An advanced Double Domain image encryption technique using modified DCT encryption.

[1]Farzana Kabir, [2]Jasmeet Kaur
[1]Masters in Technology (CSE), [2]Assistant Professor
[1]Department of Computer Science & Engineering,
[1]A P Goyal Shimla University, Shimla, India

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 used more in business and industrial process, military and medical and also in scientific researches, it is really an important issue to protect the confidential image data from unwanted access 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.

IndexTerms **- 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 evolution of multimedia technology in our modern generation has made digital images to play a more significant and unique role than the other data such as traditional texts, number. That's why images demand serious protection of users' privacy for all applications and during transmission [8]. While transmitting a private or confidential image over an insecure transmission channel over internet, it is necessary to ensure the security and privacy and preserve the confidentiality of the image. Encryption is the process of encoding messages & information in such a way that only authorized persons can be able to access 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 techniques attempt to convert original image to another image that is tough to understand; to keep the image confidential between authorized users, in other word, it is important that nobody could get to know the content without a key for decryption. Image hiding or encryption methods and algorithms ranges from simple spatial domain methods to more complicated and reliable frequency domain. [25]

To preserve secrecy and retaining the confidentiality of images is a vibrant area of study, with two different approaches being followed, the first being encrypting the images through encryption algorithms using keys, the other approach involves dividing the image into random shares to maintain the images secrecy.

Encryption of images may generally be categorized based on the nature of recovered image as either lossy or lossless image encryption. This classification resulted in the following two different lines of approaches being adopted for maintaining confidentiality of images. [29]

Encryption is a technique 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, Wenting Yuan, Xuelin Yang, Wei Guo, and Weisheng Hu proposed a double-domain image encryption using hyper chaos. This paper discovered an image encryption strategy during transmission that works in both frequency domain and spatial-domain using digital hyper chaos. In the proposed encryption technique, the image was encrypted in both frequency and spatial-domain.

Chengqing Li and Dongdong Lin did cryptanalyzing an image scrambling encryption algorithm of pixel bits 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 introduced a (k,n)-sharing matrix S (k,n) and its generation algorithm in their paper titled "Combination of sharing matrix and image encryption for lossless (k; n)-secret image sharing" in 2016. They used mathematical analysis in order to show the potential of their approach for secret image sharing. Further, they proposed a lossless private image sharing mechanism by combining sharing 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 method that is based on a modified logistic map algorithm, compressive ghost imaging, and coordinate sampling is proposed. [20] In this method, first the random phase-only mask was generated with the modified logistic map. By using the 2D discrete cosine transformation, multiple secret images were spared. These images were scrambled by different random sequences. Then the scrambled images were combined into one image with the use of coordinate sampling matrices. This image was put on the object plane of the Compressive ghost imaging system.

Hongjun, Abdurahman Kadir and Xiaobo Sun (2017) proposed another chaos based color image encryption method. The highlight of this scheme is to apply randomly sampled noise signal for serving as the initial value of the chaotic system. They got one time initial value from the 256-bit hash value of noise. In this approach, they only performed exclusive or (XOR) operation. This operation was applied to diffuse the pixels of the image. Some specific measures were taken to speed up the encryption technique. To measure the reliability and efficiency of the approach, they performed some statistical tests in terms of complexity and security.

IV. PROBLEM FORMULATION

In multimedia data high degree of redundancy is found and fast interaction is needed. Some method provide security to a great extent but slow in speed while some provide speed but less efficient. [13] Classical cryptographic algorithms such as RSA, DES etc are inefficient for image encryption due to image inherent features, especially high volume image data. Due to large data size and real time requirement, the algorithms that are appropriate for textual data may not be suitable for multimedia data.
Since image data is far more complex and part of whom is redundant, encryptions based on one-dimensional (1-D) data is not effective enough for image encryption. [19]

The important difference between image encryption and text encryption is the image size which is almost always much greater than the text size. For that the use of traditional cryptosystems need much time to encrypt the image. The other different is related to decryption, the decrypted image allowed to some changing from the original image while this is not allowed in text decryption. [17]

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 often greater than text. Therefore, the old-fashioned encryption algorithms need a lengthier time to straightly encrypt the image. Large, complex and very problematic and security examination turn the encryption technique more time overwhelming. [16]
- Security Level: Mainstream of the current image security systems are not concerned to protect against the modern breaking attacks. Once it comes to the image transmissions over the internet, image security becomes the foremost security alarm. But these existing image security mechanisms flop to afford the best image security and sometimes proved to be breakable.
- 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 technique instead of any single domain encryption. The digital image can be encrypted in both frequency and spatial-domain.
To promote robustness against any necessary image processing operations and to be resistant to various attacks, frequency-domain encryption is a key part of the scheme, where a proper spatial-domain encryption is also adopted. [19]
The results of [19] show that, the combination of frequency and spatial-domain encryptions significantly enhances the security level of image encryption.

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 technique is the coefficient based transformation in which the colored features of the input image are been analyzed and processed. [5] The DCT is a mathematical transformation that takes a signal and transforms it fromspatial domain into frequency domain. It converts an image block into its equivalent frequency coefficients. The DCT transform of an image brings out a set of numbers called coefficients. [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 used in such applications are of highly important information, and losing any amount of information is not allowed.

5.3 To Reduce Computational Time

To reduce the computational time of image encryption, we will use DCT image encryption mechanism. This algorithm will not encrypt bit by bit the whole image but only selective DCT coefficients will be encrypted.
The operation is done not by encrypting all the bytes in the image but only special frequencies in which when it return to its corresponding pixel values all the bytes of the image will be affected. The algorithm considered as a fast image encryption algorithm, due to the selective encryption of certain portion of the image (the DC and some AC coefficients). [11]

VI. METHODOLOGY

As we already mentioned we are going to use DCT image encryption and compression in a double domain phase, we need to choose which domain we will select for image encryption. Many image encryptions have been proposed, mainly by encryption in a single domain, either in spatial or frequency-domain. [20]
The results of [19] show that, the combination of frequency and spatial-domain encryptions significantly enhances the security level of image encryption.
Therefore we need to see what will happen inside the frequency domain and spatial domain when we apply DCT operation for image encryption.
The DCT is a mathematical conversion that proceeds a signal and alters it from spatial domain into frequency domain. Many digital image and video compression schemes use a block-based DCT, because this algorithm reduces the quantity of data needed to reconstruct a digitized image. In particular, JPEG and MPEG use the DCT to concentrate image material by removing spatial data redundancies in two-dimensional images. [41]
In the standard JPEG encrypting, the representation of the colors in the image is decomposed in 8×8 blocks, these blocks are changed from the spatial to the frequency domain by the DCT. Then, each DCT coefficient is divided by its corresponding persistent in a regular quantization table and rounded down to the nearest number. After this step, the DCT quantized coefficients are scanned in a predefined zigzag order to be used in the final step, the lossless compression as illustrated in figure.
In each block the 64 DCT coefficients are fixed up from the lowest upper left corner to the highest frequencies at lower right corner [42].
The most important visual characteristics of the image are placed in the low frequencies while the details are situated in the higher frequencies.

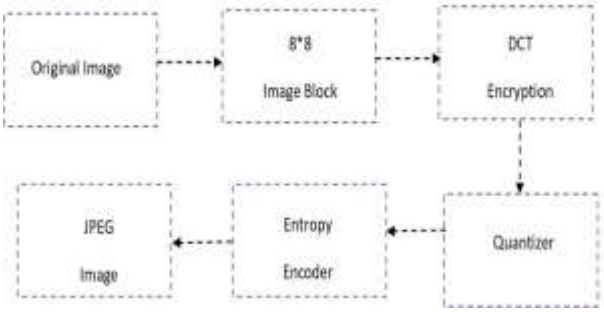


Figure 1: Steps in DCT encryption

- At first we divide original image to be transferred into 8*8 small square blocks.
- We apply two-dimensional discrete cosine transform to each of the following blocks and we obtain DCT components of each block. Working from left to right, top to bottom, the DCT is applied to each block. [44]
- Each block is compressed through quantization. The quantizer performs the quantization operation. We will use lossless compression so that the quality of the image remains unchanged.
- The array of compressed blocks that creates the image is saved in a significantly reduced volume of storage.

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.

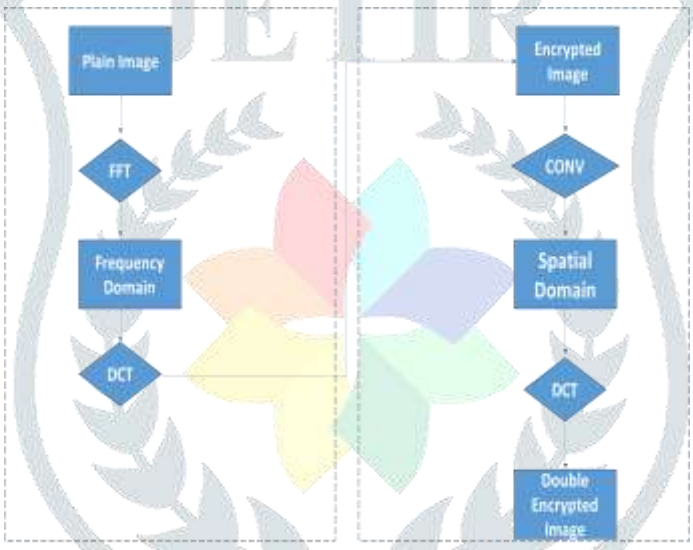


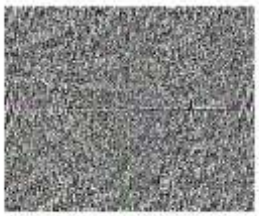
Figure 2: Block Diagram of the operations

VII. IMPLEMENTATION

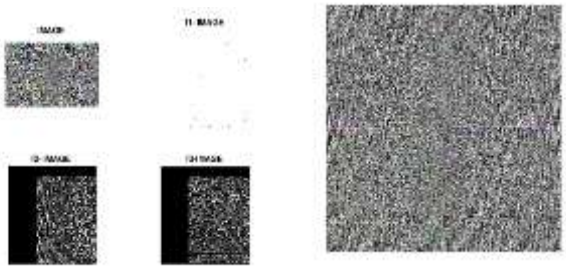
We implemented our proposed scheme in MATLAB 2018a. We had to install the image processing toolbox add on to perform the dct operation. In Matlab the Lossless DCT can be performed by using dctmtx () function. We applied this function twice.
First we transformed our original image into frequency domain 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 Image and Encrypted Image.

VIII. CONCLUSION

The experimental result shows that, the encrypted image is highly secured 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>