Implementation and Performance Evaluation of Asymmetrical Encryption Scheme for Lossless Compressed Grayscale Images

Neetu Gupta[1(✉)], Hemant Kumar Gupta[2], K. Swapna[3], Kommisetti Murthy Raju[4], and Rahul Srivastava[2]

[1] Department of Computer Science and Engineering, Manipal University Jaipur, Jaipur, Rajasthan, India
neetu.gupta@jaipur.manipal.edu

[2] Department of Electronics and Communication Engineering, Arya College of Engineering & I.T., Jaipur, Rajasthan, India
rahu_79@rediffmail.com

[3] Department of Electronics and Communication Engineering, Vaagdevi College of Engineering, Warangal, Telangana, India
swapna_k@vaagdevi.edu.in

[4] Department of Electronics and Communication Engineering, Shri Vishnu Engineering College for Women, Bhimawaram, Andhra Pradesh, India
Venkateswara.103@svecw.edu.in

Abstract. The employment of compression and encryption methods enables the transmission of images across a communication link with less bandwidth consumption and resistance against differential assaults. In this study, the gray scale images are compressed using the Huffman lossless compression approach. Each pixel is given a unique prefix code with a configurable length in this. The frequency of occurrence of characters has an inverse relationship with prefix code length. Asymmetrical RSA encryption is used to encrypt compressed images. In the RSA encryption technique, the encryption key is kept in the open as opposed to the decryption key, which is kept private. Analysis of the compression parameters, together with correlation coefficient and entropy analysis, is used to convey the effectiveness of suggested techniques. Five 512 × 512 grayscale test images are used as text images and to verify the results.

Keywords: Huffman Lossless Compression · RSA asymmetrical encryption · Correlation Coefficient analysis · Grayscale Images

1 Introduction

Compression techniques are used during transmission to efficiently convey the information via a medium of communication with a smaller bandwidth [1–4]. The redundant substance from the original information source is removed during the compression process so as to reduce the amount of the information. Lossy compression methods have

P. Pareek et al. (Eds.): IC4S 2023, LNICST 536, pp. 403–413, 2024.
https://doi.org/10.1007/978-3-031-48888-7_34

a high rate of compression, they may also exclude some crucial information, whereas lossless compression approaches keep the information's integrity and certainty while compressing it enough [5, 6]. Another crucial factor is protecting the data during transmission from different unethical assaults. During transmission, encryption methods are combined with the data to ensure data secrecy [7]. Both symmetrical and asymmetric encryption methods are possible. Key creation is typically used to accomplish encryption. The transmitter key and receiver key in symmetrical encryption processes are identical, which makes it possible to intercept information in transit [8]. Using an asymmetrical encryption technique, where the receiver key is private but the sender key is public, can enhance security characteristics.

Both the compression and encryption processes are crucial for secure data transfer on lowered bandwidth. It is possible to use the compression technique either after or before the encryption. When encryption is applied to an un-compressed image, execution time is prolonged and the encryption process is misused [9, 10]. By adopting a compression strategy before encrypting an image, the likelihood that hackers will be able to decode it is decreased [9, 11, 12].

In this study, the RSA asymmetric encryption method is used after the Huffman lossless compression algorithm. The compression efficiency metrics Peak signal to noise ratio (PSNR), Mean square error (MSE) and Compression ratio (CR) are investigated to assess the performance of image reconstruction by comparing them to existing methods. The encryption efficiency of the proposed technique is assessed using entropy and coefficient of correlation studies. Five typical grayscale test images with a 512×512 pixel size are used for the research experiment.

2 Related Work

M. Yassein et al.'s study on several encryption methods in the symmetrical and asymmetrical categories was published in 2017 [13]. The asymmetrical encryption algorithm RSA is contrasted with the symmetric encryption techniques 3DES, AES, Blowfish, and DES. The RSA encryption approach offers higher protection against various assaults, as shown by the authors' analysis of the symmetrical and asymmetrical encryption algorithms using various metrics for evaluating encryption performance. Galla et al. [14] executed RSA technique for image data encryption in 2016. The authors have shown how the RSA method depends on number factorization. Jumgekar et al. [15] also developed and illustrated basic cryptanalysis in 2013 and explained the implementation of RSA method through the production of public and private keys. A RSA encryption technique was introduced by Jonsson et al. [16] in 2002, and it was compared to the incomplete RSA algorithm. Authors have demonstrated that security characteristics based on pseudo-random functions are diminished by TLS-based algorithms. By modernizing the computing procedure, Katz et al. [17] demonstrated the contemporary cryptanalysis method in 2014, which lowers the drawbacks of complete secrecy. Authors have employed a private key encryption technique and message signal authentication.

S. Han et al. [18] solved the neural network restrictions in 2016 by demonstrating the deep compression technique. Pruning, quantization, and Huffman coding are all components of this deep compression technique. The deep compression strategy, according to the authors, lowers the need for storage without compromising the accuracy of

the rebuilt image. To improve the compression effectiveness and privacy of text-based information, E. Satir et al. [19] published a lossless Huffman compression approach in 2014. A lossless image compression technique comparable to bzip2 was devised in 2012 by Y. Zhang et al. [20] with the goal of parallelizing the development of Huffman coding, BWT and MTF. To demonstrate the advantages and disadvantages of the recommended algorithms, a performance study is also conducted.

Using LZW and Run length encoding, M. Sharma [21] examined Huffman compression approach in 2010. The author shows that Huffman coding has a higher compression ratio and efficiency than other compression techniques.

According to a survey of the literature, Huffman coding is the most popular lossless compression method, which encourages future study to increase the reconstructed image compression ratio and effectiveness. This research paper goal is to apply asymmetrical encryption on lossless compressed grey scale photos and examine the results.

3 Fundamental Information and Proposed Model

A form of lossless compression method based on how frequently pixels occur in visual data is called Huffman coding (Fig. 1).

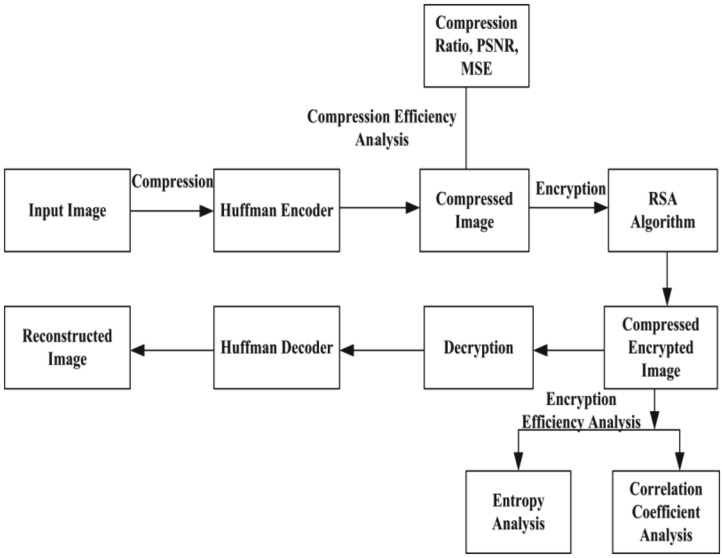

Fig.1. Fundamental structural representation of suggested system paradigm

In the Huffman coding, Image pixels are placed according to their frequency in decreasing order. Once more, each pixel is ordered in decreasing order of frequency of occurrence after merging the frequencies of the two pixels with the lowest frequencies. This procedure will continue until there are only two frequencies of pixels left. The last

two pixel frequencies are stored by giving higher frequency pixels a value of 0 and lower frequency pixels a value of 1.

Algorithm for Compression

 # Every pixel value is shown through 8 bits, each of which has a symbol and values ranging from 0 to 255.

- *Use I = imread(file) to read relevant input image.*
- *Use I = rbg2gray(file) to convert a colour image to a grayscale image if the original image was colour.*
- *Use [m,n] = size(I) to calculate the image's size.*
- *Utilise the programme to calculate the cumulative probability.*
- *Sum (k(:)) = count (cnt)*
- *Count (cnt) = Pro(cnt)/Total number of count*
- *Sigma plus Pro(cnt) equals Cumpro(cnt)*
- *Use dict = huffmandict(symbols, pro) to invoke the Huffman code dictionary.*
- *A vector is created from an array of symbols using the formula newvec (vec-size) = I (m,n)*
- *The statement hcode = huffmanenco(newvec, dict) is used to conduct Huffman encoding.*
- *Dhsig1 = huffmandeco(hcode,dict) performs the Huffman decoding.*
- *Calculate MSE, PSNR and compression ratio.*

RSA generates two unique keys. A public key has been allotted to the transmitting side of the communication. The recipient is given a private key in addition to another key. The choice of two enormous prime integers is key to the security of this procedure. The three essential components of the RSA encryption technique are key creation, encryption, and decryption.

Algorithm for Encryption

 # Encryption and decryption keys are both produced during key production.

- *Using the primer testing method, find two distinct integer prime values with same bit length, g and h.*
- *Use n = g h to calculate the key length in bits.*
- *Make sure that the encryption key e is chosen so that it cannot be a combination of 1e(g,1,h) and (g,1,h). A public key can be formed by (n,e).*
- *Choose the private decryption key d such that 1d(g-1)(h-1) and (d e)mod (g-1)(h-1) = 1.*
- *Divide the picture I into a series of blocks where each block meets the condition 0 Ii n. Put these blocks into an encryption using the equation E = Ie mod (n).*
- *Using the formula D = Ed mod (n), decryption can be performed of mage E.*

4 Evaluation of the Effectiveness of Compression and Encryption

4.1 Parameters for Evaluating Compression Efficiency

To evaluate the efficacy of the Huffman compression approach, PSNR and MSE are used. For an image to be successfully reconstructed, the PSNR must be high, or over 30 dB, and the MSE must be as low as possible.

$$\text{PSNR} = log_{10}\left[\frac{\{J \times K\}^2\}}{MSE}\right] \tag{1}$$

$$\frac{1}{J \times K}\sum_{X=1}^{J}\sum_{Y=1}^{K}[u(x,y) - v(x,y)]^2 \tag{2}$$

where $u(x, y)$ and $v(x, y)$ denotes the uncompressed and compressed pixel respectively.

4.2 Parameters for Evaluating Encryption Efficiency

4.2.1 Analysis Based on Entropy

The average amount of information in a lengthy string of pixels in an image data is referred to as entropy.

I(Xi) has m distinct symbols, and the mean value or entropy is given by

$$H(X) = \sum_{i=1}^{j} P(X_i)I(X_i) \tag{3}$$

$$H(X) = \sum_{i=1}^{j} P(X_i)\log_2 P(X_i) \tag{4}$$

4.2.2 Analysis Based on Correlation Coefficient

The correlation coefficient between two neighboring pixels on the horizontal, vertical, and diagonal axes is used to describe the correlation between the original and encrypted image. This is how the correlation coefficient is shown:

$$C = \frac{\sum_{i=1}^{j}(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\sum_{i=1}^{j}(x_i - \overline{x})^2} \times \sqrt{\sum_{i=1}^{j}(y_i - \overline{y})^2}} \tag{5}$$

where $\overline{x}$ and $\overline{y}$ can be expressed as

$$\overline{x} = \frac{1}{K}\sum_{i=1}^{k} x_i \text{ and } \overline{y} = \frac{1}{K}\sum_{i=1}^{k} y_i \tag{6}$$

The original image's neighboring pixels must be significantly connected with one another in the horizontal, vertical, and diagonal dimensions. As a result, the correlation coefficient must be high. However, an encrypted image should have little to no pixel correlation and a low correlation coefficient.

5 System Environments

MATLAB 2018 is used in this experimental investigation to simulate the outcomes. Operating system utilized is Windows 10. 512×512 standardized grayscale test pictures. To authenticate the outcomes, we use the bmp format from the SIPI data store.

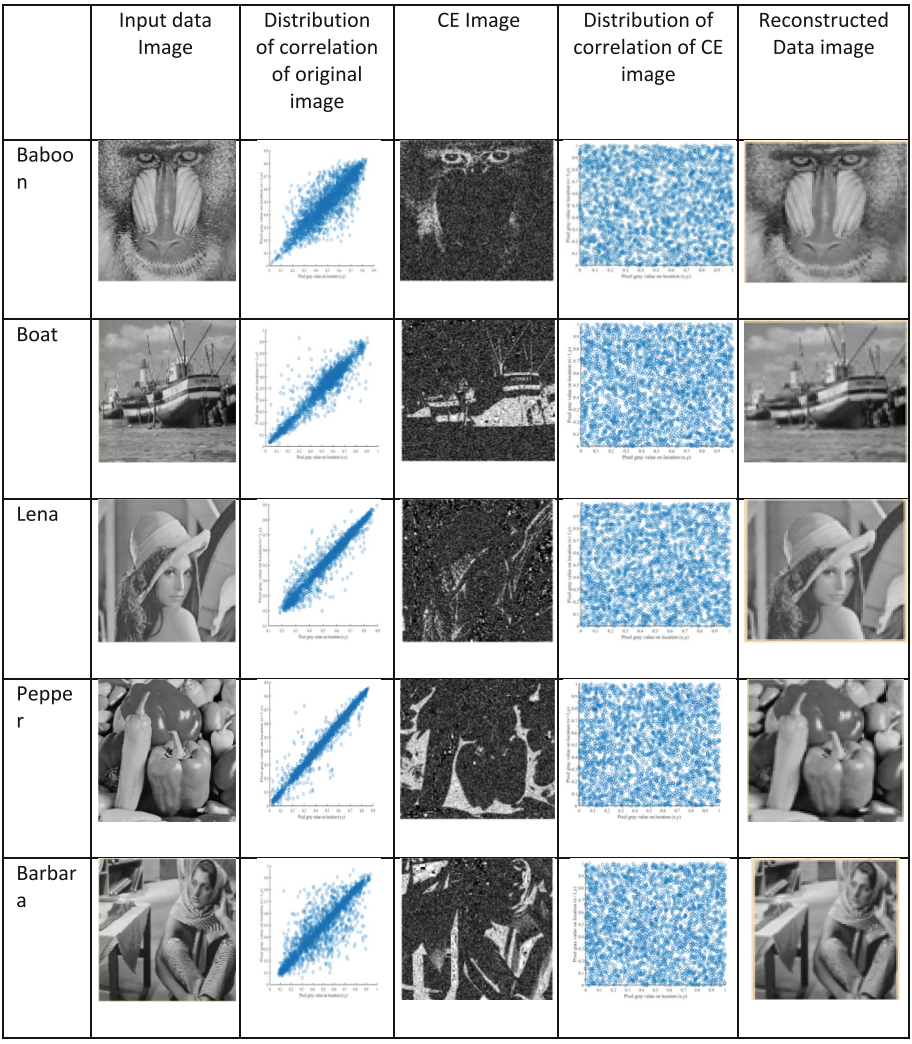

Fig. 2. Representation of pictorial outputs during proposed compression and encryption process

6 Results of Proposed Model

Table 1 displays results for compression efficiency parameters. Existing techniques are also contrasted. The compression efficiency is represented by CR, PSNR, and MSE. Graphical depiction of compression efficiency characteristics is shown in Fig. 3.

Columns 2 and 3 of Fig. 2 display the input image and distribution of the associated correlation coefficients, respectively. Columns 4 and 5 respectively display the compressed encrypted (CE) picture and the distribution of the related correlation coefficients, while column 6 displays the reconstructed image following decryption and decompression (Table 2).

Table 1. Results obtained for proposed CE technique in terms of MSE, CR and PSNR

Title	CR		PSNR in dB		MSE	
	Proposed scheme	Existing Studies	Proposed Scheme	Existing Studies	Proposed Scheme	Existing Studies
Baboon	2.9045	NA	29.3446	21.23 [22]	44.531	126.83 [22]
Boat	5.3956	NA	34.5563	29.68 [23]	16.2547	NA
Lena	7.8546	5.83 [24]	36.0938	29.57 [25]	7.3748	163.56 [26]
Pepper	7.4567	3.99 [27]	38.1706	31.26 [27]	5.5758	37.760 [27]
Barbara	4.8568	NA	34.3487	21.81 [22]	15.235	289.76 [22]

Table 2. Results obtained for proposed encryption scheme in terms of entropy and Correlation coefficient

Title	V-Direction		D-Direction		H-Direction		Value of Entropy	
	Proposed Model	Existing Studies	Proposed Model	Existing Studies	Proposed Model	Existing Studies	Proposed Model	Existing Studies
Baboon	.0712	.0093 [28]	.0687	−.0251 [28]	.0886	−.0225 [28]	3.8652	7.9987 [1]
Boat	.2294	−.0064 [1]	.1920	.00007 [1]	.2176	.010 [1]	3.8863	7.9989 [1]
Lena	.2110	.0240 [28]	.1005	−.0411 [28]	.1352	−.0094 [28]	3.7257	7.9989 [1]
Pepper	.2521	.0093 [28]	.2144	−.0251 [28]	.2470	−.0225 [28]	3.9000	7.9988 [1]
Barbara	.2894	.0079 [1]	.2426	.0200 [1]	.2666	.0122 [1]	3.9308	7.9901 [1]

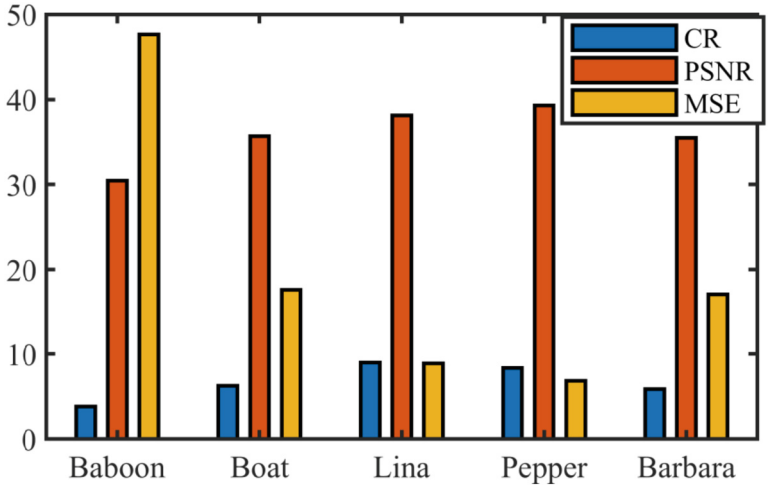

Fig. 3. Comparison chart among values of MSE, CR and PSNR

7 Conclusion and Future Scope

In this study, image data is compressed and encrypted using the Huffman lossless compression algorithm and RSA asymmetrical techniques. According to a review of the data, the dynamic range of the PSNR of the Huffman compression approach is lying between 30 to 40 dB, which is beyond the minimum requirement of PSNR for successful compression while it offers a sizable compression ratio. MSE, with a range of 6.85 to 47.64, is a less sophisticated algorithm than other cutting-edge ones. The low correlation coefficients of encrypted images show that the RSA encryption method is resilient to numerous attacks and the entropy being in the range of 3.72 to 3.93.

References

1. Tong, X.J., Chen, P., Zhang, M.: A joint image lossless compression and encryption method based on chaotic map. Multimedia Tools Appl. **76**(12), 13995–14020 (2017)
2. Singh, R.K., Kumar, B., Shaw, D.K., Khan, D.A.: Level by level image compression-encryption algorithm based on quantum chaos map. J. King Saud Univ. Comput. Inf. Sci. **33**(7), 844–851 (2018)
3. Gupta, N., Vijay, R., Gupta, H.K.: Performance analysis of DCT based lossy compression method with symmetrical encryption algorithms. EAI Endorsed Trans. Energy Web **7**(28), 1–11 (2020)
4. Daubechies, I., Barlaud, M., Mathieu, P.: Image coding using wavelet transform. IEEE Trans. Image Process. **1**(2), 205–220 (1992)
5. Maniccama, S.S., Bourbakis, N.G.: Lossless image compression and encryption using SCAN. Pattern Recogn. **34**(6), 1229–1245 (2001)
6. Zhang, X.: Lossy compression and iterative reconstruction for encrypted image. IEEE Trans. Inf. Forensics Secur. **6**(1), 53–58 (2011)

7. Al-Khasawneh, M.A., Shamsuddin, S.M., Hasan, S., Bakar, A.A.: An improved chaotic image encryption algorithm. In: International Conference on Smart Computing and Electronic Enterprise ICSCEE 2018, pp. 1–8, Shah Alam, Malaysia (2018)
8. Carpentieri, B.: Efficient compression and encryption for digital data transmission. Secur. Commun. Netw. **2018**, 1–9 (2018)
9. Setyaningsih, E., Wardoyo, R.: Review of image compression and encryption techniques. Int. J. Adv. Comput. Sci. Appl. **8**(2), 83–94 (2017)
10. Gupta, N., Vijay, R., Gupta, H.K.: Performance evaluation of symmetrical encryption algorithms with wavelet based compression technique. EAI Endorsed Trans. Scalable Inf. Syst. **7**(28), 1–14 (2020)
11. Sharma, M., Gandhi, S.: Compression and encryption : an integrated approach. Int. J. Eng. Res. Technol. **1**(5), 1–7 (2012)
12. Gupta, N., Vijay, R.: Hybrid image compression-encryption scheme based on multilayer stacked autoencoder and logistic map. China Commun. **19**(1), 238–252 (2022)
13. Yassein, M.B., Aljawarneh, S., Qawasmeh, E., Mardini, W., Khamayseh, Y.: Comprehensive study of symmetric key and asymmetric key encryption algorithms. In: Proceedings of 2017 International Conference on Engineering and Technology ICET 2017, pp. 1–7 Antalya Turkey (2018)
14. Galla, L.K., Koganti, V.S., Nuthalapati, N.: Implementation of RSA. In: 2016 International Conference on Control Instrumentation Communication and Computational Technologies ICCICCT 2016, pp. 81–87 Kumaracoil, India, (2016)
15. Jamgekar, R.S., Joshi, G.S.: File encryption and decryption using secure RSA. Int. J. Emerging Sci. Eng. **1**(4), 11–14 (2013)
16. Jonsson, J., Kaliski, B.S.: On the security of RSA encryption in TLS, Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 2442, pp. 127–142 (2002)
17. Katz, J., Lindell, Y.: Introduction to Modern Cryptography (2014)
18. Han, S., Mao, H., Dally, W.J.: Deep compression: compressing deep neural networks with pruning, trained quantization and Huffman coding. In: 4th International Conference on Learning Representations, ICLR 2016 - Conference Track Proceedings (2016)
19. Satir, E., Isik, H.: A Huffman compression based text steganography method. Multimedia Tools Appl. **70**(3), 2085–2110 (2014)
20. Patel, R.A., Zhang, Y., Mak, J., Davidson, A., Owens, J.D.: Parallel lossless data compression on the GPU. In: 2012 Innovative Parallel Computing, InPar 2012 (2012)
21. Sharma, M.: Compression using huffman coding. Int. J. Comput. Sci. Netw. Secur. **10**(5), 133–141 (2010)
22. Raja, S.P., Suruliandi, A.: Performance evaluation on EZW & WDR image compression techniques. In: IEEE International Conference on Communication Control and Computing Technologies, ICCCCT 2010, pp. 661–664 (2010)
23. Agarwal, C., Mishra, A., Sharma, A.: A novel gray-scale image watermarking using hybrid Fuzzy-BPN architecture. Egyptian Inform. J. **16**(1), 83–102 (2015)
24. Praisline Jasmi, R., Perumal, B., Pallikonda Rajasekaran, M.: Comparison of image compression techniques using Huffman coding, DWT and fractal algorithm. In: International Conference on Computer Communication and Informatics, ICCCI 2015, pp. 1–5 (2015)
25. Zhou, N., Pan, S., Cheng, S., Zhou, Z.: Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing. Optical Laser Technol. **82**, 121–133 (2016)
26. Dang, P.P., Chau, P.M.: Image encryption for secure Internet multimedia applications. IEEE Trans. Consumer Electron. **46**(3), 395–403 (2000)

27. Hu, F., Pu, C., Gao, H., Tang, M., Li, L.: Image compression and encryption scheme based on deep learning. Nauk. Visnyk Natsionalnoho Hirnychoho Universytetu **6**, 142–148 (2016)
28. Zhang, Y.: The unified image encryption algorithm based on chaos and cubic S-Box. Inf. Sci. (Ny) **450**, 361–377 (2018)