An advanced Double Domain image encryption technique using lossless DCT encryption

[1]Jaspreet Kaur, [2]Hirendra Singh

[1]Masters in Technology (CSE), [2]Assistant Professor
Department of Computer Science & Engineering,
Bells Institute of Management and Technology

Abstract: **With the tremendous rise of information exchange via internet transmission, image security is becoming an important issue that we need to deal with. As, images are being recycled more in business and industrial process, military and medical and also in scientific researches, it is really an important issue to shelter the personal image statistics from unwanted admission or hackers. Because of improvement of technology, the attacking techniques, and hackers are also becoming more and more intelligent. Therefore, traditional techniques of image encryption are not up to the level to compete with the attackers. Image encryption has been a huge area of research study. The protection of image data is very important because it contains actual features and figures of a person or anything. Image encryption is used to secure an image from unauthorized access and increase image security in the internet. Nowadays Internet is used for transferring and loading huge amount of image data. Since the internet has many loopholes and several scopes of hacking or being attacked by unauthorized persons, our personal and confidential image need to be protected during transmission over internet. Researches did satisfactory amount of researches and invented variety of image encryption algorithms. But still there is need of improvement of the image encryption techniques to make it more secure. In this paper, we proposed an advanced double domain encryption technique that encrypts the image two times. First in frequency domain and secondly in spatial domain by using DCT (Discrete Cosine Transform) encryption and compression technique.**

***Keywords*: image, security, encryption, internet.**

I. Introduction

Image is one of the multimedia data that is different from simple text data in many ways. It can be defined as graphical or pictorial representation of any information. Image inordinately assist communication over internet in this phase of multimedia evolution. The growth of hypermedia knowledge in our modern generation has completed digital images to composition an additional significant and unique role than the other data such as traditional texts, number. That's why images request solemn protection of users' discretion for all submissions and during programmer [8]. While transmitting a private or confidential image over an unconfident broadcast channel over internet, it is necessary to ensure the security and privacy and preserve the confidentiality of the image. Encryption is the procedure of encoding messages & material in such a way that only official persons can be able to entree it. An authorized person can read the message with the key provided by the sender. Any unauthorized intruder cannot access the encrypted data because he or she does not have the required key, without which it is not possible to read the confidential information [12].

II. Image Encryption

Image encryption systems stab to translate the original image to supplementary image that is threatening to appreciate; to keep the image friendly among lawful workers, in other term, it is domineering that minion could get to distinguish the pleased underprivileged of a crucial for decryption. Image walloping or encryption means and procedures ranges from simple spatial area methods to more difficult and consistent occurrence sphere. [25]

To preserve secrecy and retaining the discretion of images is a vivacious area of study, with two diverse tactics being trailed, the first being scrambling the images through encryption processes using keys, the other method contains separating the image into haphazard shares to preserve the images confidentiality.

Encryption of images may commonly be considered based on the nature of improved image as any lossy or lossless image encryption. This cataloguing occasioned in the following two diverse lines of tactics being adopted for keeping discretion of images. [29]

Encryption is a system used for security purpose of data. It is a subpart of Cryptography. It can be applied on various form of data like text, image, audio etc. with increase in online applications the popularity of also got increased. A large no. of encryption techniques exists that prevent data from illegal access. Image encryption, video encryption has many application areas like banking, multimedia, military, medical and tele- medicine. Every day a new method is discovered on the basis of encryption.

III. Related Work

In the year of 2017, Yuan proposed a double field image encryption by hyperactive confusion. This paper exposed an image encryption approach during broadcast that works in both occurrence field and latitudinal field by digital hyper mix-up. In the planned encryption organization, the image was encrypted in both occurrence and latitudinal field.

Chengqing Li and Dongdong Lin did cryptanalyzing an image cross-country encryption procedure of pixel whiles in 2017. In this paper, they reevaluated the ISEA (Iterative Seed-Extension Algorithm) algorithm in order to find the real reasons for the attacks. It scrambles the binary representation of the gray level image by using a pseudo-random number sequence which is generated by a digital chaotic map. It uses horizontal and vertical permutation operation in this strategy.

Long Bao, Shuang Yi and Yicong Zhou presented a (k,n)-sharing atmosphere S (k,n) and its group algorithm in their paper titled “Combination of sharing matrix and image encryption for lossless (k; n)-secret image sharing” in 2016. They used mathematical examination in order to show the potential of their approach for secret image sharing. Further, they planned a lossless private image distribution instrument by joining allocation matrix with image encryption.

In 2017, Huiqing Huang and Shouzhi Yang introduced a novel method for encrypting color image using the logistic map and double random-phase encoding. They used a logistic map to diffuse the color image. Then the R, G, B components of the color image were scrambled by replacement of the color matrices using logistic map. They converted the three scrambled image into one encrypted image by utilizing double random phase encoding. Some numerical simulations were performed to examine the proposed encryption algorithm for one image.

In 2016, A multiple-image encryption process that is based on a changed logistic map procedure, compressive ghost imaging, and synchronize sampling is projected. [20] In this method, first the haphazard phase-only disguise was produced with the altered logistic map. By using the 2D discrete cosine transformation, multiple secret images were spared. These images were snarled by diverse random categorizations. Then the snarled images were shared into one image with the use of coordinate sampling matrices. This image was put on the article smooth of the Compressive impression imaging organization.

Hongjun, Abdurahman Kadir and Xiaobo Sun (2017) proposed additional disorder based color image encryption technique. The highpoint of this scheme is to apply arbitrarily tested noise signal for portion as the initial value of the disordered system. They got one time first value from the 256-bit hash value of sound. In this tactic, they only achieved high-class or (XOR) process. This process was applied to verbose the pixels of the image. Some precise actions were taken to speed up the encryption method. To measure the consistency and effectiveness of the approach, they achieved some numerical tests in terms of difficulty and sanctuary.

IV. Problem Formulation

From the above discussion, we can see that there are three major concern we need to focus on and in future our main goal should be to balance these three:

- Computational time: The image size is frequently bigger than text. Therefore, the old-fashioned encryption procedures require a lengthier time to straightly encrypt the picture. Large, complex and very problematic and security inspection turn the encryption system more time devastating. [16]
- Security Level: Conventional of the current image sanctuary systems are not anxious to protect in contradiction of the contemporary breaking doses. Once it comes to the image broadcasts over the internet, image security develops the leading security alarm. But these prevailing image security instruments flop to afford the best image security and occasionally proved to be delicate.
- Transmission Rate: When we try to increase the security of image encryption techniques, the computational complexity makes the image heavier in size and this results larger transmission time. We need an image encryption technique that can transmit in a channel which has low transmission rate.

V. Proposed Solution

5.1 To Increase Security Level

To make a better, effective and non-breakable security mechanism, we can use double domain image encryption method instead of any single sphere encryption. The numerical image can be encrypted in both incidence and spatial extent.

5.2 To decrease the transfer time

To transmit image over internet, the image size should be small enough to be transmitted over a low data rate channel. When the larger images with a greater bit depth are transmitted over the internet, the size of the image has to be reduced by adopting a compression algorithm. [10]

The DCT method is the constant based conversion in which the tinted topographies of the input image are been examined and handled. [5] The DCT is a methodical adjustment that takes an indication and adjusts it from longitudinal field into occurrence field. It adapts an image block into its corresponding frequency constants. The DCT transmute of an image carries out a set of statistics called numbers. [11]

Instead of lossy DCT compression, we will apply advanced lossless DCT image compression technique to preserve the original quality of the image. [11]
Because the images secondhand in such requirements are of highly noteworthy substantial, and losing any amount of substantial is not permitted.

VI. Methodology

As we already stated we are going to use DCT image encryption and density in a double domain stage, we need to select which domain we will select for image encryption. Numerous image encryptions have been probable, mostly by encryption in a single field, either in longitudinal or occurrence field. [20]
The fallouts of [19] display that, the grouping of occurrence and longitudinal arena encryptions significantly augments the refuge close of image encryption.
Therefore we need to see what will ensue inside the incidence domain and spatial domain when we apply DCT operation for image encryption.
The most significant visual physiognomies of the image are located in the low occurrences while the minutiae are positioned in the higher occurrences.

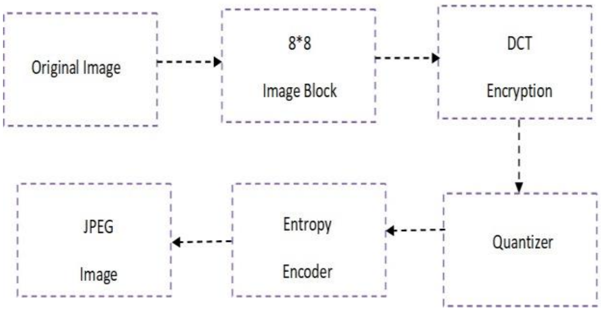


Figure 1: Steps in DCT encryption

- At first we gulf innovative image to be transported into 8*8 small square chunks.
- We apply two-dimensional detached cosine convert to each of the subsequent blocks and we find DCT machineries of each block. The DCT is resolute to each hunk. [44]
- Each hunk is trodden concluded quantization. The quantize achieves the quantization process. We will use lossless compression so that the quality of the image remains unchanged.
- The collection of trodden blocks that generates the image is saved in a meaningfully reduced volume of storing.

In the following figure we created a block diagram to show the operations we perform in both frequency domain and spatial domain. The DCT (Discrete Cosine Transform) operation is performed twice. Once in frequency domain and again in spatial domain.

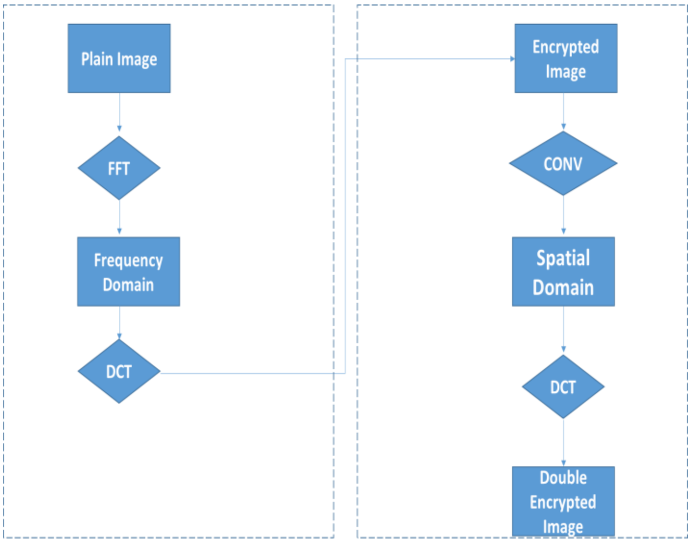
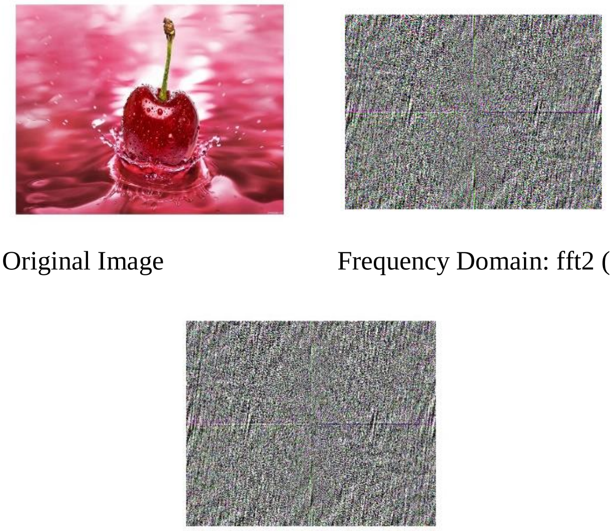


Figure 2: Block Diagram of the operations

VII. Implementation

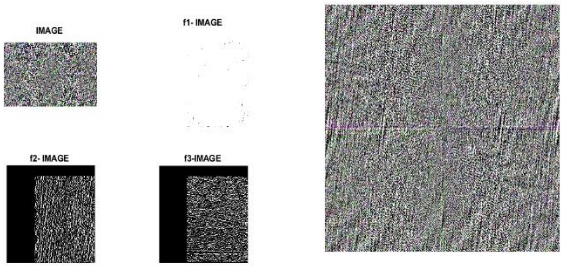
We implemented our proposed scheme in MATLAB 2018a. We had to install the image processing toolbox add on to perform the dct operation. In Matlab the Lossless DCT can be performed by using dctmtx () function. We applied this function twice.
First we transformed our original image into frequency domain and applied dct function. Then we converted it into spatial domain and applied dct again.
We got our result as a fully encrypted cipher image which is totally unrecognizable.
The experimental results are shown in the figures below:



Original Image Frequency Domain: fft2 ()

DCT: dctmtx()

Figure 3: Operations in Frequency Domain.



Spatial Domain: conv() Final Image: dctmtx()

Figure 4: Operations in Spatial Domain.

The step by step implementation procedure can be described as a form of algorithm:

```
1. get image data= x
2. if (imread=true)
3. { perform 2D fourier transform:
      x= Fft2(x);
      read the new image=x;
      execute 2D DCT encryption:
      x= dctmtx(x);
      transform image into spatial domain:
      x= conv2(x);
      execute 2D DCT for second time:
      x= dctmtx(x);
}
4. read output image:
   imshow (x);
5. end ;
```

We can see the difference of the input image and the output image:

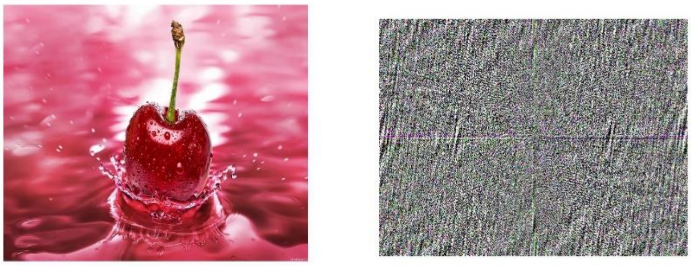


Figure 4: Original and Encrypted Image.

VIII. Conclusion

The investigational result displays that, the encrypted image is highly protected in terms of confidentiality and reliability. This double domain encryption technique encrypts the image two times within a very satisfactory computational time. As the dct function also compress the image, the transmission time is also reduced. And as this is a modified dct of lossless compression, the quality of original image remains unchanged.

As a future work for this we suggest to test this scheme against different kind of attacks that are possible in DCT encryption.

References

[1] Ahmad, Jawad & Ahmed, Fawad. (2012). Efficiency Analysis and Security Evaluation of Image Encryption Schemes. IJENS. 12. 18-31.

[2] Ahmad, J., Khan, M.A., Ahmed, F. Et al. Neural Comput & Applic (2017). Https://doi.org/10.1007/s00521-017-2970-3

[3] Alireza Jolfaei, Abdolrasoul Mirghadri. An image encryption approach using chaos and stream cipher (Journal of Theoretical and Applied Information Technology - 2010)

[4] Alireza Jolfaei, Xin-Wen Wu, Senior Member, IEEE, and Vallipuram Muthukkumarasamy. On the Security of Permutation-Only Image Encryption Schemes (Ieee Transactions On Information Forensics And Security- 2015)

[5] Bajpai, P., Kumar, P., & Tewari, R. G. (2017). Greedy Algorithm for Image Compression in Image Processing. International Journal of Computer Applications, 166(8).

[6] Dalal, M. S. (2017). Review Paper on Image Compression Using Lossless and Lossy Technique.

[7] Jeyanthi, N., Thandeeswaran, R. (2017). A Contemplator on Topical Image Encryption Measures. Security Breaches and Threat Prevention in the Internet of Things (chapter 9).

[8] JOLFAEI, A., & MIRGHADRI, A. (2010). An Image Encryption Approach Using Chaos and Stream Cipher.

[9] Jolfaei, Alireza & Wu, Xin-Wen & Muthukkumarasamy, Vallipuram. (2015). On the Security of Permutation-Only Image Encryption Schemes. IEEE Transactions on Information Forensics and Security. 10.1109/TIFS.2015.2489178.

[10] Khan, Sahib & Irfan, Muhammad Abeer & Ismail, Muhammad & Khan, Tawab & Ahmad, Nasir. (2017). Dual lossless compression based image steganography for low data rate channels. 60-64. 10.1109/COMTECH.2017.8065751.

[11] Krikor, L., Baba, S., Arif, T., & Shaaban, Z. (2009). Image encryption using DCT and stream cipher. European Journal of Scientific Research, 32(1), 47-57.

[12] Pakshwar, R & Kumar Trivedi, V & Richhariya, V. (2013). A survey on different image encryption and decryption techniques. Int Journal of Computer Science and Information Technologies. 4. 113-116.

[13] Ramandeep Kaur & Er Sumeet Kaur. (2016). A Survey on Existing Image Encryption Techniques. IJSTE International Journal of Science Technology & Engineering | Volume 2| Issue 12

[14] Sagade A.G, Prof. Pratap Singh. (2013) Image encryption using chaotic sequence and its cryptanalysis. IOSR Journal of Computer Engineering.

[15] Saidi, M., Hermassi, H., Rhouma, R., & Belghith, S. (2017). A new adaptive image steganography scheme based on DCT and chaotic map. Multimedia Tools and Applications, 1-18

[16] Shanker Yadav, Ravi & Rizwan Beg, Mhd &, Manish & Tripathi, Madhava. (2013). Image Encryption Techniques: A Critical Comparison. International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR). 3. 67-74.

[17] Tambe Chaitali, Gadilkar Rupali, Pawar Vimal. A Survey on New Image Encryption Algorithm Based on Diffie-Hellman and Singular Value Decomposition (International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 1, January 2017)

[18] Thota, N. R., & Devireddy, S. K. (2008). Image compression using discrete cosine transform. Georgian Electronic Scientific Journal: Computer Science and Telecommunications, 17(3), 35-43.

[19] Wenting Yuan, Xuelin Yang, Wei Guo and Weisheng Hu, "A double-domain image encryption using hyper chaos," 2017 19th International Conference on Transparent Optical Networks (ICTON), Girona, 2017, pp. 1-4.

[20] X. Deng, C. Liao, C. Zhu, and Z. Chen: A novel image encryption algorithm based on hyperchaotic system and shuffling scheme, in Proc. IEEE International Conference on High Performance Computing and Communications & International Conference on Embedded and Ubiquitous Computing, Zhangjiajie, 2013, pp. 109-116.

[21] Vinay Kumar, Manas Nanda. Image Processing In Frequency Domain Using Matlab®: A Study For Beginners. 2008. <inria-00321613>