Image Encryption Using Different Algorithms

Garugu Alekhyaa*

GMR Institute of Technology Razam, Neyyula 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 Adleman (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 EnC system stronger. Showed that it enhances security against ciphertext-only attacks which it’s effective for EnC 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 decrypt the image.

- [5]. This research presents a 3D chaotic map based 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

![Image encryption with RSA](image1)

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

![Block diagram of image compression](image2)

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

![Encryption-then-Compression with JPEG image](image1)

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.

![Conventional grey scale-based block scrambling image encryption](image2)

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.

![proposed grey scale-based scrambling image](image3)

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.
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 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.
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


