International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Image Encryption Using Different Algorithms

Garugu Alekhya*

GMR Institute of Technology Razam, Neyyala Street, Bobbili, Andhra Pradesh, Pin -535558 India.

ABSTRACT

This article shows about the varied image encryption techniques. Now a days, where all cognizant about the net and other means of sharing of multimedia information between two parties which happens publically environment, so it's important to take care of the protection of those reasonably personal data which is stored at computers, on cloud or within the personal storage. To create the data secure it need to convert the data from one form to another form is said to be encryption. Simple encryption algorithms aren't suitable for digital image encryption. To overcome these drawbacks there several algorithms come into existence. Encryption method include plain text, cipher text and keys. So as to secure data during communication, data storage and transmission several algorithms are widely used. RSA could be a asymmetric cryptographic algorithm. The algorithms use to secure data form unauthorized user. The algorithm is employed for text data yet as for image data. During this a picture is given as input to the algorithm which converts it into encrypted image and vice versa done in the decryption process. This study presents about cryptography and explains about different algorithms.

Keywords: Rivest Shamir Adlemam (RSA), Pixel mixing, S-box, Zaslavsky map, 3D chaotic map , two dimensional lorenz , jigsaw puzzle, cryptography ,Steganography encryption , decryption.

1. Introduction

Image encryption is that the cryptographic process that contains the transformation of plain text information, using cipher algorithm to make it unreadable to anyone except the those who are having the special knowledge about the encryption usually called the key. Rivest Shamir Adleman (RSA) algorithm is an asymmetric cryptographic technique that contains 2 keys.one of the secret's public key and therefore the other one is private key. during this both sender and receiver contain public and personal keys. Image information comprises privacy and security, which indicates the importance of securing the web transmission of digital image. Image information comprises privacy and security, which indicates the importance of securing the web transmission of digital images. Thus, such images require encryption before they're sent. Many image encryption techniques are in use and providing different levels of security. The protection of digital content is increasingly becoming a big issue for researchers and engineers as voluminous digital images are transmitted every second to all or any corners of the planet.

2. Literature Review

- [1]. The main theme of this article is to reduce the physical space on the various storage media and reduce the time of sending data over the Internet and hiding data from intruders. In this the plain text is compressed by Huffman coding, the cover image is compressed by DWT based that compacts through the lossy compression in order to reduce the cover image dimensions.
- [2]. The proposed scheme demonstrates the most efficiency in terms of lowering the computational cost and shows its effectiveness against a wide range of cryptographic attacks. This paper proposes a method for scrambling color image data at two levels. The first aims to modify the positions of bits within the pixel data, and the second involves changing the positions of pixels in the original image based on the S-box.
- [3]. Images encrypted by using the proposed scheme include less color information due to the use of grayscale images, which makes the EtC system stronger. Showed that it enhances security against ciphertext-only attacks which it's effective for EtC systems in terms of image quality. The main aims to protect visual information of data that enables us to identify an individual, a time and also the location for taking a photograph.
- [4]. In this paper, an image encryption algorithm is used. The classical chaotic model is used in the encryption algorithm to generate two sets of chaotic sequences to encrypt the image. The two-dimensional Lorenz chaotic model is used to generate chaotic sequences to encrypt and encrypt the image.
- [5]. This research presents a 3D chaotic mapbased symmetric algorithm for multiple images to improve encryption efficiency and encourage secure transmission. The protection of digital content is increasingly becoming a significant issue for researchers and engineers as millions of digital images are transmitted every second to all corners of the world.

3. Methodologies

3.1 Hiding Data using Efficient Combination of RSA Cryptography, and compression Steganography techniques

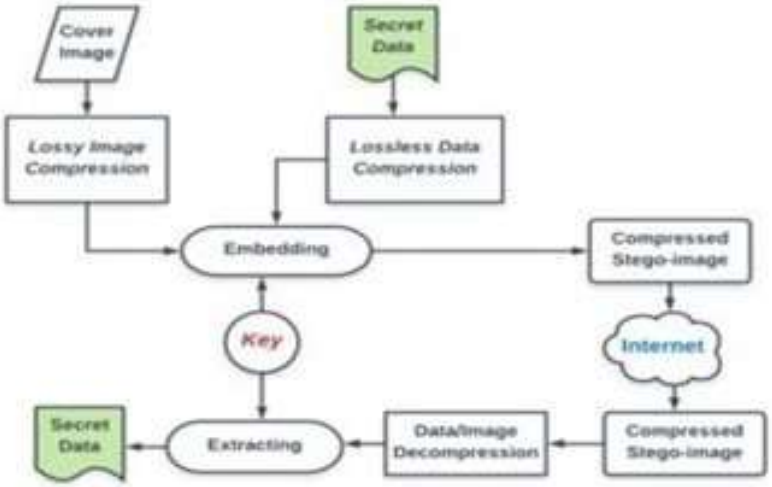


Fig: Image encryption with RSA

3.2 Provably Secure and Fast Color Image Encryption Algorithm Based on S-Boxes and Hyperchaotic Map. Firstly, associate S-box is created based on

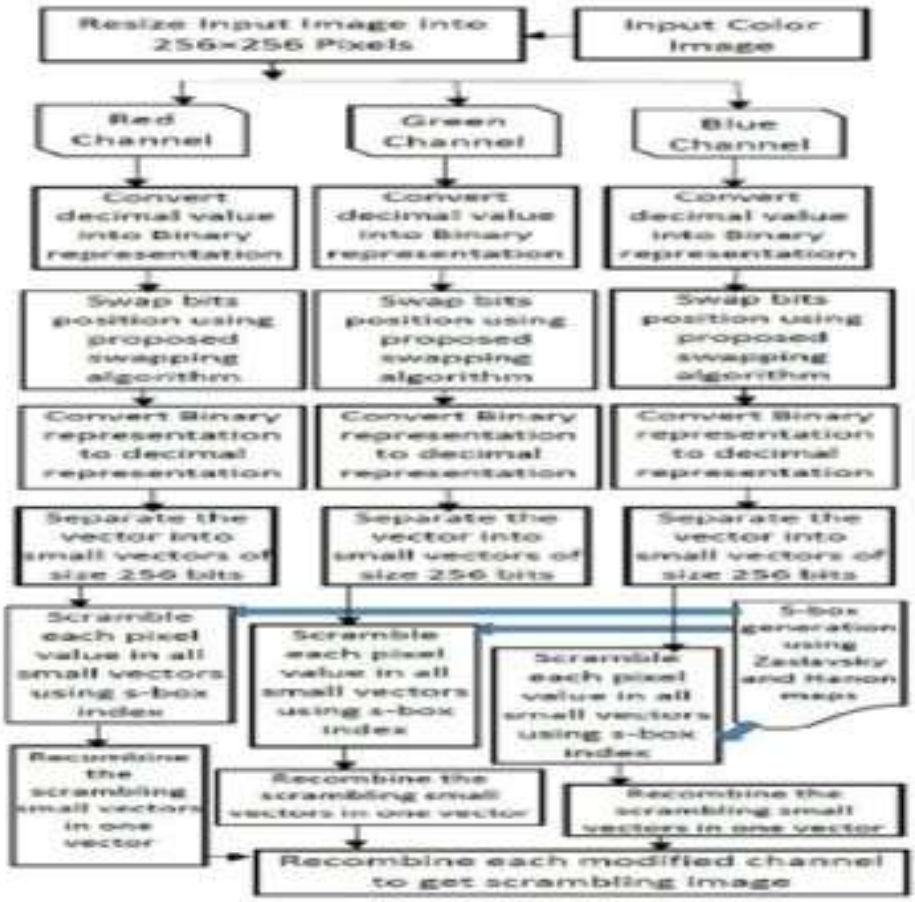


Fig: Block diagram of image compression

The Zaslavsky and Henon maps. Secondly, a hyperchaotic key sequence is created by combining the Henon map equation with obtained values by the Logistical map equation. The symmetric secret key production contained a hybrid type supported the 3D Henon map and therefore the Logistic map parameters. The sequence of the HyperLogVarHenon map was saved as a matrix. The matrix has divided into three same matrices. Finally, XOR operation generates a cipher image that acts as a lightweight operation between the scrambling image channels and therefore the arbitrarily created

HyperLogVarHenon matrices. Finally, perform XOR operation between the scrambling image and also the created HyperLogVarHenon matrices acquire a cipher image.

3.3 Encryption-then-Compression technique

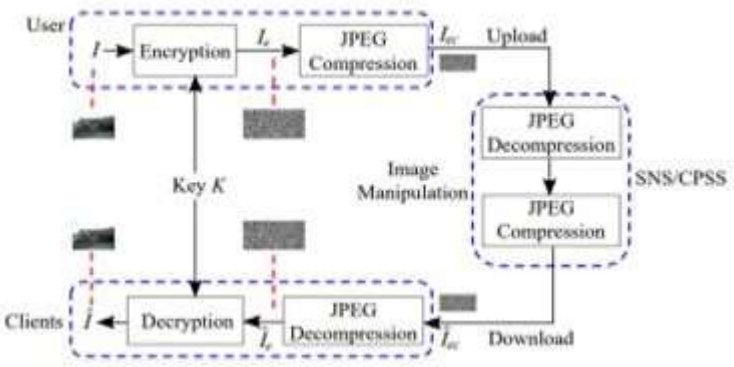


Fig: Encryption-then-Compression with JPEG image

The conventional encryption used in EtC systems has a limitation on block size, i.e. Bx = By = 16, to avoid the effect of color sub-sampling. If Bx = By = 8 is chosen as a block size, the compression performance decreases and some block distortion is generated in decompressed images.

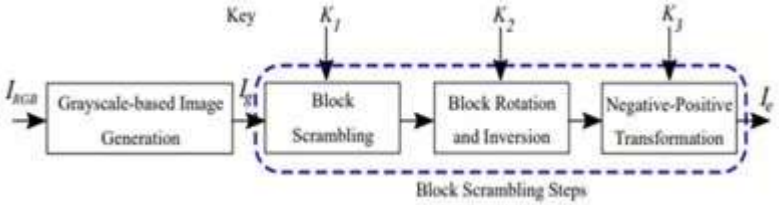


Fig: Conventional grey scale-based block scrambling image encryption

Although Bx = By = sixteen is used as the smallest block size in the conventional block scrambling-based image encryption to avoid the impact of color sub-sampling in JPEG compression, the suggested methodology allows us to use Bx = By = eight as a block size, which enhances strength against ciphertext-only attacks. Moreover, applying EtC systems with the suggested scheme to social media performs better than with the standard one.

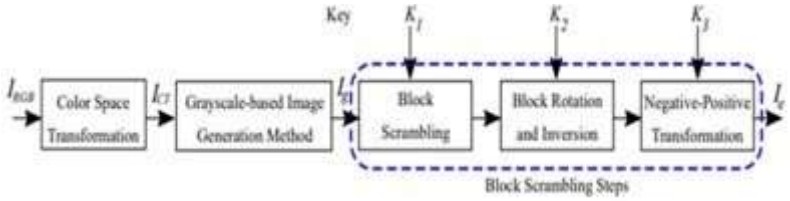


Fig: proposed gey scale-based scrambling image

4. RESULTS AND DISCUSSIONS

4.1 Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques:

Image compression is a useful technology that helps save memory space and time while transferring images over a network. This helps to increase storage capacity as well as transfer speed. In this paper, a combination of RSA, Huffman coding, and DWT has been carefully proposed as a method of securing and compressing messages, and even masking messages in the cover image, with the aim of producing a high-quality image with a small size. In our paper, the author evaluated and discussed the RSA algorithm for encrypting and decoding the secret file with two different algorithms that can be used for image compression. Author also reviewed and discussed the two algorithms that can be used to compress images for both lossy and lossless techniques. In this paper, the distinct types of image compression techniques are evaluated on the basis of certain criteria such as compression ratio, compression time, compression speed, Saving Percentage, Structural Similarity Index, and saving ratio.

Table1: Huffman coding algorithm results

Cover images	Message size	Huffman coding (Lossless)							
		SSIM	CR	CT	CS	SP%	BPP	MSE	PSNR
Man	38278	0.8832	35.76	0.277	113452	17.9	1.51	1.3	38.91
Boy	25000	0.7832	34.73	0.287	71864	17.5	1.67	1.37	38.88
Girl	30178	0.7965	35.12	0.185	135067	17.2	1.75	1.39	39.68
Apple	33145	0.8743	34.52	0.197	140824	16.3	1.73	1.4	34.52
Bear	43123	0.8503	34.95	0.201	179786	16.2	1.66	1.42	34.93
Lena	22652	0.8827	35.01	0.266	69574	18.3	1.15	1.27	36.13
Average	32063	**0.8450**	**35.02**	**0.236**	**118428**	**17.2**	**1.58**	**1.36**	**37.18**

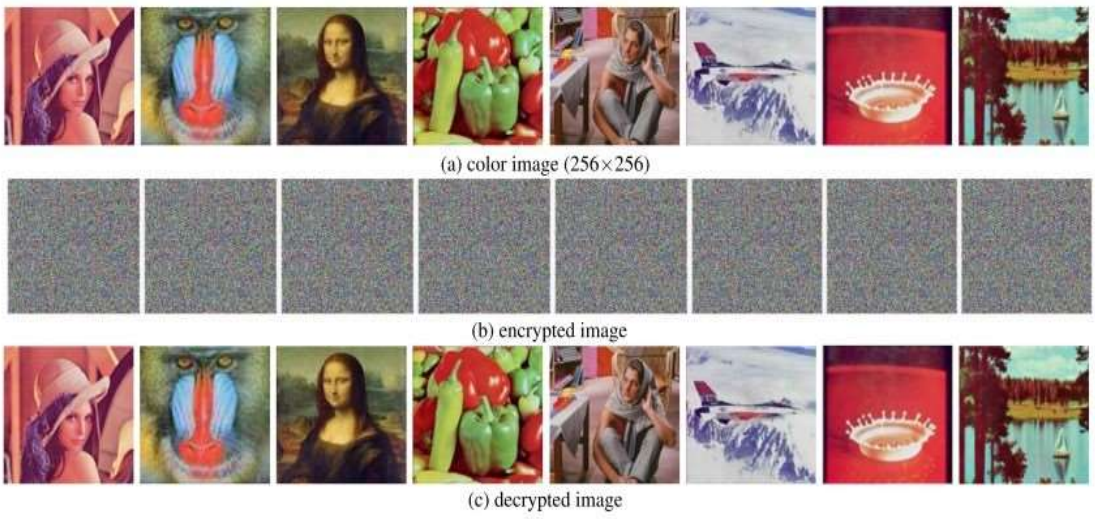
Table 2: DWT algorithm results

Cover images	Message size	DWT (Lossy)							
		SSIM	CR	CT	CS	SP%	BPP	MSE	PSNR
Man	38278	0.9288	28.17	0.008	3933065	17.8	0.98	0.25	40.51
Boy	25000	0.9295	28.66	0.018	1127778	18.8	0.89	0.08	41.33
Girl	30178	0.9277	29.45	0.009	2729432	18.6	0.88	0.23	42.35
Apple	33145	0.9243	29.94	0.021	1295812	17.9	0.95	0.05	46.7
Bear	43123	0.9311	31.29	0.011	3155820	19.5	0.86	0.19	45.87
Lena	22652	0.9151	30.69	0.015	1218678	19.3	0.97	0.13	43.91
Average	32063	**0.9261**	**29.70**	**0.0137**	**2243431**	**18.7**	**0.92**	**0.16**	**43.45**

Provably Secure and Fast Color Image Encryption Algorithm Based on S-Boxes and Hyperchaotic Map:

This part used eight 256 × 256×3 standard color pictures as input digital images to confirm the potential of the image encryption method. Thus, the suggested algorithm has enough key space to resist brute-force attacks. Our suggested method achieves much lower encryption and decryption time.The keys generated in the suggested scheme will add a lot of randomness to their dependence on the hyperchaotic map throughout the generation. The proposed algorithm demonstrates its tough ability to protect the differential attack. The openness and vulnerability of the transmission to attacks show the importance of applying security to the transmitted image.

4.1 Using



(a) color image (256×256)

(b) encrypted image

(c) decrypted image

Encryption-then-Compression technique:

The proposed encryption scheme aims to protect visual information of images to allow us to identify an individual a time and the location for taking a photograph. Encryption image mainly depends on the block size. In addition, most conventional jigsaw puzzle solvers also use color information to assemble puzzles. It contains a higher security level than that of the conventional scheme, because it provides big blocks and a small block size.

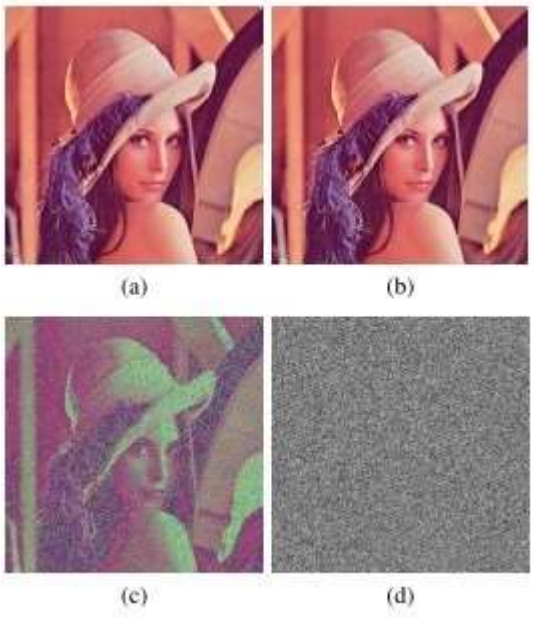


Fig: (a) Original image (b) proposed scheme (c) Encryption scheme (d) Encrypted image

5. Conclusion

I studied the efficient algorithms that have been proposed for secure sharing of images. This paper proposed a hybrid data compression algorithm increases the input data to be encrypted by RSA cryptography method to evaluate the security level and it can be used in executing lossy and lossless compacting Steganography methods. The results proved that considering method shows the high-level performance. The proposed mechanism has the more effective visual quality and storage capacity and it as high security and acceptable durability against attacks. In future we will consider many predictions by using Huffman coding for reversible data hiding in the images.

REFERENCES

1. O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein and H. F. A. Hamed, "Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques," in IEEE Access, vol. 9
2. Z. A. Abduljabbar et al., "Provably Secure and Fast Color Image Encryption Algorithm Based on S-Boxes," in IEEE Access, vol. 10.
3. T. Chuman, W. Sirichotedumrong and H. Kiya, "Encryption-Then-Compression Systems Using Grayscale-Based Image Encryption for JPEG Images," in IEEE Transactions on Information Forensics and Security, vol. 14.
4. T. Li, B. Du and X. Liang, "Image Encryption Algorithm Based on Logistic and Two-Dimensional Lorenz," in IEEE Access, vol. 8, pp. 13792-13805, 2020, doi: 10.1109/ACCESS.2020.2966264.
5. .M. Tanveer et al., "Multi-Images Encryption Scheme Based on 3D Chaotic Map and Substitution Box," in IEEE Access, vol. 9, pp. 73924-73937, 2021, doi: 10.1109/ACCESS.2021.3081362.
6. C. 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.
7. A. K. Pal, K. Naik, and R. Agrawal, ‘‘A steganography scheme on JPEG compressed cover image with high embedding capacity,’’ Int. Arab J. Inf. Technol., vol. 16, no. 1, pp. 116–124, 2019.
8. A. A. Karawia and Y. A. Elmasry, ‘‘New encryption algorithm using bitlevel permutation and non-invertible chaotic map,’’ IEEE Access, vol. 9, pp. 101357–101368, 2021.
9. J. Sun, ‘‘2D-SCMCI hyperchaotic map for image encryption algorithm,’’ IEEE Access, vol. 9, pp. 59313–59327, 2021.
10. R. M. Lin and T. Y. Ng, ‘‘Secure image encryption based on an ideal new nonlinear discrete dynamical system,’’ Math. Problems Eng., vol. 2018, pp. 1–12, May 2018
11. S. Ibrahim and A. Alharbi, ‘‘Efficient image encryption scheme using Henon map, dynamic S-boxes and elliptic curve cryptography,’’ IEEE Access, vol. 8, pp. 194289–194302, 2020

12. X. Zhang and X. Wang, ‘‘Multiple-image encryption algorithm based on mixed image element and chaos,’’ Comput. Electr. Eng., vol. 62, pp. 401–413, Aug. 2017, doi: 10.1016

13. W. Lv, R. Bai, and X. Sun, ‘‘Image encryption algorithm based on hyperchaotic lorenz map and compressed sensing theory,’’ in Proc. Chin. Control Conf. (CCC), Jul. 2019

14. J. Zhang, D. Fang, and H. Ren, ‘‘Image encryption algorithm based on DNA encoding and chaotic maps,’’ Math. Problems Eng., vol. 2014, Dec. 2014

15. X. Zhang, “Lossy compression and iterative reconstruction for encrypted image,” IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 53–58, Mar. 2011.