is superior to that of earlier approaches, according to experimental results.

Anil Kumar.A proposed that encrypteddata can be compressed via distributed source coding.Authors looked into encryption first, then lossless compression of grayscale and colour photos in this work[5] Instead of directly encrypting the images, they proposed encrypting the prediction errors and reducing the cypher texts via distributed source coding. The simulation results show that, notwithstanding encryption, comparable compression increases may be achieved using the suggested technique,with compression ratios ranging from 1.5 to 2.5.

IV. EXISTING SYSTEM

Compression followed by Encryption

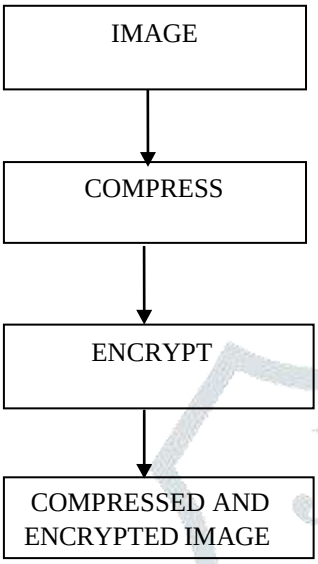


Fig.1 First compress and then encrypt

An invader has less cleave to access the image, as shown in Fig.1 , but encryption may increase the size again.

Encryption followed by Compression

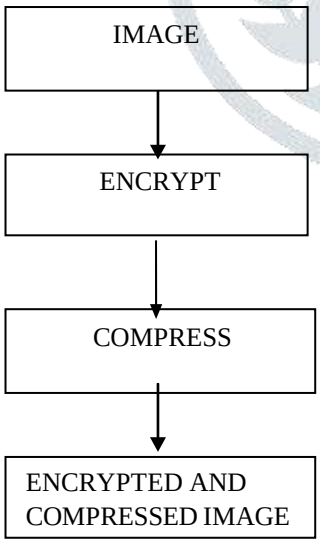


Fig.2 First Encrypt and Compress

The size is not enlarged again, as shown in Fig.2 , but an intruder may have more hints to view the image. The techniques that act directly on raw photos are included in this category. These algorithms, on the other hand, are often inapplicable for lossy compression since the pixel value in the cipher-image cannot be entirely recovered to the same value as the plain-image under lossy compression. Furthermore, executing encryption before compression generally breaks the correlation in plain-image, leaving little space for compression, making these techniques unsuitable for compression.

V. PROPOSED METHODOLOGY

The suggested system is efficient since it compresses and encrypts data at the same time, making computing faster and more secure.

In the intermediatary stages of JPEG, we use the AES encryption technology. The procedures are carried during at the transformation and quantization stages of JPEG. To improve the dispersion property of cryptosystems, we use adaptive keys for encryption based on the plain-image content. We raster scan a given plain-image into non-overlapping 8X8 blocks and apply order-8 DCT to these blocks transformation. We distribute the coefficients of each 8X8 block to fit within the existing JPEG bitstream architecture.

VI. SYSTEM DESIGN

The input image can be retrieved from any directory. The picture's path as well as the input image will be displayed. Fig.3 shows the architectural design. We first raster scan and convert a given plain-image into non-overlapping 8X8 blocks, then use the AES Encryption approach, followed by

Quantization, and finally scanning. We used Zigzag Scanning in this case. In every stage, compression and encryption are performed simultaneously.

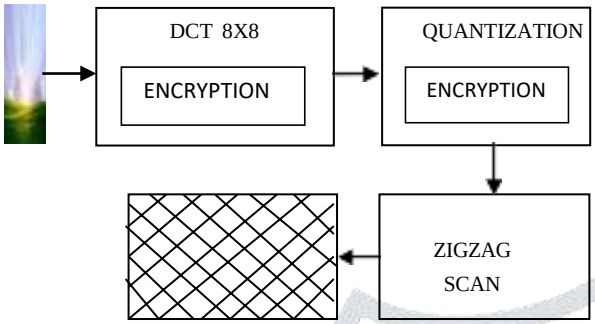


Fig.3 Archeitectural Design

There are mainly three stages of JPEG compression

- Transformation stage
- Quantization stage
- Zig-Zag Scan stage

TRANSFORMATION

A function or operator that accepts an image as input and outputs a transformed image. The input and output images may appear completely different and have distinct interpretations depending on the transform used.

It removes the weaker colour in an image in the translation module. As a result, the image's size and intensity are reduced. The image will not be affected by deleting the weaker colour.

DISCRETE COSINE TRANSFORMATION

The Discrete Cosine Transform (DCT), as shown in Fig.4., is a technique for transforming picture pixels in the spatial domain into a frequency domain in which redundancy can be discovered.

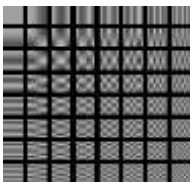


Fig.4 8X8 DCT

To execute DCT Transformation on a picture, we must first obtain image file information (pixel value expressed as an integer with a range of 0–255), which we divide into 8 X 8 matrix blocks, and then apply discrete cosine transform to that block of data.

QUANTIZATION

Quantization is a compression technique that reduces a large number of values to a single quantum. To put it another way, it's

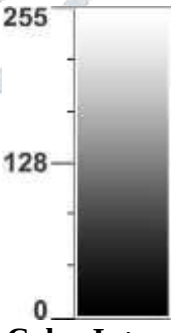


Fig.5 Color Intensity for Quantization

the process of transforming a continuous range of values into a finite range of discrete values. When the number of discrete symbols in a stream is reduced, the stream becomes more compressible. Digitizing of colour intensity, as seen in

Fig.5, is difficult since it might have unlimited values. The number of various colours an image can have is determined by quantization.

Each and every pixel of an image will have a quantum value in this process. We must obtain one single value by converting all of the quantum values to matrix representation. To put it another way, it's the process of transforming a continuous range of values into a finite range of discrete values. When the number of discrete symbols in a stream is reduced, the stream becomes more compressible.

K-MEANS CLUSTERING

K-means clustering is an unsupervised learning method that is straightforward to use. By locating clusters of pixel values, this method can be used to apply colour quantization in an image.

WORKING

A coloured image includes three channels: Red(R), Green(G), and Blue(B), and each pixel represents a colour with 24 bits (8 bits (unsigned integers from 0 to 255) each for R, G, and B).

K distinct Clusters are created from the datapoints. The centroid of each cluster serves as a unique identifier. This algorithm divides similar values into K Clusters, with each pixel value being replaced by the value of the cluster's centroid.

ZIGZAG SCAN

The zig zag pattern is a typical image compression scanning pattern that is used to the outcome of the quantization process, which reorders the pixel values in a 2-D square matrix into a 1-D matrix.The goal of the Zigzag Scan is to find lines and edges in an image.

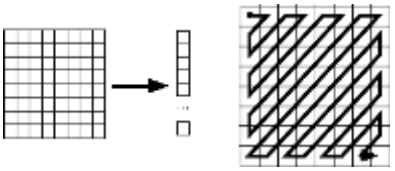


Fig.6 Zigzag Scan

Low frequency coefficients are grouped at the top of the vector, whereas high frequency coefficients are grouped at the bottom. It transfers an 8 x 8 vector to a 1 x 64 vector in Fig.6. It ruins the original image's adjacency connection.In 1D data, adjacent pixels in a 2D image are widely spaced and dispersed. It prevents images with partial patterns from being shared.

VII. ADVANCED ENCRYPTION STANDARD

The Advanced Encryption Standard (AES) algorithm is a symmetric block cipher that uses three distinct cipher key sizes of 128,192, or 256 bits to process images with blocks of 128 bits. The number of execution rounds of the algorithm is 10, 12, or 14 depending on the key size length employed as shown in Fig.8

WORKING

AES is a cryptographic algorithm that transports data across many phases. A 4x4 matrix carries the data in a single block, with each cell containing a single byte of information, because a single block equals 16 bytes.

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

Fig.7 4X4 AES

A state array is the matrix depicted in Fig.7 above. Similarly, the initial key is expanded into (n+1) keys, where n is the number of rounds in the encryption procedure to be followed. The number of rounds for a 128-bit key is 16, and the number of keys to be created is 10+1, for a total of 11 keys.

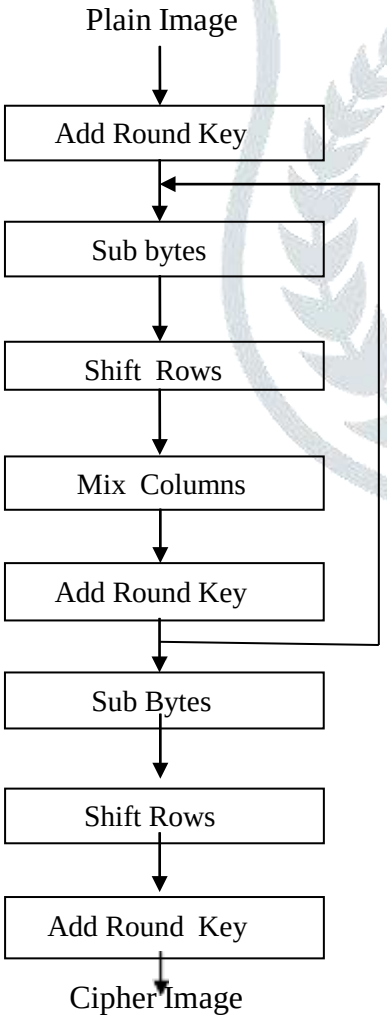


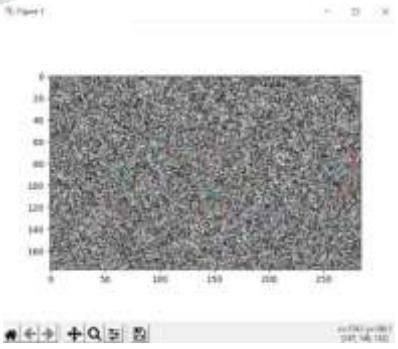
Fig.8 STEPS IN AES

VIII. RESULTS

Graphical User Interface

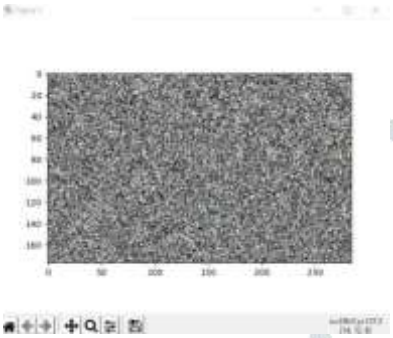
Image After Browse

Image After Translation



Translated Encrypted Image

Image After Quantization



Quantized Encrypted Image

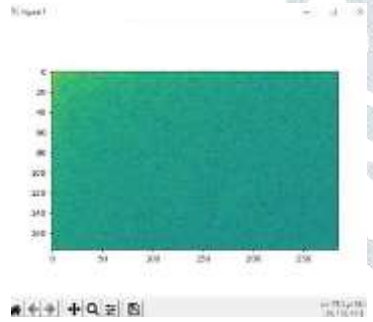
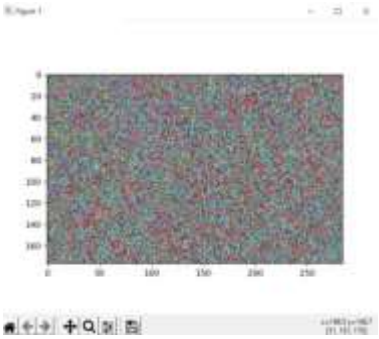


Image After Zigzag Scan



Zigzag Scanned Encrypted Image

IX. CONCLUSION

A new Joint Image Compression and Encryption strategy is presented and implemented to reduce the concept of expensive resources such as hard drive and transmission bandwidth. This proposed technique ensures the user's data privacy and confidentiality without compromising the data's quality.The performance of the proposed scheme is evaluated using compression ratio.

X. FUTURE ENHANCEMENT

NEXT GENERATION (.next-gen) pictures are image formats that outperform their JPEG(.jpeg) and PNG(.png) progenitors in terms of compression and quality. These next-generation image formats have the added benefit of consuming less data while keeping great quality.The Next Generation Image Formats lower the size of image files without sacrificing quality. The image extensions listed above are good at compression but not so good at security. As a result, in future applications such as internet communication, multimedia systems, medical, and military imaging systems, we will prioritise both compression and security.

XI. REFERENCES

[1] Mohammed Rasheed Omar, M.saligh , Mohammed siddeq , Joint Image Compression and Encryption Schemes based on Hexa Coding. ISSN 2303-4521(2021)

[2] Pratibha Chaudhary,Ritu Gupta,Abhilasha Singh, Pramathesh, Majumder, Ayushi Pandey, Joint Image Compression and Encryption using a novel column-wise scanning and optimization algorithm.167(2020)244-253

[3] Xinsheng Li,Taiyong Li,Jiang Wu,Zhilong Xie,Jiayi Shi,Joint Image Compression and Encryption based on sparse Bayesian learning

and bit-level 3D Arnold cat maps(2019)

[4] Xinpeng Zhang, Yanli Ren, Liquan Shen ,Zhenxing Qian and Guorui Feng ,Compressing Encrypted Images with Auxiliary Information.1520-9210(2013)

[5] AnilKumar.A,Anamitra Makur Makur, Distributed Source Coding based Encryption and Lossless Compression of Gray Scale and Color Images.978-1-4244-2295(2008)

[6] Younes M.A.B, Jantan.A, An image encryption approach using a combination of permutation technique followed by encryption, Int. J. Comput. Sci. NetworkSecur. 8 (4) (2008) 191–197.

[7] Faragallah.O.S, Efficient confusion–diffusion chaotic image cryptosystem using enhanced standard map, SIViP 9 (8) (2015) 1917–1926.

[8] Mitra.A, Rao.Y.S, Prasanna.S, et al., A new image encryption approach using combinational permutation techniques, Int. J. Comput. Sci. 1 (2) (2006) 127-131.

[9] Ponnain.D,Chandranbabu. K,Crypt analysis of an image encryption algorithm and an enhanced scheme, Optik-Int. J. Light Electron Opt. 127 (1) (2016) 192–199.

[10] Kurihara.K, Shiota.S, Kiya.H, An encryption-then-compression system for jpeg standard, in: 2015 Picture Coding Symposium (PCS), IEEE, 2015, pp. 119–123.