Study on generating a Cryptography Algorithm for image transmission with no losses

Tribodh Tripathi , Anshuj Jain, Bharti Chourasia

Abstract— In this research work an effective algorithm is proposed for Digital Image Transmission to happen without any losses.

Proposed work provides a new symmetric key generation method for colour images. The encrypted image is obtained with the help of three OTP (One Time Password) which provide two public key of matrix size 4*4 and 8*8 along the image. To obtain original image from encrypted data, a decryption process (reverse process of encryption) was used. Through this, the original image was retrieved successfully at receiving end.

To make transmission lossless, a perfect divisible matrix approach has been followed; encrypted image was transmitted by changing the pixel value of original image

The experimental result has been shown by implementing proposed algorithm in MATLAB simulator software. Mean square error represents that proposed algorithm is lossless for image transmission.

Index Terms— Encryption, Decryption, Cryptography, Symmetric key, Cipher Image

INTRODUCTION

During the last decade the use of internet has grown rapidly and widely used for valuable information transmission. This information may be in the form of multimedia (text, image ,video). With the rapid growth of technology in multimedia transmission, Security is primary need for multimedia data transmission. The multimedia data needs to be protected from unauthorised user .To protect data from unauthorised user , data protection technique is required. Data encryption is one of the important techniques used for data protection

Digital image processing is an emerging area of research. Digital images are transmitted over a channel and in our daily life we share our valuable images with friends and family. At present two fundamental technologies are used to protect the image, these are Water marking and Encryption. A lot of research work has been completed in Water marking, however image encryption is still a promising area of research where much is unexplored.

TECHNICAL REVIEW

Kaladharan N, 2014 [1] 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 [2] 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, [3] 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, [6]: 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, [7] 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, [10] 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.

METHODOLOGY

A colour image with resolution of 165*124 has been used. We have used 24 bit colour image of JPG format for encryption and decryption process.
To make encryption more secure we have used 2 symmetric key by providing 3 one time password .To make transmission lossless, a perfect divisible matrix approach has been followed; encrypted image was transmitted by changing the pixel value of original image

Proposed Algorithm

Step 1- Take an original image
Step 2- Make a 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 separately by using keys
Step 7- Combine all encrypted RGB component into a single matrix
Step 8- End

RESULT ANALYSIS

Results were found after implementing experimental setup in MATLAB. In proposed algorithm an original image (figure 1.1) is used for encryption and decryption. We have implemented a new symmetric key generation method for colour image. In symmetric key cryptography, the two people that exchange information use the same algorithm. The encrypted image is obtained with the help of two secret key of matrix size 4*4 and 8*8 along the image. To obtain original image from encrypted data a decryption process was used. Original image was retrieved successfully at receiving end.

Fig- 1.1 Original image

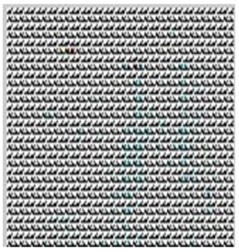
Fig - 1.2 Cipher Image

Fig -1.3 Decrypted image

Here, figure 1.2 represents encrypted image which is also known as cipher image , the cipher image is totally different than original image and this image can be accessed by any person. It may be noted, only valid person will be able to decode or decrypt the original image. Figure 1.3 represents the decrypted image. This algorithm provides content security because image cannot be read without the secret key. 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. Different colour components were extracted from original image. Colour components were encrypted by applying symmetric keys. Figure 1.7 represents encrypted red colour component of original image. Figure 1.8 represents encrypted green colour component of original image. Figure 1.9 represents encrypted blue colour component of original image

Fig -1.4

Fig-1.5

Fig-1.6

Fig-1.7

Fig- 1.8

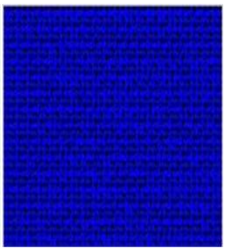
Fig-1.9

HISTOGRAM REPRESENTATION OF IMAGES

By definition histogram of an image represents the relative frequency of occurrence of the grey levels in an image. In plotted histogram x axis represents the grey level and while y axis represents number of pixels in each gray level, here figure 1.9 represents the histogram of original image , figure 1.10 represents the histogram of decrypted image and figure 1.1 represents the original image which is used for encryption purpose

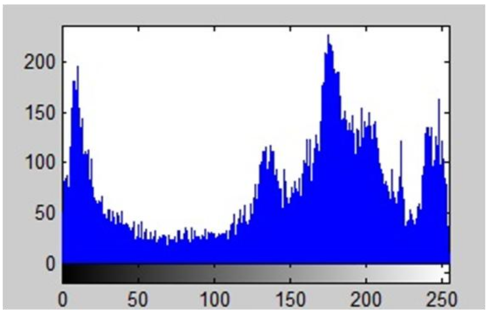

Fig-1.9 Histogram of original image

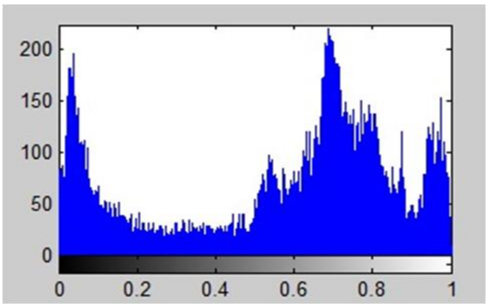

Fig- 1.10 Histogram of decrypted image

Both histograms either encryption or decryption are similar that means decrypted image has same intensity as original image.

MEAN SQUARE ERROR OF PROPOSED WORK

Image	N=32	N=64	N=120	N=128
Mean Square Error	0	0	0	0

Table - Mean Square error for proposed algorithm

In proposed work mean square error is calculated by comparing original image matrix to decrypted image matrix. [7]Sah Result describes that proposed work provides satisfactory outcome. Here N represents the block size. zero mean square error indicate that transmission is lossless

CONCLUSION

In this research work we have successfully provide a unique cryptography algorithm and implement it effectively with the help of MATLAB software. The feature of cryptography includes symmetric key generation encryption and decryption. We have provided two keys for more security. Image was reconstructed successfully at receiving end. Here, the algorithm was implemented, tested and analyzed for the result of proposed technique. The results were compared with other encrypted techniques and show the acceptable quality of study. According to the result analysis, the proposed algorithm is secured for image transmission. Mean square error of reconstructed image shows that proposed work provides lossless data transmission and suitable to real situations

REFERENCES

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

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

[3] 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.

[4] 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.

[5] 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)].

[6] 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].

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

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

[9] 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]

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