Implementation Image Encryption Algorithm by using DCT Method

Keerti Tripathi[1] Anil Khandelwal[2]
[1]M.Tech Scholar
[1,2]VNS Group of Institution Bhopal, India

Abstract— This paper generally design for encrypted image scan pattern. The images captured with a camera is saved or otherwise sent over the internet without encryption. If the camera is stolen, then all the images stored inside it will be stolen by others. For real time applications to impose sanctuary, image is to be captured, compressed and encrypted in the camera itself. To tenacity this issue, scan pattern based image encryption is proposed while capturing the image. Experiments are made in MATLAB and resul6 carried out in term of PSNR analysed with various measures to prove the efficacy of the proposed algorithm.

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. The positions of the pixels in the original image are firstly scrambled in a pseudorandom manner with the purpose of erasing the strong relationship between adjacent pixels. Then the pixels values are sequentially mixed with a chaotic key stream sequence so as to confuse the relationship between cipher-image and plain-image. The whole permutation-substitution operation is often performed for several rounds according to the security requirement. To better meet the challenge of real-time secure image communication applications, much work has been done in recent years on improving the efficiency of chaos-based image encryption technology. Many of the existing studies have pointed out that the substitution procedure consumes the highest percentage of execution time of a permutation substitution type image cipher.

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]. Fig. 1 shows the encryption of original image is convert encrypted one. In recent years, approaches of colour 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]

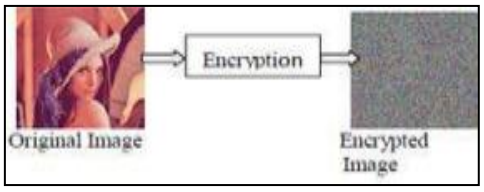

Fig. 2: Encryption Methods

Encryption methods 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.

A-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 [6].

B. Discrete Cosine Transform (DCT)

Is used in image and video coding since early 1970s. The block 8x8 pixels in two-dimensional DCT are used in forward DCT for 64 pixel values and get 64 DCT coefficients. The coefficient in the top left corner is called DC component of the DCT coefficient matrix and the Other DCT coefficients are called AC components. The DCT transformation can be achieved by using 8x8 pixels block to sum of cosine signals weighted. These weights are represented by the matrix DCT coefficient [4]. The coefficients, which represent to the low spatial domain frequencies, are near to the top left corner and the coefficients, which represent to the high spatial domain frequencies, are near to the bottom right corner. The low frequencies are gradual changes and slow representation, and the high frequencies are sharp changes and fast representation in the pixel domain. There is a spatial domain redundancy and the low frequency dominates the high frequency. The energy or information can be concentrated in the forward DCT contained in 8*8 block coefficient matrix in the top left side. The coefficients in the matrix near the DC coefficient differ a lot from zero and the other high coefficients are very close to zero.

II. IDEA BEHIND THE PROPOSED WORK

As we discussed in the introduction, there are several method for image encryption which deals in their own ideas.

III. PROPOSED APPROACH

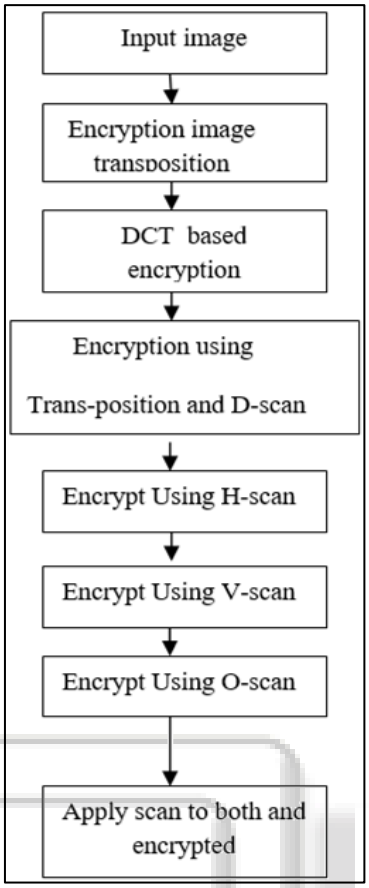

Fig. 1: Flow Chart of Proposed Method

In few image encryption algorithms, encryption process depend only on the keywords, but in some other algorithms they use only carrier image for encryption. Anyhow, we have an idea to hybrid the existing algorithms to get a new path for encryption by taking the advantages of individual methods. Hence we come up with the concept of hybridizing SCAN pattern and Carrier image for Image encryption to get highly distorted Images. 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.

IV. RESULTS & DISCUSSION

Here we have taken "image." as a reference image to apply deferent encryption algorithm. Figure 3 show GUI Window of Scan Pattern Encrypted Image and 4 shows the different encrypted image when only SCAN encryption process is done for different keys. Figure 5 shows the encrypted H-SCAN images if original image is added with the carrier images for different keywords i.e. key1 in the block diagram. Figure 6 shows encrypted images using SCAN Carrier encryption process at the input of original image and addition of carrier image. Figure 7 shows Fig. 8 show decrypted images. Fig. 9 show scan carrier encrypted imagecarrier decrypted image.

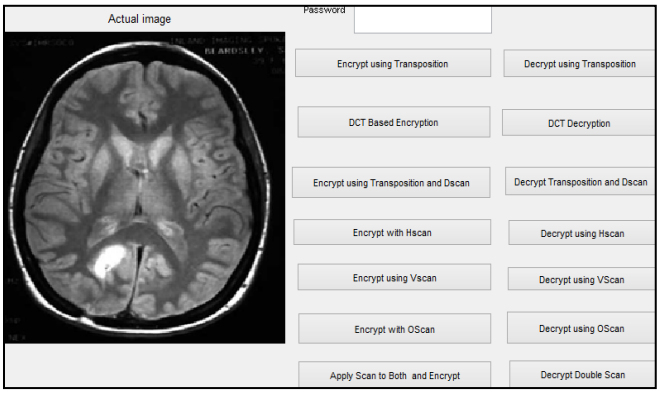

Fig. 3: GUI Window

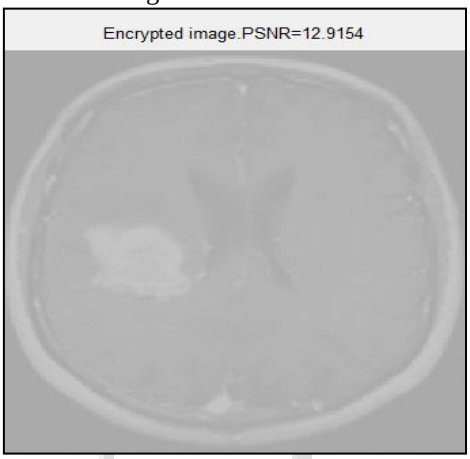

Fig. 3: DCT- Encrypted Image

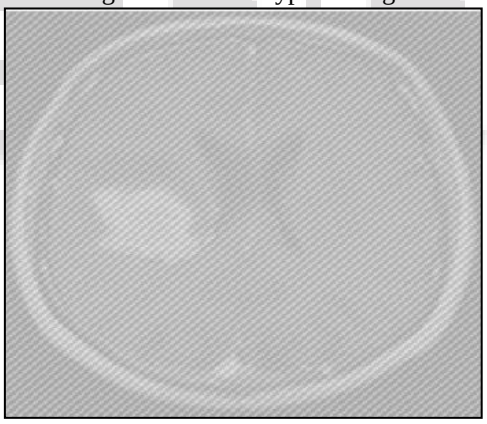

Fig. 4: Carrier Image

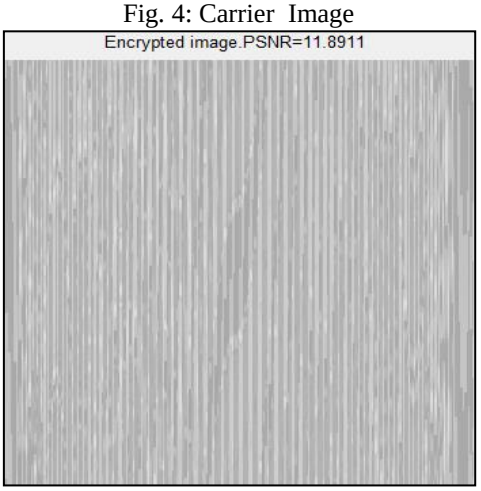

Fig. 5: H-SCAN Encrypted Image

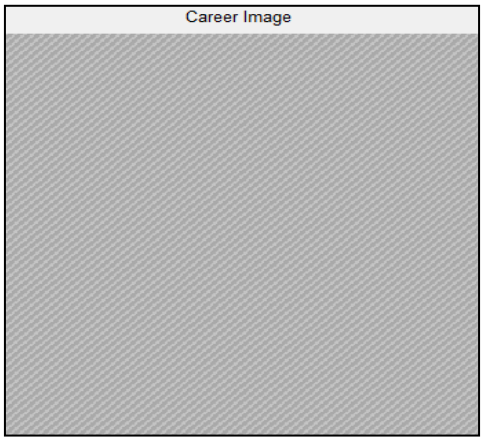

Fig. 6: Carrier Encrypted Image

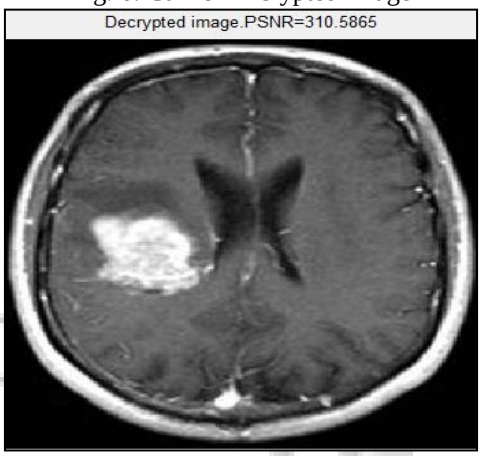

Fig. 7: Decrypted Image

Fig. 8: Scan Carrier Encrypted Image

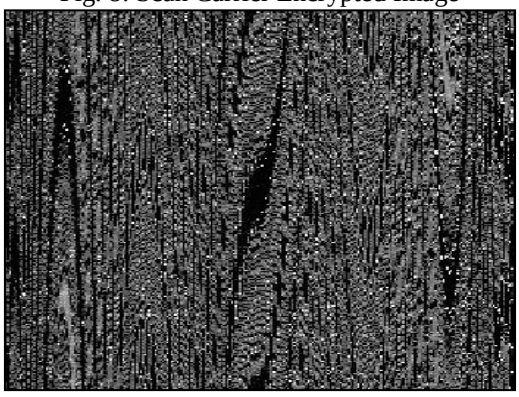

Fig. 9: Carrier Decrypted Image

	Method	Encryption	Decryption
PSNR	Encryption Using Transposition	11.5366	310.5865
	Encryption Using DCT Based	11.5344	294.65
	Encryption Using Transposition And D-Scan	11.5148	310.5865
	Encryption Using H-Scan	11.561	310.5865
	Encryption Using V-Scan	11.5498	310.5865

Table 1: Various PSNR Result

Method	Previous Method Edi Jaya Kusuma[1]	Proposed Method
Encryption Image	72.1777	12.9154

Table 2: Comparison Table

V. CONCLUSION

From the experimental results we conclude that the proposed Scan Pattern Based Image Encrypted approach for image gives very good result as compare to individual encryption process. For the sake of simplicity we used only few SCAN patterns and few carrier-keywords, but proposed algorithm also works for complex SCAN pattern and complex carrier-keywords. In future we want to develop a hybrid algorithm which uses more SCAN patterns, Carrier images along with some bit-manipulation techniques to provide more security to the images. Result shown various in PSNR values

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 (ICI Tech), 1763419010.1109/INNOCIT.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 is 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
[6] S.R.M Prasanna, Y.V. Subba Rao and A. Mitra., "An Image Encryption method with Magnitude and Phase Manipulation using carrier images", IJCS, vol. 1, No 2, pp.132-137, 2006.
[7] Chao Shen Chen and Rong Jian Chen, "Image encryption and decryption using SCAN methodology," Proc. PDCAT, 2006.
[8] S.S. Maniccam and N.G. Bourbakis, "Image and video encryption using SCAN patterns," Pattern Recognition, vol. 37, pp. 725-737, 2004.
[9] Sinha, K. Sing., "A technique for image encryption using digital signeture"., Optics Communication" , 218, pp.229-234, 2003.
[10] Panduranga H.T, Naveen kumar S.K, "A novel 3-step combinational approach for image encryption", IJCEIT, vol 03, 2009 [6] Panduranga H.T, Naveen kumar S.K, "A novel image encryption method using 4outof8 code", proc. CommV'09, pp 460-462, 2009.

