International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 09 | Sep-2016 www.irjet.net p-ISSN: 2395-0072

A Two Symmetric Keys Technique to Encrypt/Decrypt Digital Colored Image to Minimize Loss

Swati Kuamri

M.Tech. Student, National Institute of Technical Teachers' Training and Research, Bhopal, M.P., India

---

Abstract - *In modern days, data transfer through internet has become very frequent and because of that, security of data has become a matter of great concern. Therefore, hacking of data by an unauthorized user must be stopped by using a technique in such a way, so that the decrypted image may be protected from loss.*

Key Words: Encryption, Decryption, Symmetric keys, DCT.

1. INTRODUCTION

From the last few years, the use of internet has grown rapidly and widely which are used for valuable information transmission. This information may be in the form of multimedia i.e. text, image, audio, video. With the rapid growth of technology in multimedia transmission, security has become one of the most concerned fields for multimedia data transmission. The multimedia data needs to be protected from unauthorized users. To protect the data from unauthorized users a data protection technique must be required. Data encryption is one of the important techniques used for data protection. There are mainly two types of cryptography:

(i) Symmetric key Cryptography (Secret Key)
(ii) Asymmetric key Cryptography (Public Key)

In symmetric key cryptography, both sender and receiver use the same key to encrypt and decrypt the data respectively.
In asymmetric key cryptography, sender and receiver use different keys to encrypt and decrypt the data.
This encryption and decryption technique is used when secret messages are transmitted from one end to another end.

1.1 Background and Motivation of Research

Usually, people share their private information through the network. People use internet banking, online shopping and billing. Hence, data security has become the major concern for all users. Emerging changes of technology and dependability on Digital technology creates a huge demand of cryptography which is the back bone of modern digital communication system.

This research proposes an encryption and decryption technique which will be used to transmit and receive a highly sensitive data which requires security where the transmitted data is likely to be stolen by the unauthorized person. That means transmission may suffer from hacking of data. Figure 1.1 shows, 1st symmetric key which is 4*4 key has been applied on original image. Then, 2nd 8*8 Symmetric key has been applied to get double secured encrypted image. Then it is sent to receiver side where again same 8*8 symmetric key and 4*4 symmetric key has been applied to get decrypted image.

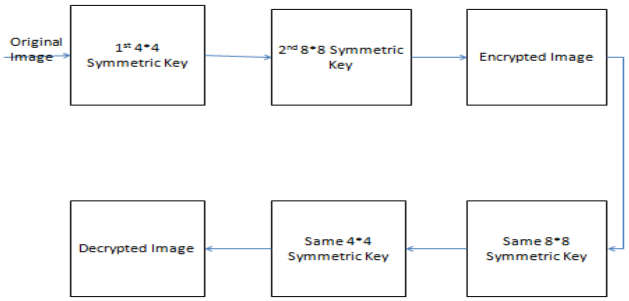

Figure 1 Encryption and Decryption Using Two Symmetric Keys.

2. ALGORITHM

2.1 Image Encryption Algorithm Using Two Symmetric Keys:-

1) A colored image has been taken in the MATLAB.
2) After this, a 4*4 symmetric key has been applied on each layer of image..
3) This process provides 1st level security to encrypted image.
4) After this, an 8*8 symmetric key has been generated.
5) Now this key matrix has been applied to each layer of 1st level of encrypted image and the final encrypted image has been generated.

2.2 Image Decryption Algorithm Using Two Symmetric Keys:-

1) The same 8*8 symmetric Key is applied to the encrypted image to get one level of decrypted image.

2) Then, 4*4 symmetric key is applied to the image to get the original image.

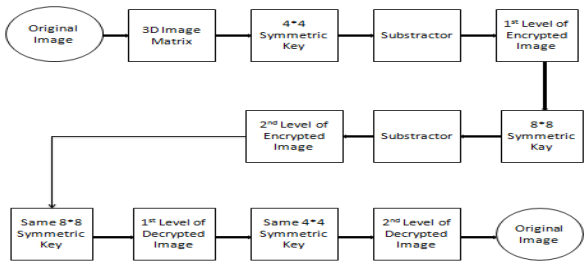

Fig - 2: Block Diagram of Proposed Technique.

Figure 2 is showing block diagram of proposed technique. In this diagram, 4*4 symmetric key is applied on original image and it is followed by 8*8 symmetric key which gives encrypted image. At receiver end, reverse process has been done and original image is obtained.

3. EXPERIMENT AND RESULT

3.1 Experiment

Table 1 Original Image which is to be implemented.

Image Name	Image Format	Image Size	Image Dimension
(a) nitttr	.jpg	48.3KB	332*314
(b) food2	.targa	57.8KB	419*601
(c) tree	.exif	397KB	382*680
(d) drop	.png	395KB	297*602

Table 1 is showing original images with their properties which is to be implemented.

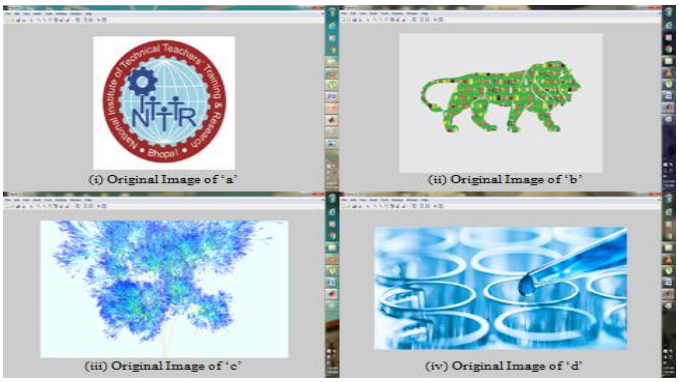

Fig- 3: Original image

Figure 3 is showing original image on which proposed technique is going to be implemented.

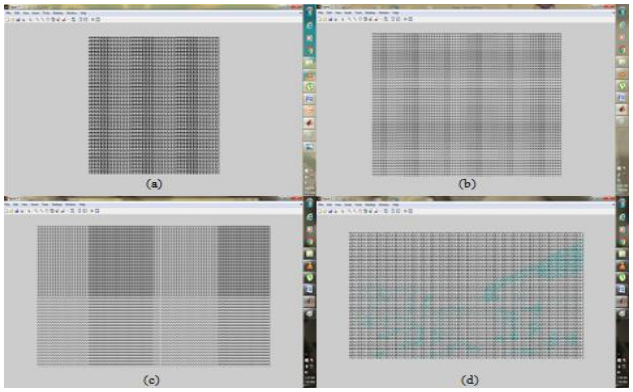

Fig - 4: Encrypted image using two symmetric keys

Figure 4 is showing final encrypted image using two symmetric keys i.e. 4*4 and 8*8 symmetric keys.

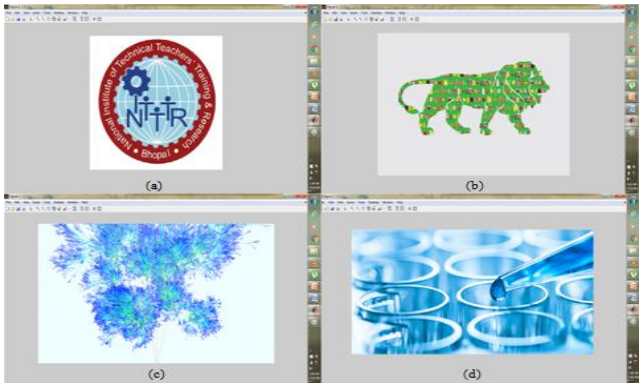

Fig - 5: Decrypted image using two symmetric keys

Figure 5 is showing finally decrypted image using 8*8 symmetric key and 4*4 symmetric key.

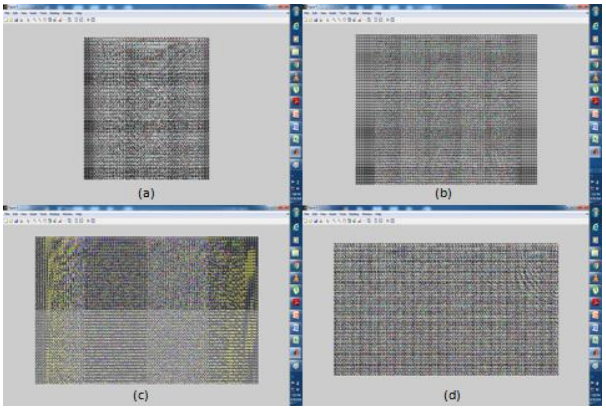

Fig - 6: Encrypted image using DCT algorithm

Figure 6 is showing encrypted image of each original image using DCT algorithm.

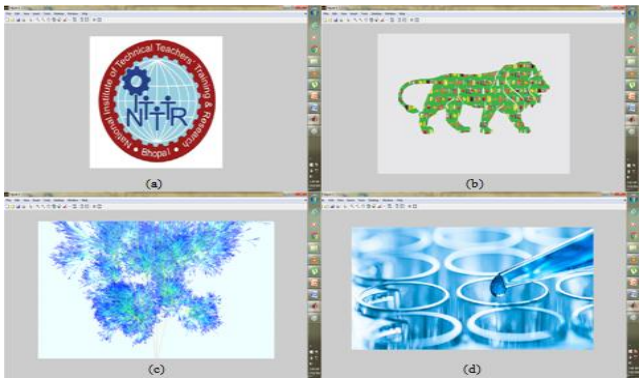

Fig - 7: Decrypted image using DCT algorithm

Figure 7 is showing decrypted image of original image using DCT algorithm.

3.2 Results

Table 2 Mean square error of images using two symmetric keys and DCT

Image Name	MSE Of DCT Algorithm	MSE Of Two Symmetric Keys Algorithm
(a)	27.4013	0
(b)	91.9224	0
(c)	82.7632	0
(d)	2.6638	0

Table 2 is showing comparison of MSE of each image using two symmetric keys and DCT algorithm. With this comparison, it can be observed that two symmetric keys algorithm has negligible MSE, unlike DCT algorithm which is showing large amount of MSE. Thus, with this comparison it can be concluded that two symmetric keys technique is showing better results than DCT algorithm in terms of MSE for each image.

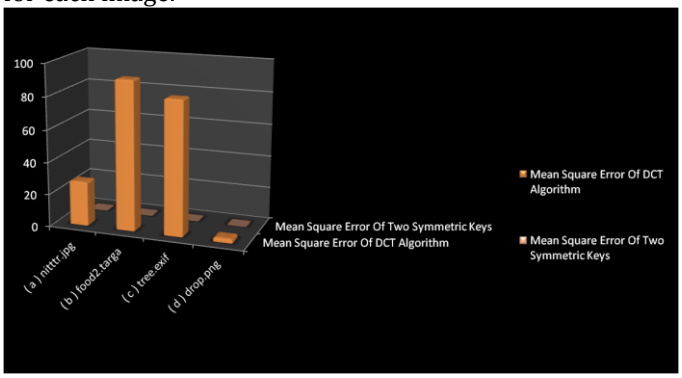

Fig - 8: Comparison of two symmetric keys and DCT algorithm in terms of MSE

Now, Figure 8 is showing comparison of mean square error of discrete cosine transform and mean square error of two symmetric keys algorithm with the help of column chart.

4. CONCLUSION

By referring results in section 3.2, it can be concluded that proposed algorithm (two symmetric keys technique) is showing better result than DCT algorithm in terms of mean square error (MSE) for the digital colored image of any size, dimension and format.

REFERENCES

[1] Alireza Jolfaei, Xin-Wen Wo, "On The Security Of Permutation-Only Image Encryption Schemes", *IEEE Transaction on Information Forensics and Security,* Vol.11, No.2, Feb 2016.

[2] Mariusz Dzwonkowski, Michal Papaj, Roman Rykaczewski, "A New Quaternion-Based Encryption Method For DICOM Images", *IEEE Transaction On Image Processing,* Vol.24, No.11, Nov, 2015.

[3] Firas Hassan, Michael Limbird, Vishwanath Ullagaddi, Vijay Devbhaktuni, "A New Image Stream encryption Technique", *IEEE,* 2014.

[4] T. Uehara, R. Safavi-Naini, "Chosen DCT Cofficients Attack On MPEG Encryption schemes" *in Proc. IEEE Pacific-Rim Conference Multimedia, pp. 316-319,* Dec 2000.

BIOGRAPHY

Swati Kumari, M.Tech. Student, National Institute of Technical Teachers' Training and Research, Bhopal, M.P., India.