Secure Data Transfer with Image Encryption

M. Kundalakesi[1] M. Harinee[2]
[1]Assistant Professor [2]Student
[1,2]Sri Krishna arts and Science College, India

Abstract— A secure data transfer framework is developed using a novel scheme based on data hiding. A separable reverse data hiding is designed in the image encryption in this approach. Initially the data owner encrypts the original image with an encryption image. Then, a sender compresses the image with least significant bits to create a sparse space to cover some additional data. With the data-hiding key, he/she can able to obtain additional data. In the same way with the encryption key he/she can decrypt the original image but cannot extract the additional data. In order to obtain the both image and additional data the user have to know both the keys.

Key words: Image Security, Image steganography, Encryption, Data hiding, Decryption

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 assists 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 [1]. During the image transformation over internet security is a major issue. Encryption is the only way to create a secure ciphertext which will be accessed by a authorized users. 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 [2]. Encryption is the process of disguising a message [3]. In encryption, the content of confidential data is protected and a key is required to decrypt the information properly. The original message is called the Plaintext and the encrypted message is called the ciphertext [3]. It can be employed to various types of data like text, image, audio etc. [4] Image encryption is one of the techniques that grips restraint of image. Image encryption provides a prominent strategy to secure the image over internet. Encryption of image is possible with the traditional data encryption algorithms such as DES, RSA etc. But they are not totally efficient for image data. [4] Digital image contents needs to be secured from various types of attacks such as interruption, interception, modification, and fabrication etc. [5]. The image size is usually more than text. For which, the traditional encryption algorithms need more time to directly encrypt the image data. While applying large, complicated and difficult performance and security analysis, the encryption technique becomes more time-consuming. [6] Most of the existing image security systems are not up to date enough to fight against the latest possible attacks. While transferring images over the internet, image security becomes the major security concern for military, security agencies, social or mobile applications. But existing image encryption mechanisms fail to provide better image security and sometimes proved to be breakable or hackable. The security of a recently published image encryption scheme based on a compound chaotic sequence was studied. It was proved before that with only three images, the scheme can be broken. The attack takes less than one minute on MATLAB running on Mac OS to completely break the image encryption algorithm. [7]

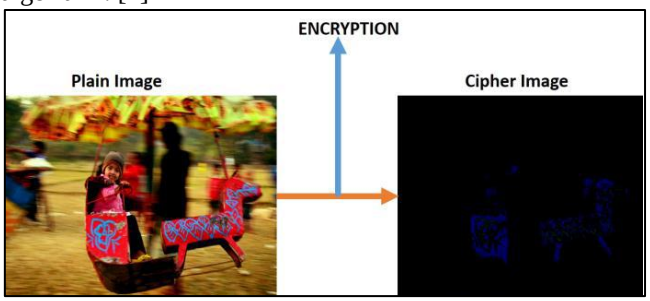

Fig. 1: Image Encryption Technique

II. LITERATURE REVIEW

Eman A. Al-Hilo, Rusul Zehwar [8] proposed the fractal compression technique by Jacquin is investigated for 24 bits/pixel color image. The data of the color component (R, G, B) are transformed to (YIQ) color space, to take the advantage of the existing spectral correlation to gain more compression. In addition the low spatial resolution was used to improve the compression ratio without making significant subjective distortion. The experiment was performed with Lena image (256x256) pixel and the performance evaluation results show that PSNR (31.05) dB with CR (8.73) and encoding time (57.55) sec.

Xiangui Kang, Jiwu Huang [9] has been demonstrated the water marking extraction for JPEG compression. In watermark extraction, authors at first detect the template in a possibly corrupted watermarked image to obtain the parameters of affine transform and convert the image back to its original shape. Then they have performed translation registration by using the training sequence embedded in the DWT domain and finally extract the informative watermark. The performance evaluation is performed which shows the watermark generated by the proposed algorithm. In particular all affine transform in StirMark 3.1 and JPEG compression with quality factor as low as 10 simultaneously.

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. This scheme is named as SMIE-SIS. SMIE-SIS encrypts the plain image by substitution. They implemented many simulation

operations with binary, grayscale and color images by using SMIE-SIS with sharing matrices to determine the robustness of this method. [10]

Wenting Yuan, Xuelin Yang, Wei Guo, and Weisheng Hu proposed a double-domain image encryption using hyper chaos. The author found an image encryption approach during transmission which works in both frequency domain and spatial-domain. The image is encrypted in both frequency and spatial-domain using XOR operation in this proposed approach. The author focused on entropy correlation and the multi-level chaotic encryption was tested and verified using the experiments contacted. This double domain encryption approach had the maximum entropy value and minimum absolute value of correlation. The performance evaluation shows the security efficiency in encryption But in future, the speed of transmission needs to be increased more to make it more efficient. [11]

III. PROPOSED SYSTEM

The framework for secure data transfer is designed based on image encryption. This work is designed with the separable reversible data hiding technique. The original image is encrypted using an encryption key and the additional data are embedded into the encrypted image using a data-hiding key. The receiver has to contain both data-hiding key and encrypted key to obtain the original image. With the data hiding key the user can extract the additional data respectively the image can be obtain with the encrypted key. Therefore the receive has to know the both keys. The main process of the proposed approach is shown in figure 1. In this approach the content owner first encrypt the original image using encryption key then additional information is hided in the image using hiding key. This secured data is transferred over the network. On the other hand the receiver has to follow the same reverse process to obtain the additional information and the image as the plaintext.

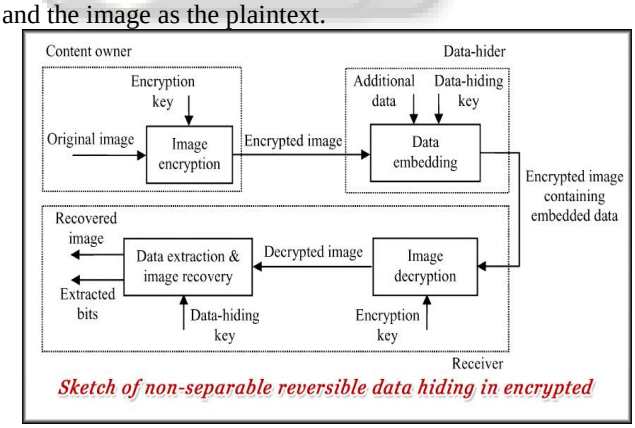

Fig. 2. Image Encryption + Data Hiding Process

IV. IMAGE ENCRYPTION

Assume the original image with a size of [N1, N2] is in uncompressed format and each pixel with gray value falling into [0, 255] is represented by 8 bits.

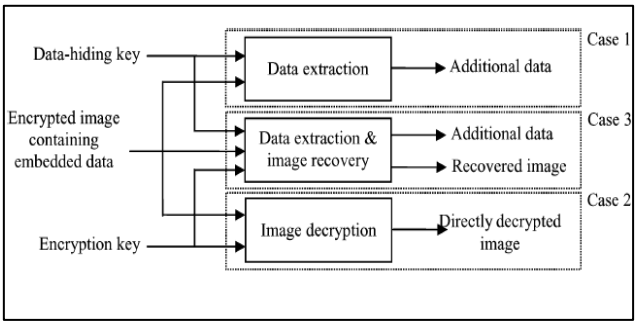

Fig. 3: Three Cases at the Receiver Side

V. DATA EMBEDDING

In the data embedding phase, some parameters are embedded into a small number of encrypted pixels, and the LSB of the other encrypted pixels are compressed to create a space for accommodating the additional data and the original data at the positions occupied by the parameters.

VI. DATA EXTRACTION & IMAGE RECOVERY

In this phase, we will consider the three cases that a receiver has only the data-hiding key, only the encryption key, and both the data-hiding and encryption keys, respectively. With an encrypted image containing embedded data, if the receiver has only the data-hiding key, he may first obtain the values of the parameters.

	$S=1$	$S=2$	$S=3$	$S=4$	$S=5$
$M=1$	54.2	52.4	51.7	51.4	51.3
$M=2$	47.2	45.4	44.7	44.4	44.3
$M=3$	40.9	39.1	38.5	38.2	38.1

Table 1: Theoretical Values of PSNR ($_D$B with Respect tp S and M)

And

$$p_{i,j} = \sum_{u=0}^{7} b_{i,j,u} \cdot 2^u.$$

$$\begin{bmatrix} B'(k,1) \\ B'(k,2) \\ \vdots \\ B'(k,ML-S) \end{bmatrix} = \mathbf{G} \cdot \begin{bmatrix} B(k,1) \\ B(k,2) \\ \vdots \\ B(k,ML) \end{bmatrix}$$

VII. EXPERIMENTAL RESULT

The proposed approach is developed in C#.NET version 2011. The hardware specification are Laptop (Dell): Intel (R) Core (TM) i3-2430M CUP @ 2.40 GHz Processor, 64-bit Operating System and 4.00 GB RAM. To evaluate the performance, the proposed system has been tested using image dataset as test images. These tests explore the effect of the following coding parameters on the compression performance parameters of the established system: This set of tests was conducted to study the performance parameters of the reconstructed image.

Fig. 4:

VIII. CONCLUSIONS

The developed framework ensures the improve image security during transmission by facilitating the quick image transfers. This approach focuses on several attacks and developed an approach to overcome from those attacks. Most of the techniques tried to enhance the efficiency of the encryption technique for color image. A novel scheme for separable reversible data hiding in encrypted image. In the proposed scheme, the original image is encrypted using an encryption key and the additional data are embedded into the encrypted image using a data-hiding key. With an encrypted image containing additional data, if the receiver has only the data-hiding key, he can extract the additional data though he does not know the image content.

REFERENCES

[1] Xiangui Kang, Jiwu Huang, "A DWT-DFT Composite Watermarking Scheme Robust to Both Affine Transform and JPEG Compression", ITCSVT, vol. 13, issue 8, pp. 776-786, IEEE, 2003.
[2] KabirA survey on different image encryption and decryption techniques. Int Journal of Computer Science and Information Technologies. 4. 113-116.
[3] Ramandeep Kaur & Er Sumeet Kaur. (2016). A Survey on Existing Image Encryption Techniques. IJSTE International Journal of Science Technology & Engineering | Volume 2| Issue 12.
[4] Ahmad, J., Khan, M.A., Ahmed, F. et al. Neural Comput & Applic (2017). https://doi.org/10.1007/s00521-017-2970-3.
[5] 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.
[6] Sagade A.G, Prof. Pratap Singh. (2013) Image encryption using chaotic sequence and its cryptanalysis. IOSR Journal of Computer Engineering.
[7] Xiangui Kang, Jiwu Huang, "A DWT-DFT Composite Watermarking Scheme Robust to Both Affine Transform and JPEG Compression", ITCSVT, vol. 13, issue 8, pp. 776-786, IEEE, 2003.
[8] Gary C.Kessler, "An Overview of Cryptography: Cryptographic", HLAN, ver. 1, 1999-2014.
[9] L. Bao, S. Yi and Y. Zhou, "Combination of Sharing Matrix and Image Encryption for Lossless (k,n) - Secret Image Sharing," in IEEE Transactions on Image Processing, vol. 26, no. 12, pp. 5618-5631, Dec. 2017.
[10] 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.

