Cryptography algorithm using DCT transform for colour images

Tribodh Tripathi , Bharti Chourasia, Anshuj Jain

***Abstract*-** In this research work a cryptography algorithm is proposed for colour images using DCT transform. Proposed work provides symmetric key cryptography method for colour images. Image is encrypted with the help two public key of matrix size 4*4 and 8*8 along the image. Cryptography algorithm follows perfect square matrix approach to reduce losses during encryption and decryption process. Here 24 bit jpg image is used for encryption purpose. Proposed algorithm is implemented in MATLAB simulator software. Mean square error represents that proposed algorithm using DCT shows acceptable quality of results. Histogram representation of images describe that output shows acceptable error and proposed algorithm without using any transform shows better results.

***Index Terms*-** Encryption, Decryption, Cryptography, Symmetric key, DCT, Cipher Image

Objective-

The objective of this research work is to access need of new cryptography algorithm to provide secure image transmission with acceptable quality of results.

Literature Review

Vincy.J , Gowtham.K , 2014 [2] has proposed new approach of cryptography algorithm. Algorithm gives fine results with some draw backs. Whenever image size is increased, it takes more time to encrypt. So further analysis of various techniques of encryption and decryption of image are very much needs to achieve satisfaction.

Niraj kumar, Dr. Sanjay Agrawal, 2013 [3] provided symmetric key cryptography algorithm for image transmission they drew certain conclusion:

1. There is a need of new version of Video Encryption Algorithm (VEA) is developed, which required less computation than the old version and achieve the same encryption results. That algorithm can be used to secure many MPEG video applications.
2. Some algorithm can achieve an acceptable quality of service and suitable for different security level of the video
3. Some encryption model based on the orthogonal transforms for images. Symmetric encryption method use Malakooti Raeisi (M-R) transform algorithm for key generation of DCT, HT and MT.
4. Cryptography algorithm for multimedia (that is images and video) is not so easy. DES, AES, RES are not suitable for colour images and video, which have 3D arrays of data

Dr. Mohammad V. Malakooti, Mojtaba Raeisi Nejad Dobun, 2012, [4] has proposed a new algorithm for images based on the orthogonal transforms. This method is based on the block cipher symmetric key cryptography. In this paper Author emphasis on development of a novel lossless digital encryption system for multimedia.

Francesco, Benedetto, Gaetano Giunta, 2011, [7] Researcher provided a fast generation procedure of authentication codes, for images content cryptography, whose length and computational complexity can be tuned accordingly to the specific mobile service and application. Authors suggested a digital algorithm to generate a pair of long (asymmetric) keys from one short primitive key.

Sahar Mazloom, Amir-Masud Eftekhari –Moghadam, 2011, [8] proposed a novel image cryptographic algorithm based on confusion–diffusion architecture that is specifically designed for color images encryption, which are 3D arrays of data streams. An image encryption is somehow different from text data encrypted due to some inherent features of the images.

Piyush Marwaha, Paresh Marwaha, 2010, [11] has described that Cryptography and steganography area unit the foremost wide used techniques to beat this threat. Cryptography involves changing a text message into an unreadable cipher. On the opposite hand, steganography embeds message into a canopy media and hides its existence. Each these techniques give some security of information neither of them alone is secure enough for sharing data over an unsecure communicating and area unit susceptible to trespasser attacks.

ISSN: 2278 – 7798

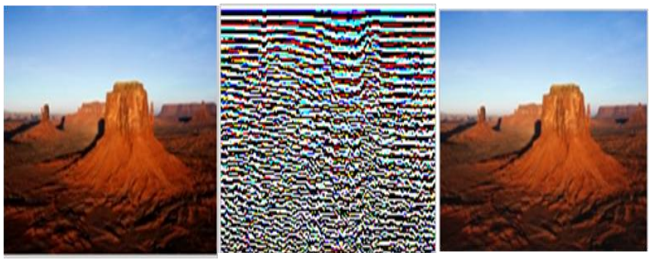
Methodology

Step 1- Take an original image
Step 2- Divide image into divisible image matrix
Step 3- Extract red colour component from original image
Step 4- Extract green colour component from original image
Step 5- Extract blue colour component from original image
Step 6- Reshape RGB component separately by using two keys
Step 7- Combine all encrypted RGB component into a single matrix
Step 8- Apply DCT transform to get encrypted image
Step 9- End
Proposed algorithm is implemented in MATLAB software

Result Analysis

Results were found after implementing experimental setup in MATLAB simulator software

Here Discrete Cosine Transform is used to encrypt the image Figure 1.2 represents encrypted image using DCT transform, Figure 1.4 represents red colour component of original image, Figure 1.5 Represents green colour component of original image, Figure 1.6 Represents blue colour component of original image, 1.7 Represents encrypted red colour component, 1.8 Represents encrypted green colour component, 1.9 Represents encrypted blue colour component Figure 1.10 represents encrypted red colour component using DCT transform, Figure 1.11 represents encrypted green colour component using DCT transform, Figure 1.12 represents encrypted blue colour component using DCT transform.



1.1 Original Image 1.2 Encrypted image using DCT 1.3 Decrypted image

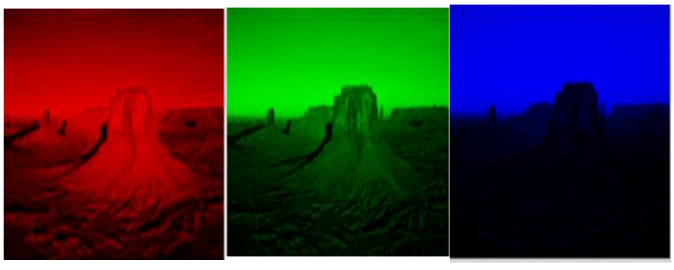


Fig-1.4 Fig- 1.5 Fig-1.6

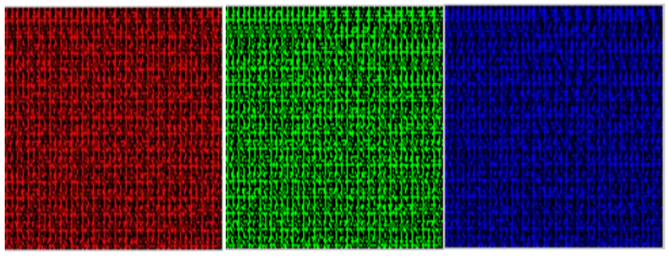


Fig-1.7 Fig-1.8 Fig-1.9

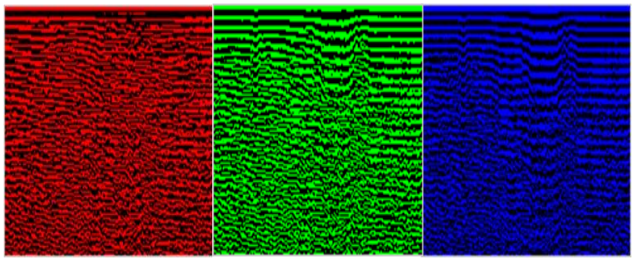
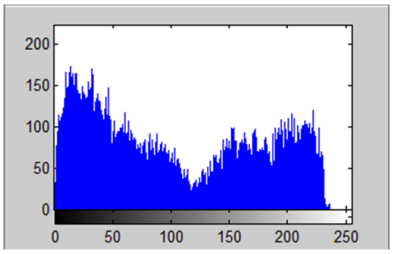


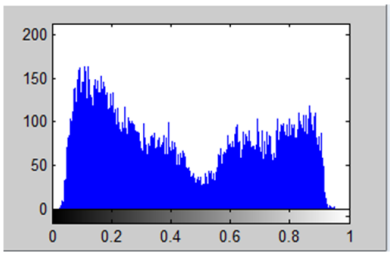
Fig-1.10 Fig-1.11 Fig-1.12

Histogram Representation of Images

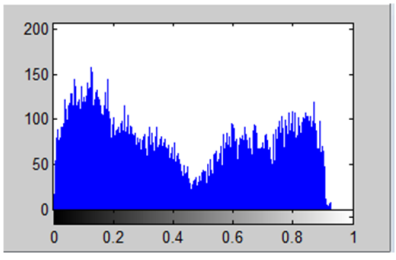
In plotted histogram x axis represents the grey colour level of given image and y axis represents number of pixels in each grey level. Figure 1.13 represents histogram of original image. Figure 1.14 represents histogram of decrypted image using DCT. Here both histograms is not identical, Figure 1.14 shows certain losses as compare to Figure 1.13. Here we can say that proposed algorithm using DCT provide certain error, Figure 1.15 is similar to Figure 1.13 that means histogram of decrypted image without using any transform shows better result



1.13 Histogram of original image



1.14 Histogram of decrypted image using DCT



1.15 Histogram of decrypted image without using any transform

ISSN: 2278 – 7798

Mean Square Error of Proposed Work

Here proposed algorithm is compared with other algorithms. Result describes that proposed work provides satisfactory outcome. Here N represents the block size, Zero mean square error represents that transmission is lossless.

Transform / Mean Square Error	**N=32**	**N=64**	**N=128**
Discrete Cosine Transform (DCT)	5.079 E-9	5.640 E-9	6.249 E-9
Malakooti Transform (MT)	0	0	5.749 E-17
Hadamard Transform (HT)	0	0	0
Proposed algorithm using DCT	2	2	1
Proposed algorithm without using any transform	0	0	0

Table 1.1 Mean Square error for various transform

Conclusion

We have successfully received the original image by implementing unique cryptography algorithm. Here symmetric key cryptography is used for encryption and decryption purpose. Results were found after implementing proposed algorithm in MATLAB software. Results were compared with other encryption techniques by using various transform. Present study shows the acceptable quality of results. Result analysis describe that the proposed algorithm is secured for image transmission. Mean square error shows that proposed work provides acceptable error during using DCT transform. Proposed algorithm without using any transform provides zero mean square error.

References

[1] Tribodh Tripathi, Anshuj Jain, Bharti Chourasia "Study on generating a cryptography algorithm for image transmission with no losses"; October 2015 ; IJSETR, Volume 4, Issue10

[2] Vincy.J , Gowtham.K "Design of New Cryptosystem Using Menezes Vanstone Cryptosystem " ; February 2014 ; IGARCSSE ,Volume 4, Issue 2

[3] Niraj kumar, Prof Sanjay Agrawal "Issues and Challenges in Symmetric Key based Cryptographic Algorithm for Videos and Images "; May 2013; IGARCSSE ,volume 3

[4] Dr. Mohammad V. Malakooti, Mojtaba Raeisi Nejad Dobuneh "A Lossless Digital Encryption System for Multimedia Using Orthogonal Transforms"; 2012; IEEE; 978-1-4673-0734-5/12/2012 IEEE.

[5] W. Puech, Z. Erkin, M. Barni, S. Rane, and R. L. Lagendijk "Emerging Cryptographic Challenges In Image And Video Processing Mitsubishi Electric Research Laboratories", TR2012-067 September 2012.

[6] Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh Sushanta Biswas, D. Sarkar, Partha Pratim Sarkar "Image encoding exploitation Affine remodel and XOR Operation" Proceedings of 2011 International Conference on Signal process, Communication, Computing and Networking Technologies (ICSCCN 2011)].

[7] Francesco, Benedetto, Gaetano Giunta "An Effective Code Generator for Frequent Authentication of Multimedia Contentsin Mobile Applications and Services" IEEE; 2011 Digital Signal Processing, Multimedia, and Optical Communications Lab. Dept. of Applied Electronics, University of ROMA TRE©2011978-1-4244-8331-0/11].

[8]SaharMazloom,Amir-MasuEftekhar–Moghadam,"ColorImage Cryptosystem using Chaotic Maps"; 2011 IEEE ; Faculty of electricacomputer and IT Engineering, 978-1-4244-9915-1.

[9]Sandeep Bhowmik Sriyankar Acharyya "Image Cryptography: The Genetic Algorithm Approach" IEEE; 2011, 978-1-4244-8728-8/11]

[10] Fan Wu, Chung-han bird genus, and Hira Narang "AN economical Acceleration of bilaterally symmetrical Key Cryptography victimization General Purpose Graphics process Unit" technology Department Tuskegee University 2010 Fourth International Conference on rising Security data, Systems and Technologies]

[11]Piyush Marwaha, Paresh Marwaha "Visual Cryptographic Steganography In Images" IEEE Infosys Technologies Limited, India, @2010, 978-1-4244-6589-7/10/2010].

ISSN: 2278 – 7798