

# A Review: On Design & Image Encryption Algorithm by using DCT Method

Keerti Tripathi<sup>1</sup> Anil Khandelwal<sup>2</sup>

<sup>1,2</sup>VNS Group of Institution, Bhopal, India

**Abstract**— In this paper propose an image encryption technique which employs the concept of carrier image and SCAN patterns generated by SCAN methodology. Although it involves existing method like SCAN methodology, the novelty of the work lies in hybridizing and carrier image creation for encryption. Image encryption plays a paramount part to guarantee classified transmission and capacity of image over web. Then again, a real-time image encryption confronts a more noteworthy test because of vast measure of information included. This paper exhibits an audit on image encryption in spatial, frequency and hybrid domains with both full encryption and selective encryption strategy. The resulting image is found to be more distorted in hybrid technique. By applying the reverse process we get the decrypted image.

**Key words:** Scanning Techniques, Image Encryption, Scan Pattern

## I. INTRODUCTION

Image encryption technology has been widely investigated over the past two decades or so to meet the increasing demand for real-time secure image transmissions over public networks. Existing studies have shown that though modern block ciphers such as DES and AES can be applied to any kind of data, they are not suitable for practical image encryption. This is because the security of these algorithms is mainly ensured by their high computational cost, and they are difficult to meet the demand for online communications when dealing with digital images characterized by bulk data capacity. With the regularly expanding development of applications of sight as well as sound, security is one of the critical issues in correspondence and capacity of Images, and encryption is one of the approaches to guarantee security. Image encryption systems attempt to change over unique image to another image that is difficult to comprehend; to keep the image private between clients, in other words, it is fundamental that no one could be acquainted with the substance without a key for decryption [1]. The encryption of image is to transmit the image safely over the system so that no unapproved client can ready to unscramble the image. Image encryption, video encryption, chaos based encryption have applications in many areas including the web correspondence, transmission, restorative imaging, Tele-solution and military communication, and so on [2]. Encryption is advancing and moving towards a fate of unlimited conceivable outcomes. The image information has exceptional properties, for example, mass capacity, high excess and high correlation among the pixels. Encryption methods are exceptionally valuable devices to secure secret data. Encryption will be characterized as the transformation of plain message into another form which is called as cipher text that can't be perused by any individuals without decoding the scrambled content. Decryption is the reverse procedure of encryption which is the way towards changing over the encrypted content into its unique plain content [3].

Cryptography is the field of mathematics and computer science which provides many security services. These services include the protection by means of an appropriate encryption plan, of private data from being gotten to by an unapproved party. Various traditional encryption plans have showed up in the writing, like, the Data Encryption Standard (DES), the International Data Encryption Algorithm (IDEA), the Advanced Encryption Standard (AES), and so on, these plans require a substantial computational time, and are for the most part used to ensure literary information

## II. RELATED WORK

1) Edi Jaya Kusuma et.al.

An Imperceptible LSB Image Hiding on Edge Region Using DES Encryption Sending image in a plain form has a high risk for the data being vulnerable to steal. Thus, due to reducing the risk, data security techniques should be implemented. Data security techniques can be done using Cryptography and Steganography. Based on the literature, the combination of cryptography and steganography can enhance results. Cryptography as one of science in information security, which used in the process of securing image. One of the cryptographic methods that have been used to secure the data is Data Encryption Standard (DES). This algorithm often implemented for the encryption process in an ATM machine and SIM card operator worldwide. Our proposed method firstly encrypts the image message using DES encryption. This process produces visible data, which is caused suspicion by others. In this paper, to conceal the encrypted image, we used steganography method. Our experiment chooses Least Significant Bit (LSB) based on canny edge detection. LSB algorithm was chosen because it is simple to be implemented and has good imperceptible value. Then, canny edge detection used to determines the coordinates of the object's edges of the cover image. We utilize the Canny coordinate result as the position to embed the image message because of the results more accurate and it can improve imperceptibility. Our experimental results were measured using Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). From the measurement, results obtained the best MSE value is 0.0038557 and PSNR are 72.2698 dB.

2) Zheng Zou et.al.

A Novel Image Encryption Method based on Modular Matrix Transformation and Coordinate Sampling- Information security is very important in modern society. Image encryption is a branch of information security. It can be not only used to protect the copyrights of the ownership of the images from the internet, but also to be used to image information hiding as a key pre-processing in order to increase the security. A novel image encryption method based on modular matrix transformation and coordinate sampling is presented in this paper. The algorithm has an advantage that images can be encrypted by their grey information and their coordinate information in the same time. As an application, the algorithm is used to image information hiding based on

LSB. Experiments show that the method reaches a very good image encryption effect, and also can endure some image attacks.

3) Chandra Prakash Singar et.al.

Image Encryption based on Cell Shuffling and Scanning Techniques Information containing sound, video and images exchanges over the web is open and not secure. Security is required for storing and transmission of digital images to avoid from unauthorized entities. This paper presents the novel approach using cell shuffling and scanning techniques for image encryption. The proposed method contain two stage, first divide the image in to number of blocks and then shuffled the original image and in second stage the spiral wave scan pattern are applied to get encrypted image. A number of parameters, like correlation coefficient, information entropy, PSNR, MSE, number of pixels change rate, average intensity and unified average change intensity etc. , are used to check the quality of cipher image.

4) Chong Fu et.al.

A Novel Parallel Image Encryption Scheme Using Chaos In recent years, chaos-based image cipher has been widely studied and a growing number of schemes based on permutation-substitution architecture have been proposed. To better meet the challenge of real-time secure image communication applications, this paper suggests a new image encryption scheme using a parallel substitution. In the permutation stage, the Arnold cat map is employed to shuffle the pixel positions so as to erase the strong relationship between adjacent pixels. In the substitution stage, the scrambled image is firstly decomposed into eight bit-planes which are then parallely mixed with key streams generated by the chaotic logistic map. Theoretically, the parallel substitution strategy runs eight times faster than the serial strategy on an 8- thread processor as the volume of data processed by each substitution unit is 1/8 of that of the input image. Experimental results show that the proposed parallel scheme runs more than five times faster than the serial scheme. Extensive security analysis is carried out with detailed analysis, demonstrating the satisfactory security of the proposed scheme.

5) Mohammed Es-sabry et.al.

Grayscale image encryption using shift bits operations- In this work, we propose a method of cryptography of grayscale images. The principle of this approach is to encrypt any image (called the original image), into a sequence of N images whose (N-1) are generated randomly and the N<sup>th</sup> image is determined from the original image and the (N-1) generated images. A key will be used in order to increase the security of the image transmitted to the receiver. The pixels of the original image are first converted into bits and then we use the shift bits operators to obtain a matrix, which will be used in the encryption procedure. All N images as well as the key used are needed in the decryption process, to obtain the source image. Experiments show the importance and quality of the approach that we proposed in terms of accuracy.

#### A. Image Encryption

Image encryption method prepares information as unreadable. Images are widely used in many different applications. Therefore, security of image data acquired from unauthorized users is important [4].the encryption of original

image is convert encrypted one. In recent years, approaches of color image encryption are widely used. Up to this point, different in-formation encryption algorithms were proposed and broadly utilized, for example, AES, RSA, or IDEA the greater part of which are utilized as part of content or binary data [5]. It is hard to utilize them straightforwardly in mixed media information and wasteful for shading picture encryption due to high relationship among pixels [1]

### III. PROPOSED APPROACH

In this section, we will describe our proposed method. Firstly, the secret image will be encrypted using DES algorithm. Then, based on edges area of the cover image, which is generated by canny edge detection, then, inserted the encryption result into it. For more detail, the author separated the process into two main parts.

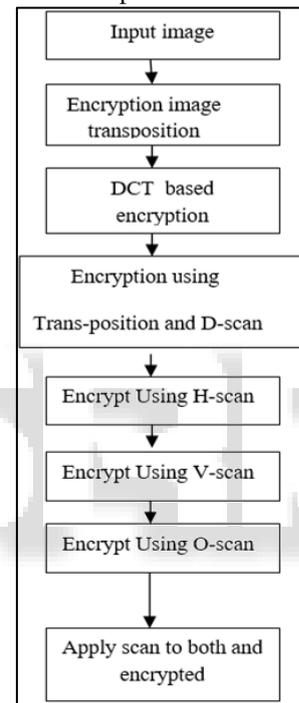


Fig. 1: Flow Chart of Proposed Method

#### A. Encryption Method

Have two possibility of converted cipher or encrypted image that is either stream based or block based encryption. Fig. 2 shows that the alternate way of encryption method to obtain encrypted image. The transformation procedure will be utilized to separate the original image into various blocks that are then rearranged their positions inside the image

#### B. Scanning Techniques

As image are two dimensional array of pixel values, exploring it in different ways produces a different sequence of pixel? Scan is a formal language- based two-dimensional spatial-accessing methodology which can represent and produce countless assortments of examining ways effectively. Exploring the image in a different way can generate different sequence. This exploring is called as Scan. Scan is a fractal based image processing language; it is a context-free language Most image encryption and image compression method uses this language [1].

#### IV. CONCLUSION

This paper provides several encryption results of grayscale, medical and colour images in order to show the performance of the presented algorithm for image encryption. The new algorithm is based on the discrete parametric cosine transform. The encryption process is a straightforward data transformation from the spatial domain to the frequency domain and then back into the spatial domain. Experimental results will be demonstrated that the presented algorithm can fully or partially protect the 2D and 3D images.

#### REFERENCES

- [1] Edi Jaya Kusuma Et.al An Imperceptible LSB Image Hiding on Edge Region Using DES Encryption 2017 International Conference on Innovative and Creative Information Technology(ICITech),1763419010.1109/INNOVATIVE AND CREATIVE INFORMATION TECHNOLOGY (ICITECH).2017.8319132 Salatiga, Indonesia
- [2] Zheng Zou Et.al.A Novel Image Encryption Method based on Modular Matrix Transformation and Coordinate Sampling ,Proceedings of IEEE International Conference on Applied System Innovation 2018 IEEE ICASI 2018- Meen, Prior & Lam (Eds)
- [3] Chandra Prakash Singar et.al.Image Encryption based on Cell Shuffling and Scanning Techniques Proceeding International conference on Recent Innovations in Signal Processing and Embedded Systems (RISE-2017) 27-29 October,2017 ISBN 978-1-5090-4760-4/17/\$31.00©2017 IEEE
- [4] Chong Fu et.al.A Novel Parallel Image Encryption Scheme Using Chaos 2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on Ubiquitous Computing and Communications (ISPA/IUCC) 0-7695-6329-5/17/31.00 ©2017 IEEE DOI 10.1109/ISPA/IUCC.2017.00180
- [5] Mohammed Es-sabrya et.al. Grayscale image encryption using shift bits operations 978-1-5386-4396-9/18/\$31.00 ©2018 IEEE