Indian Journal of Computer Science and Technology
Volume 3, Issue 1 (January-April 2024), PP 17-21.
www.indjcst.com **ISSN No: 2583-5300**

Review on RSA Cryptography, Steganography and Compression Techniques for Data Security

P. Jeno Paul[1], M I Thaslima[2]
[1]*Professor, EEE Department, ASIET, Kalady, Kerala, India.*
[2]*PG Student, CSE Department, ASIET, Kalady, Kerala, India.*

Abstract: *One of the earliest public key cryptosystems still in use for safe data transfer is called RSA (Rivest–Shamir–Adleman). Information hiding is a component of steganography. Since compressed data is easier to handle and more secure,data compression is a crucial component of information security. Efficient, safe, and readily connectable data is produced via effective data compression technology. Compression algorithm approaches come in two flavours: lossy and lossless. These methods are applicable to any type of data format, including audio, video, text, and image files. This study's primary goal was to decrease the amountof physical space on different storage devices and theamount of time it takes to transport data over the Internet while completely guaranteeing that the data would be encrypted and hidden from prying eyes. In this paper, the secret massage is encrypted using RSAcryptography and compressed using Huffman coding.A cover image is compressed using Discrete WaveletTransform (DWT). The compressed encrypted message is embedded into an image using Least Significant Bit (LSB).*

Keywords: *Cryptography, steganography, datacompression, Huffman coding, DWT, RSA, image compression.*

I.INTRODUCTION

Secret messages can now be conveyed by concealing them in a text or image such that only the sender and the recipient can read or see them. The process of hiding and revealing data is called steganography. Because it conceals the secret message, the image thatconceals data in steganography is referred to as a "cover image." The image that remains after the data has been hidden is called a "stego-image." LSB insertion is a widely used and well-liked method in steganography that embeds data in a cover file. According to the LSB embedding approach,information can be concealed in the LSBs of the coverfile so that not even the unaided eye can decipher the concealed information. It is a domain that is spatial.

One technique that transforms the communication into a useless format is cryptography. Thus, applying cryptography plus steganography will result in a double layer of security. Data compression has shown to be a successful energy-saving technique that lowers the volume of data that needs to be transferred across a network. The encrypted communication is compressedusing lossless data compression (Huffman coding). Tomake the message more easily hidden, image compression is utilised to lower the message's size [1]. One may say that one of the most important uses of digital image processing is image compression. The cover image is compressed using lossy image compression (DWT).

A. Basic Model

The secret message is encrypted using RSA cryptography, then compressed by Huffman's algorithm, and the cover-image is compressed by the DWT algorithm. then the cover-image is combined with the secret message via LSB and sent them over the Internet to the destination as a compressed file. These encoded streams (bits) are then sent to a decoder that decodes these streams (bits) and the final output imageis retrieved as a decoding file output. Lossy and lossless image decompression [5] is used to reduce the numberof bits required to represent an image.

B. RSA Encryption

Symmetric key algorithms and asymmetric key algorithms are the two general categories into which cryptographic algorithms fall. The key is used in symmetric encryption for both encryption and decryption. Although it is incredibly straightforward and simple to use, there are a few significant drawbacks. An attacker can quickly find the information if they know the unique key [6]. Two distinct keys are utilised for encryption and decryption in asymmetric key encryption. Only a particular user (the recipient) is aware of the private key; the public key is shared with all senders. However, the primary drawback of this key coding is that it is slower than symmetric algorithms [7].

Two different types of keys are public key and privatekey. Public key is known to all users and private is kept secret. In symmetric key cryptography, only one public key is used for both data encryption and data decryption. In asymmetric key cryptography, a publickey is used for data encryption and a private key is used for data decryption. So, there is less chance of data stolen and manipulated and data is more secure inpublic key cryptosystem.

The security of the algorithm is based on the rigidity of the analysis of a large number of compounds and a complex number for a specified odd integer (e) computation of the unit of moral roots. The RSA public key consists of an integer pair (n, e). Typical isthe result of multiplying 2 primes. Using the keyfeature of RSA, a variable key size, and cipher block to improve security [9].

To clarify RSA encryption and decryption as follows:

Key Generation Procedure:

Choose two distinct large prime numbers p & qsuch that p not equal to q.
Calculate n = p x q Calculate *8* (n) = (p-1) (q-1)
Choose an integer e such that gcd (*8* (n), e) = 1 ;1 < e < *8*(n)
Compute d to satisfy the congruence relationd = e^ −1 mod *8* (n); d is kept as private Public Key KU = {e, n }
Private Key KR = {d, n }
The public key is (n, e) and the private key is (n, d).Keep d, p, q and *8* secret.

Encryption:

Plaintext Message < n
Ciphertext C = Message^ e mod n

Decryption:

Ciphertext C
Plaintext Message = C^ d mod n

C. Steganography

Steganography is divided into four domains:

1. The spatial domain: This kind of technology often uses straightforward algorithms to implant private message segments into the cover media. One of the most well-known algorithms in the field is called LSB(least significant bits), and it substitutes LSB for the secret message bits in cover media. Although this alteration is not visible to the human eye, statistical tests can identify it [1], [3]. LSB techniques are easy to use and highly quick. 2. Transform domain: This group incorporates secure communications into cover media by transposition [4]. Included in these transformations are: Discrete Cosine Transform, or DCT: The cover media in this kind is separated into 8x8 blocks. A quantization table is used to quantize these blocks.

The cover medium in a DWT (Discrete WaveTransform) is separated into four main sub-bands (LL,HL, LH, and HH). The primary characteristics of covermedia reside in LL, and should a hidden message be contained within, it will remain intact even under varied compression settings [5].

Discrete Fourier Transform (DFT): This converts each input signal point into two output points. A combination of samples taken at regular intervals serves as the input signal for the DFT [6]. 3. Spread spectrum: Using this technique, the cover media noise produced during the picture acquisition process contains the hidden message. There is a payload capacity in this type of technique, which is a blind system [7]. 4. Model-based: Using this approach, the cover media is split into two sections. The initial segment will not be utilised throughout the embedding procedure. The second section contains the secret message without altering the cover media's statistical characteristics. One benefit of this approach is its great modulation capacity [8]. Some advantages of the transform domain include increasing the size of the secret message during the embedding process and having a high level of resistance against several knownassaults. One potential flaw is the lengthy embedding and extraction times caused by using more cover mediaor secret messages [10].

D. Compression Techniques

Two types of compression techniques are: Lossless data compression and Lossy image compression. **Lossless data compression** is a class of data compression that allows the original data to be perfectly reconstructed from the compressed data with no loss of information. Huffman coding is lossless data compression technique. Lossy image compression removes background data and approximates certaindetails of an image file, making it smaller and easier tohandle, store or send. Discrete Wavelet Transform is lossy image compression technique. Fig 1, illustrates the stages of the compression process.

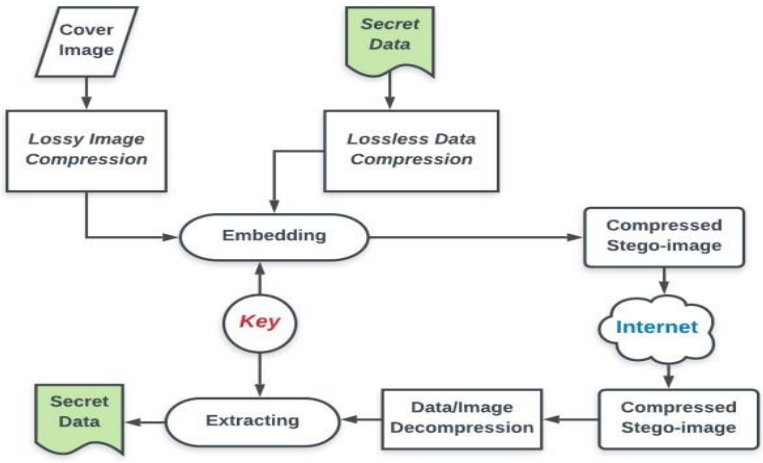

Figure 1. Block diagram of compression

E. Huffman Coding

Compared to other methods, Huffman coding has a number of advantages, such as lossless data compression, which can be inexpensive and efficient to use. Every data point is implemented, and it is thereafter sorted in ascending order. The process resulted in a Huffman tree, which may be used to restore data to its original state following compression. One of the earliest lossless image compression methods, huffman coding was created to minimise code repetition without sacrificing the quality of the reconstructed image. Let's look at utilising the following example to better understand the algorithm. The digital image has seven source codes (B1, B2, B3, B4, B5, B6, B7), each of which has a likelihood value (0.25, 0.25, 0.125, 0.125, 0.0625, and 0.0625). The procedure for acquiring.

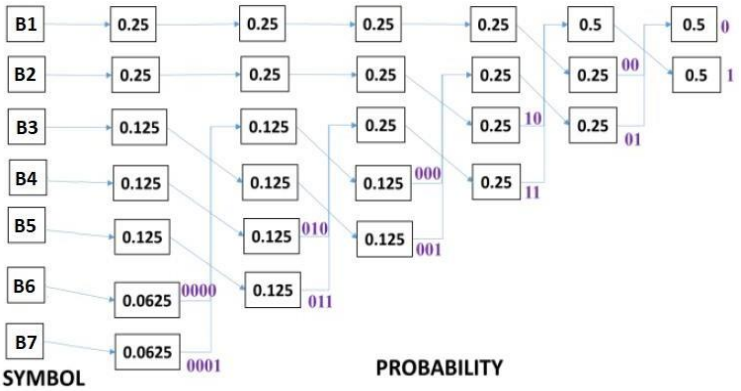

Figure 2: Huffman encoding: average wordlength=2.625 bits, bit assignment process

Symbol	Probability	Code Word	Length
B1	0.25	10	2
B2	0.25	11	2
B3	0.125	1	3
B4	0.125	10	3
B5	0.125	11	3
B6	0.0625	0	4
B7	0.0625	1	4

Table 1: Huffman encoding: code word

Lavg=0.25*2+0.25*2+0.125*3+0.125*3+0.125*3+0.0625*4+0.0625*4

Lavg=2.625 bits

F. Discrete Wavelet Transform(DWT)

Discrete wavelet transformations, which convert an image into a collection of wavelets that may be stored more effectively than blocks of pixels, are a potent tool in image processing. The signals are split into high and low frequencies for a single dimension. DWT is a significant technique that is essential to compressing an image without losing any of its information. DWT is compressed with lossless quality. how discrete-time signals are converted to distinct wavelength representations.

There are various filters that can be used in DWT to process the signal; the most commonly used and simplest filter is Haar. The 2D image is divided into four parts in order to apply DWT.

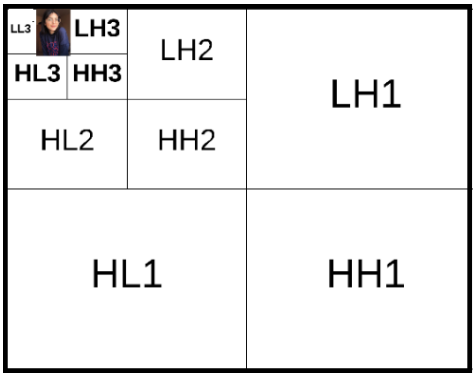

Figure 3.Dwt Subbands

II.PROPOSED ALGORITHMS

In this instance, the suggested technique combines RSA with Huffman coding, or DWT, in an effort to minimise the bit of information in steganography. As seen in figures 4 and 5, there are two main processes at play: embedding the information process and receivingor extracting the message process.

A. Embedding Algorithm

In this process, the secret message is encrypted using RSA encryption and then compress using Huffman coding. The cover image is compressed using DWT. The compressed encrypted message is embedded into the cover image using LSB. Now, the output is a compressed stego-image.

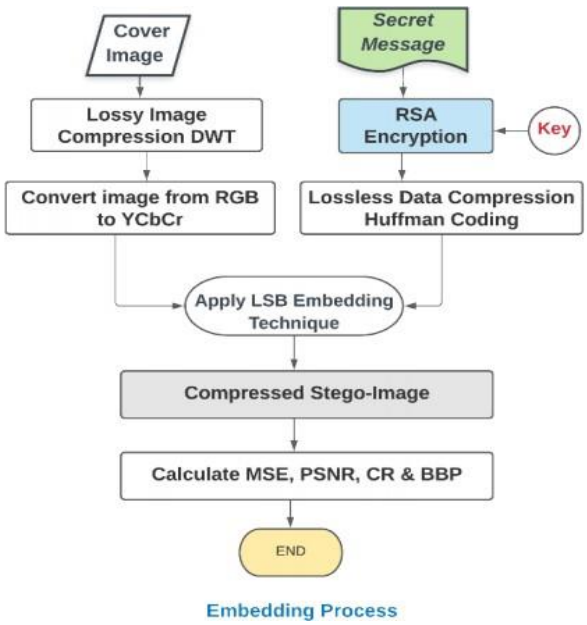

Figure 4. Process of embedding the secret message

B. Extracting Algorithm

In this process, firstly, read the compressed stego- image. Decompress the already compressed stego-image using DWT and Huffman coding inorder to produce an uncompressed stego-image. Extracting themessage using LSB from each pixel will help in retrieving stego-image binaries. Finally, decrypt the RSA-encrypted message using a key and output the secret message.

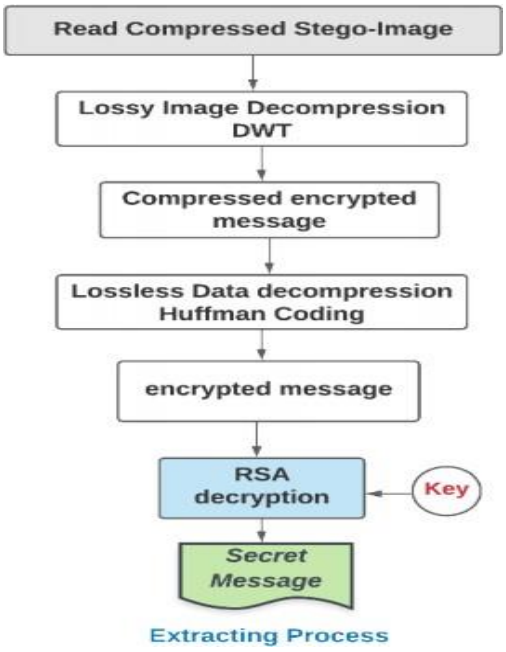

Figure 5. Process of extracting the secret message

III.CONCLUSION

When sending photos over a network, image compression is a helpful technique that helps save timeand memory. Both storage capacity and transfer speed are aided by this. This work presents a well-consideredstrategy for protecting, compressing, and even maskingmessages in the cover image using a combination of DWT, RSA, and Huffman coding. The goal is to createa compact, high-quality image.

Combining RSA, Huffman Coding, and DWT to encrypt a message and conceal it within the coverimage resulted in a small file size and high-quality image. By lowering the total message bits by up to 25% of the initial message bits, you can increase capacity.

REFERENCES

1. *A. Sari, G. Ardiansyah, and E. H. Rachmawanto, ''An improved security and message capacity using AES and Huffman coding on image steganography,'' Telkomnika, vol. 17, no. 5, pp. 2400–2409, 2019.*
2. *O. F. AbdelWahab, A. I. Hussein, H. F. A. Hamed, and H. M. Kelash, ''Hiding data in images using steganography techniques with compression algorithms,'' Telkomnika, vol. 17, no. 3, pp. 1168– 1175, 2019.*
3. *N. Sharma and U. Batra, ''Performance analysis ofcompression algorithms for information security: A review,'' ICST Trans. Scalable Inf. Syst., vol. 7, no. 27,Jul. 2018, Art. no. 163503.*
4. *R. L. Rivest, A. Shamir, and L. Adleman, ''A method for obtaining digital signatures and public-keycryptosystems,'' Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978.*
5. *R. M. Thanki and A. Kothari, ''Data compression and its application in medical imaging,'' in Hybrid and Advanced Compression Techniques for Medical Images. Cham, Switzerland: Springer, 2019, pp. 1–15.*
6. *Jeromel and B. Žalik, ''An efficient lossy cartoon image compression method,'' Multimedia Tools Appl., vol. 79, nos. 1–2, pp. 433–451, Jan. 2020.*
7. *F. Adhanadi, L. Novamizanti, and G. Budiman, ''DWT-SMM-based audio steganography with RSA encryption and compressive sampling,'' Telkomnika, vol. 18, no. 2, pp. 1095–1104, 2020.*
8. *R. Praisline Jasmi, B. Perumal, and M. Pallikonda Rajasekaran, ''Comparison of image compression techniques using Huffman coding, DWT and fractal algorithm,'' in Proc. Int. Conf. Comput. Commun. Informat. (ICCCI), Jan. 2015, pp. 1–5.*
9. *Setyaningsih, R. Wardoyo, and A. K. Sari, ''Securing color image transmission using compression-encryption model with dynamic key generator and efficient symmetric key distribution,'' Digit. Commun. Netw., vol. 6, no. 4, pp. 486–503, Nov.2020.*
10. *M. Y. Valandar, P. Ayubi, and M. J. Barani, ''A new transform domain steganography based on modified logistic chaotic map for color images,''J. Inf. Secur. Appl., vol. 34, pp. 142–151, Jun. 2017.*