International Journal of Advances in
Soft Computing and Intelligent Systems (IJASCIS)
2023, Vol 02, Issue 01, 48-55

Science Transactions © 2023

Original Paper

A SECURE AND EFFICIENT IMAGE ENCRYPTION AND COMPRESSION APPROACH FOR PSEUDO COLOR IMAGE IN CLOUD STORAGE

Mamta Khanchandani [1]*, Dr. Sanjay Buch[2]

[1]Research Scholar, Bhagwan Mahavir University,
mamta.mk22@gmail.com
[2]Dean, Bhagwan Mahavir College of Computer Application, Bhagwan Mahavir University, drshbuch@gmail.com

Abstract

Due to the growing need for data and information transmission in a safe and secure manner, cryptographic and compression techniques are being used to protect and secure images. Cloud as a blooming technology offers numerous applications and services in today's market to user's on-demand in an inexpensive way. One can say that it is rightly hyped. The demand to store a large number of images on social media, E-Health and other domains has increased drastically over the years. Because of this increasing usage of digital images, an encryption technique followed with a compression technique that is faster and efficient is needed for cloud applications. The digital images are stored in the cloud server that can be accessed by the user when requires. This paper proposes a structured and comprehensive work of image cryptography and compression using hybrid encryption and Deep Learning in order to encrypt the image and also to reduce the storage capacity of the data with images. The strategy can provide storage efficiency through the way of compressing and reconstructing the image in future when needed.

KEYWORDS

Image encryption, Image compression, CNN, Autoencoder

1. INTRODUCTION

In Cloud computing provides various resources and services on demand over the network for instance platform, software and infrastructure. It facilitates huge storage capacity and builds a virtual infrastructure for its users using remote computing. Few examples of cloud computing service providers are Google, Amazon, IBM, etc. These service providers also offer data storage like Simple Storage Service (S3) construct on Google Drive and the Amazon EC2 along with online access to other resources. It also increases storage efficiency by raising the data availability and faster processing of data over the cloud. It rents virtual machines and storage space to store information, organizational data and application data. It achieves storage from optical storage media, flash memory, magnetic tapes and disks attached to network storage in storage space management. In today's world, the most effective way of representing information i.e., digital images have scattered the network and taken up much of the storage space. Using communication lines where images are sent is prone to being intercepted or stolen by eavesdroppers, which makes data safety of the utmost concern. The process of hybrid encryption leads to the image security for the user to store images on cloud storage. This techniques is followed with image compression to compress the data for transmission applications and data storage in a favorable way that reduces transmission time and bandwidth. Image Compression comprises two methods: Lossless compression and Lossy compression. Lossless compression is adequate for the reason that there is no loss of data over cloud storage in this technique. Whereas in Lossy compression, a little loss of information occurs but it goes unnoticed in the human eye.

A) IMAGE ENCRYPTION

If images are to be kept private and sent safely, encryption is essential. To perform the encryption process, the input image's pixel intensity must be warped in order to produce a cypher image. that differs greatly from the image input. The receiver decrypts the message using the secret keys. images and then gives you the original picture. The sender and receiver each use a different private key. They are also employed in asymmetric key cryptography to produce the shared secret key On the On the other hand, symmetric-key cryptography uses a single key for both encryption and decryption. The identity of the sender and recipient is known only to them .

B) IMAGE COMPRESSION

Going a step deeper into data security, we consider image security. It becomes extremely necessary to protect private and copyrighted images since images form a major part of online data in the cloud. There has been a noticeable shift in the trend of saving personal images and videos on the cloud as a backup. This gives birth to various data security issues on the cloud pointing out to the fact that digital images are not completely protected in the cloud. There is a possibility of a massive breach on the cloud which might result in personal data getting leaked. This is why an efficient algorithm is a must for image security. The digital images need to be compressed first before storing them over the cloud to minimize storage space. Compression is a representation of an image in a minimal number of bits (Chowdhury and Khatun 2012). The following compression ratio is used to quantify the compression achieved by the following formula:

$$CR=n1/n2$$

Wheren1 denotes the number of bits in the original image

n2 denotes the number of bits in the compressed image.

In most cases, only those bits that carry important information are considered. The first step in image security is image compression but the selection of the image compression technique should be such that it is compatible with the cloud computing system. Table 1 presents the description of the image compression methods (Katharotiya et al. 2011)

Table 1 Methods of image compression

Method of Compression	Description
1) DWT (discrete wavelet transform)	1) Has a larger compression ratio. 2) Identifies which data is more important to human perception. 3) Uses a more optimal set of functions for the sharp edges.
2) DCT (discrete cosine transform)	1) Has better performance time. 2) Uses coefficient optimally. 3) Does not result in a block-like appearance.

Comparison of discrete wavelet transform and discrete cosine transform: Image compression and decompression methods (Gupta and Choubey 2015)

2. RELATED WORK

Al-Maadeed et al[39] combined approach of selective image encryption and compression was put forth. The main goal of this suggested technique is to show how using multiple keys can increase security by upping the number of external keys used in each encryption operation. An encryption technique based on chaos that approximates the outcomes of the DWT transformation is used during the encryption process.

In their combination of lossless compression using the Quadtree and Huffman coding method and symmetric cryptosystem using the partial method, Hassan and Younis[41] proposed a way to incorporate encrypted data into compressed data using the AES method.

A hybrid picture encryption-compression technique based on CS and random pixel exchange was proposed by Zhou et al.[45], where compression and encryption are carried out simultaneously. The first compresses and encrypts the image by splitting it into four blocks. After that, the randomised pixels are exchanged and compressed and encrypted.

A CS-based encryption approach that effectively combines sampling, compression, and encryption was also proposed by Huang et al. [46]. The testing results show that the suggested encryption method does not produce exceptional unpredictability; even the diffusion and sensitivity method, when used concurrently, performs better than image encryption.

Autoencoders were initially considered as the default image compression neural network because of their ability to reduce dimensions, extract complex visual representations, and convert images to compressed binary formats [15]and other applications. Nowadays, various auto encoders used to capture hidden representations directly have been gaining so much popularity due to their parameterization trick and generative nature[12].

Over the years, the image compression study using Deep Learning has gone beyond autoencoders. Toderici et al[1] proposed variable-rate image compression that presents a recurrent neural architecture based on convolutional LSTMS (Conv. LSTM). Earlier, neural networks required a fixed compression rate. But this framework compresses 32*32 sized images that help obtain better SSIM values than JPEG. However, it was limited to 32*32 sized images. The researcher presented [2] another method where images of varied size could be used; provided they were multiples of 32*32. The results of the second research were superior to JPEG results.

Johnson et al [4] further researched by incorporating hidden-state priming, spatially adaptive bit rates and SSIM weighted loss and obtained improved results. [3] It trains autoencoders for image compression, out-performing the RNN based approaches and make auto encoders efficient with the help of sub-pixel architecture. It implements a recurrent autoencoder for image compression that supports spatially adaptive bit rates and a loss function built on structural similarity (SSIM). It presents non-line art transform coding for image compression, optimized end-to-end for rate-distortion performance. [6] It implements GAN’s for image compression that helps in obtaining significantly lower bit rates than the previous state of the art.

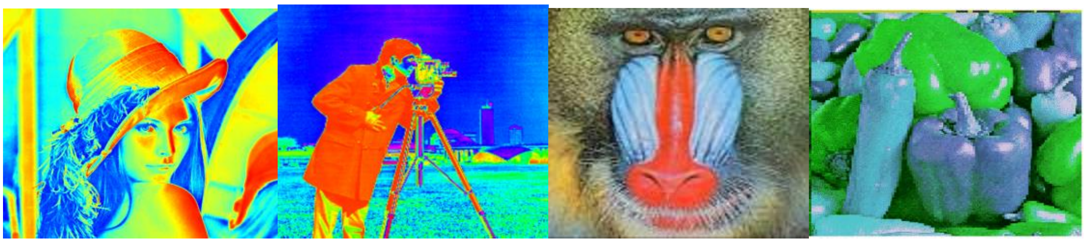


Figure 1. pseudo color images

2.1. DATA

Figure 1, four pseudo color images are selected i.e.Lena ,Cameraman, Babbon and Pepper. All the images are of varying sizes having varied content. The CNN encoder required fixed-size inputs for the fully connected layer.

3. METHODS, EXPERIMENTS AND RESULTS

3.1. Hybrid encryption and compression technique

The Elliptic Curve Cryptography (ECC) with Hill Cipher (HC) image encryption and decoding methods are combined.

Km = K- 1 is a self-invertible matrix that is created for Hill Cipher. The self-invertible matrix is a 2 by 2 size. By using the most original picture pixels to create the corresponding cypher pixels, a self-invertible matrix of 4 x 4 size performs the encryption and decryption process relatively faster and causes more distortion in the encrypted image. It is not necessary to send the matrix along with the encrypted image because it may be derived from the shared secret key. This technique focus on the encryption and decryption process of pseudo color image.

3.2. Evaluation Metric

We have evaluated our results in terms of PSNR (Peak Signal to Noise Ratio) and Structured Similarity (SSIM) in the field of image compression. PSNR is the ratio between the maximum possible power of a signal and the power of corrupting noise.[9] It is most easily defined in terms of mean squad error (MSE), which is the cumulative squared error between the compressed and the original image.

Given an image l (x, y) of size (M*N) and the compressed version l' (x, y), MSE and PSNR are defined in the equations below[10]: MSE = 1 MN Σ My = 1 Σ Nx = 1[l(x, y)-l 0 (x, y)] 2 PSNR = 20*log 10 255√MSE

A higher value for PSNR/a lower value for MSE means less error between the original and compressed image.

SSIM is another evaluation metric for gauging the similarity between two images. PSNR and MSE consider an estimate of the absolute error whereas SSIM considers the perceived change in structural information while incorporating perceptual phenomena such as luminance masking and contrast masking.[11]

To calculate SSIM between two images, we have used the SSIM function that takes values between 0.0 and 1.0. A higher value indicates a higher similarity between the two images. For autoencoders that produce a fixed-size encoding, the compression rate and the space are also considered evaluation metrics. There is a natural trade-off between reducing the size of an image and maintaining the quality of the image. The input image having a perfect SSIM and PSNR score will be the 'compressed' version. Practically, it is useless as it occupies the same amount of space. As we go on reducing the size of the image, the quality of the image also drops. Let us know about this aspect of image compression with the following:

$$\textit{Compression ratio} = \frac{\textit{size of uncompressed image}}{\textit{Size of the original image}}$$

2.3. CNN AUTOENCODER

Autoencoders are a deep neural network model that can take input data, propagate it through several layers to condense and understand its structure, and finally generate that data again. To complete this task, an autoencoder uses two different types of networks: an encoder and decoder. The decoder is a reflection of layers inside the encoder.

Simple convolutional autoencoder architecture is our first model of study. It consists of an encoder that takes in an input image and generates a code (an intermediate representation of the compressed image). It consists of a decoder that takes in the code and reconstructs a lossy version of the original input.

For the baseline architecture, the encoder is a convolutional layer, followed by a non-linearity (ReLU), and later followed by a dense layer. This creates the compressed form of the image (the code). The decoder is a de-convolutional layer, followed by a non-linearity and this non-linearity act as a sigmoid for the output to have pixel values in the same range as the original output. The architecture is shown in Figure 2.

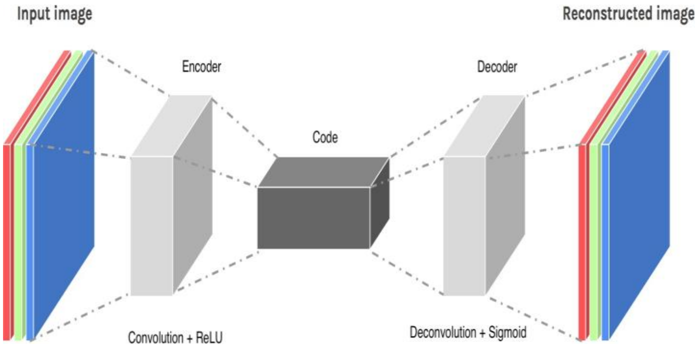


Figure 2 CNN autoencoder architecture

Table 2 Results of both the auto encoder models on test set

	Conv. AE	**VAE**
Average PSNR	71.05	58.17
Average SSIM	0.93	0.21
Compression Ratio	0.01	0.13

3. EXPERIMENTS

3.1. ENCRYPTION PROCESS:

(A) read the image to be encrypted and collect the image pixels separately for the channels r, g, and b.

(B) Group every channel of pixels into 4 x 4 matrices and perform matrix multiplication with computed self-invertible matrix.

(C) The encryption is done using the subsequent formula:

$$Ci = km \, . \, Pi$$

Where, km is the self-invertible matrix and pi is the current input image block to be encrypted;

(D) Allocate the cipher pixels exactly to the same position as of the corresponding input image pixels. A cipher image is formed of size identical to the size of input image.

(E) Send the cipher image and ecc public key to the receiver. The encryption process can be visualized as in figure 3,4,5,6.

(F) Since the cnn autoencoder model has fully connected layers with images of varying sizes, all the images are resized to be of the same size (128*128).

(G) The convolutional layer has been chosen in the encoder for 32 filters, each of size 3*3 and stride 1. The output has been transformed from a convolutional layer into a code of dimensions 1*128 with the help of a fully connected layer

(H) There are 3 channels in the de-convolutional layers in the decoder that made the output match the original input (1*1 filters). This baseline model is based on the training set of 585 images using adam optimizer and mse as the loss function.

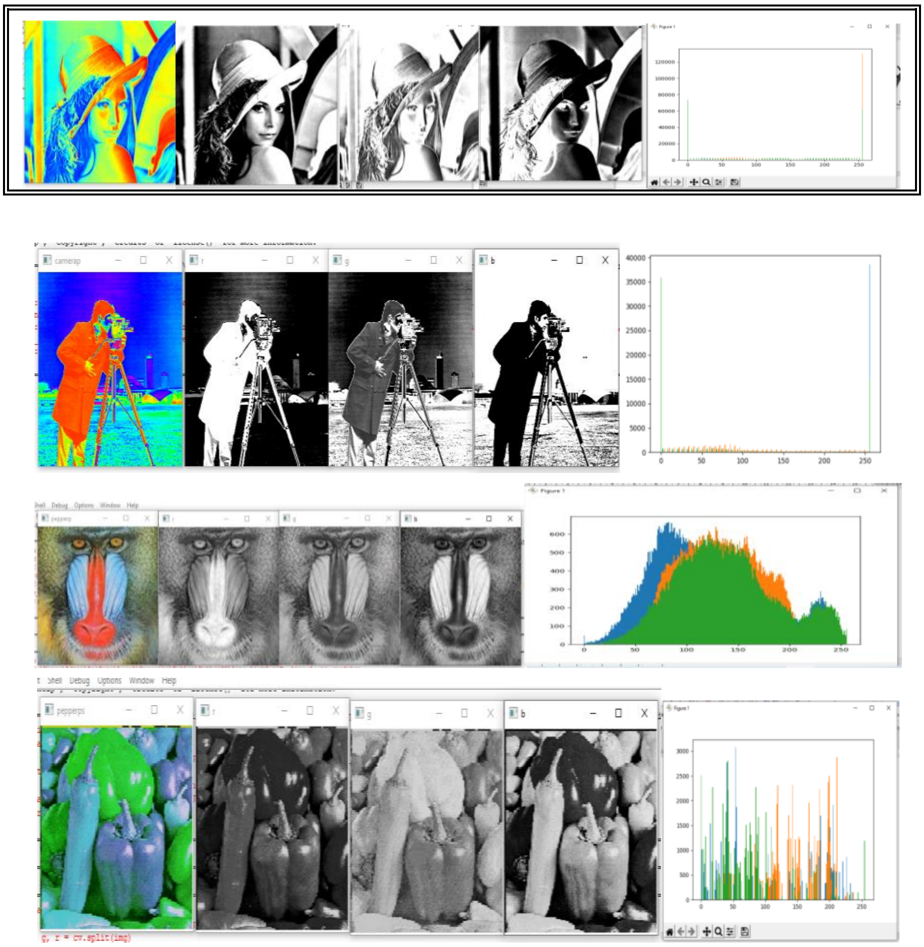
(I) The learning rate has been tuned from range 1e-1 to 1e-4 using the validation set provided (41 images). The model with the lowest loss on the validation set was evaluated on the test set.

4. RESULTS

The model with the highest PSNR and SSIM scores was trained with the learning rate 1e-3. Table 1 shows the results of our best models on the test set. The table represents a list of average PSNR and SSIM scores on the test set with the compression rate. Here,

$$\text{Compression ratio} = \frac{128 \times 4}{128 \times 128 \times 3}$$

This is because the compressed image (code) is of size 1*128 with floats and the original image is of size 128*128*3 with Unit8 characters.



```
g, r = cv.split(img)
```

Figure 3-6 Left: Original images. Right: Compressed images

Figure 3,4,5,6 shows few illustrations of encrypted and compressed images from the model. The model performs well despite the significant encryption and compression of pseudo color image. The drawback of this model is that variable-rate encoding is not possible which means in order to change the compression rate; the autoencoder needs to be retrained.[1]

5. Conclusion

The hybrid compression-encryption technology has such a low computational cost that it is capable of boosting the efficiency and security of images that are   transfered while still being able to guarantee actual data security. As a result, the concept is eligible for and may enhance data security and transmission efficiency by enhancing the effectiveness of each compression and cryptography technique individually. This idea is anticipated to be able to combine the best qualities of lossy and lossless compression techniques with the disadvantages of symmetric and asymmetric cryptographic methods, particularly with regard to cypher key management, to produce data that is much smaller in size while maintaining high quality during reconstruction and security assurance. With the rapid development and usage of handheld cameras, the photography skills and their cost have become much lower than before. Users all over the world have been capturing and posting photos using their mobile phones, digital cameras and other portable devices largely on a daily basis. People use it to share their day-to-day life, experiences and promote the business as well. Storing and maintaining these huge amounts of photos securely has become a necessity nowadays. Here, we propose our CNN based autoencoder image compression method to compress image size and encrypt the image cryptography using hybrid encryption in the cloud and increase the storage space in the drive.

REFERENCES

1. Toderici, g., o'malley, s. M., hwang, s. J., vincent, d., minnen, d., baluja, s., ... & sukthankar, r. (2015). Variable rate image compression with recurrent neural networks. Arxiv preprint arxiv:1511.06085.
2. Workshop and challenge on learned image compression (https://www.compression.cc)
3. Wikipedia-peak signal-to-noise ratio (https://en.wikipedia.org/wiki/peaksignal-to-noiseratio. Http://www.debugmode.com/imagecmp/
4. Wikipedia-structural similarity (https://en.wikipedia.org/wiki/structuralsimilarity)
5. Shankar, k., elhoseny, m., kumar, r. S., lakshmanaprabu, s. K., & yuan, x. (2020). Secret image sharing scheme with encrypted shadow images using optimal homomorphic encryption technique. Journal of ambient intelligence and humanized computing, 11(5), 1821-1833.
6. Chowdhurymmh,khatuna(2012) image compression using discretewavelet transform. Int j comput sci 9(4):327–330
7. Katharotiya a, patel s, goyani m (2011) comparative analysis between dct&dwt techniques of image compression. J inform eng appl 1(2):9–18
8. Diederikpkingma,maxwelling-“auto-encodingvariationalbayes”,arxiv:1312.6114
9. G. E. Hinton and r. R. Salakhutdinov. Reducing the dimensionality of data with neural networks. Science, 313(5786):504507, 2006.
10. P. Vincent, h. Larochelle, y. Bengio, and p.-a. Manzagol. Extracting and composing robust features with denoising autoencoders. Journal of machine learning re-search,2012
11. Toderici et al. Full resolution image compression with recurrent neural networks, google arxiv
12. Johnston, n., vincent, d., minnen, d., covell, m., singh, s., chinen, t., ... & toderici, g. (2018). Improved lossy image compression with priming and spatially adaptive bit rates for recurrent networks. In proceedings of the ieee conference on computer vision and pattern recognition (pp. 4385-4393).
13. Ballé, j., laparra, v., & simoncelli, e. P. (2016). End-to-end optimized image compression. Arxiv preprint arxiv:1611.01704.
14. Agustsson, e., tschannen, m., mentzer, f., timofte, r., & gool, l. V. (2019). Generative adversarial networks for extreme learned image compression. In proceedings of the ieee/cvf international conference on computer vision (pp. 221-231).
15. S. Al-maadeed, a. Al-ali, and t. Abdalla, “a new chaos-based image-encryption and compression algorithm,” journal of electrical and computer engineering, vol. 2012, pp. 1–11, 2012.
16. N. S. Hassan and h. A. Younis, “approach for partial encryption of compressed images,” journal of babylon university/pure and applied sciences, vol. 21, no. 3, pp. 1–10, 2013.
17. R. . Huang, k. H. . H. Rhee, and s. . Uchida, “a parallel image encryption method based on compressive sensing,” multimedia tools and applications, vol. 72, no. 1, pp. 71–93, sep. 2014.
18. Ahmad, J., Khan, M. A., Hwang, S. O., & Khan, J. S. (2017). A compression sensing and noise-tolerant image encryption scheme based on chaotic maps and orthogonal matrices. Neural computing and applications, 28, 953-967.