ENCRYPTION OF COLOUR IMAGE WITH RUBIK'S CUBE ALGORITHM FOR SECURE TRANSFER

K. Aishwarya Bhavani, M. Sri Sai Navya, M. Sivani,S. Baby Sahithi
Department of CSE, Koneru Lakshmaiah Education Foundation,
Andhra Pradesh, India
Dr Amarendra K
Professor, Department of CSE, Koneru Lakshmaiah Education Foundation,
Andhra Pradesh, India
Venkata Ramana Gupta.N
Assistant Professor, Department of CSE,
Prasad V Potluri Siddhartha Institute of Technology, Vijayawada

ABSTRACT:
For several years, the method of shielding information has been on and changes and progress have been made to ensure that the message reaches the intended recipient without unauthorized access in the middle. As pictures are being utilized more in military, business, industrial processes and furthermore in clinical and scientific research. It has become significant to ensure that these confidential images are not accessed by unauthorized users and intruders. There is a greater improvement in hacking methods and hacker intelligence with the growth of technology. Therefore, conventional encryption methods struggle to secure sensitive information or photographs because it includes the most extreme highlights of someone or something, the protection of image information is more important.Image encryption is the method of encoding a hidden image in such a way that unauthorized users cannot access it with the aid of any encryption algorithm.A lot of research on this has been done and lots of image encryption techniques have been developed.

Keywords:
Rubik's Cube Algorithm,Encryption, Confidential, Encoding, Srcambling
Article Received: 18 October 2020, Revised: 3 November 2020, Accepted: 24 December 2020

1. INTRODUCTION

Encryption is a security method in which information is encoded in such a manner that only accessed by authorized users. It uses encryption algorithm to generate cipher text that can only be access if decrypted. In the current trends, the technologies areadvanced. Many people tend to use the Internet as the main medium for transmitting data across the internet from one end to another. There are several potential ways to use the Internet to connect and transmit data. In the present communication world, images and videos are widely in use. However, security and confidentiality are one of the key issues with transmitting data over the Internet. Image encryption is a technique that converts the original image to another form which is difficult to understand. No one can access the content without having a decryption key. Encryption is the process of encoding Plain text message to text message cipher, while reverse process of transforming cipher text to plain text is called decryption. Here, we are using the Rubik's cube principle for the image to be encrypted and decrypted. Weare proposing a new algorithm for image encryption based on the Rubik cube principle. The theory of the Rubik cube is deployed first to scramble the pixels of the original Grey-scale image, which only changes the location of the pixels.The bitwise XOR is applied to odd rows and columns using two random secret keys, and then the bitwise XOR is also applied to even rows and columns using the flipped secret keys.These steps are repeatable while the number of iterations is not reached. The decrypted image appears in the blurred format that can give total security to the original image.

2. LITERATURE SURVEY:

A Survey of Image Encryption Algorithms
Data Encryption Standard (DES):

Data Encryption Standard (DES) is one among earliest block ciphers developed. Even though the processes for encryption and decryption include the number of rounds, the DES security mechanism is breakable by many ways. Brute force attack, known-plain text attacks and chosen plain text attacks are the most common approaches.

International Data Encryption Algorithm (IDEA):

The encryption and decryption structures are similar and use eight full rounds plus an additional half-round, making a total of 8.5 rounds. IDEA is vulnerable to various attacks like narrow-bicliques attack and man-in-the-middle attack.

Blowfish Algorithm:

Blowfish is a symmetric-key block cipher algorithm. Its main component is a Feistel network, iterating 16 times. Blowfish has small block size, lar4ger files are not recommended to be encrypted.

Advanced Encryption Standard (AES):

AES utilizes a substitution and permutation network structure, while the previously widely used DES was based on Feistel network. Different encryption and decryption processes uses similar byte substitution, shift row, mix column, and add round key steps. There are three different kinds of AES algorithm. These had an equal block size of 128-bit but had different key sizes of 128, 192, 256-bits signifying increase in security strength.With increase in bits AES gets vulnerable to full brute force attack.

Triple Data Encryption Standard (TDES):

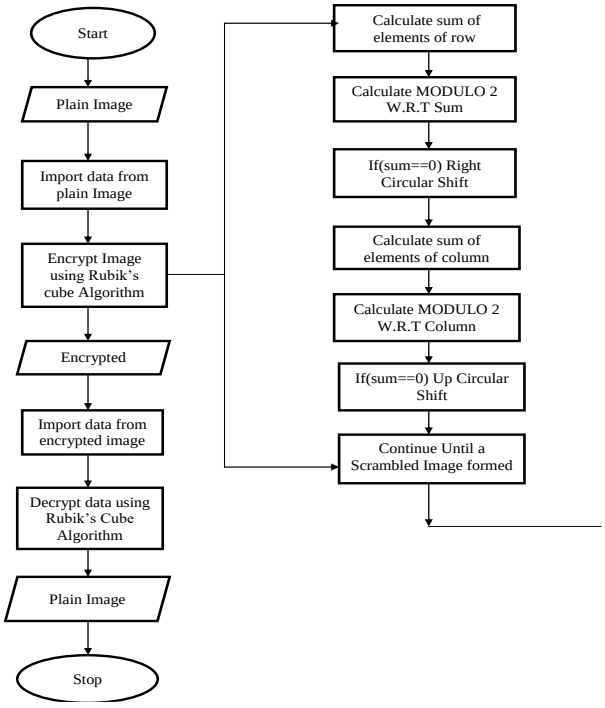
Triple Data Encryption Standard (TDES) is a symmetric-key block cipher. The algorithm uses the DES algorithm three times in encryption, decryption, and key generation processes. However, Triple DES is more secure than DES, but it is vulnerable to meet-in-the-middle attack and block collision attacks.

3. PROPOSED METHOD

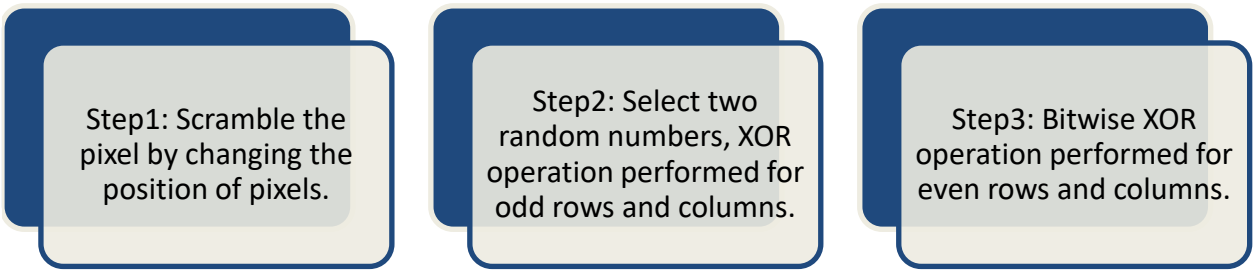
Rubik's Cube Principle

Rubik's cube principle is used to scramble the original image pixels. This method changes the position of the pixels. Here two random keys are used. Using these two secret keys, the circular shift is applied toall the rows and columns. To improve the security the steps can be repeated as many times required.

FLOW CHART:



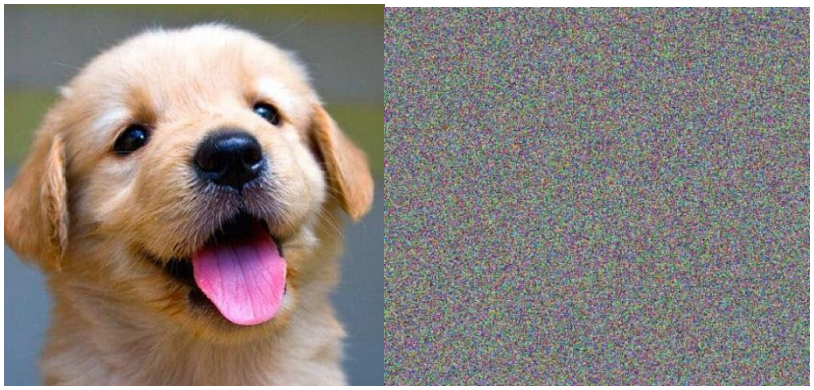
SCHEMATIC DIAGRAM:



4. EXPERIMENTAL ANALYSIS

By Rubik's cube principle for the image to be encrypted and decrypted. Weare presenting a novel image encryption algorithm that is based on the Rubik's cube principle.First the concept of Rubik's cube is applied to scramble all the pixels of the original Gray-scale image, which only changes the position of the pixels.Using two random hidden keys, the odd rows and columns are implemented with bitwise XOR.The bitwise XOR is then also extended using flipped hidden keys to even rows and columns. These steps should be repeated up to number of iterations based on security requirement.Here are the some of expected outputs of encrypted images:

(a)



Original colour image(512*512) Encrypted image using Rubik's cube

(b)

Original colour image(512*512) Encrypted image using Rubik's cube

5. FUTURE SCOPE

We are really enthusiastic about the vast future possibilities that our project has to offer. Possible improvements include encrypting and decrypting the videos both in black & white and color by extracting each frame and encrypting the images simultaneously. We know that all the images have sound. So, it can plan to encrypt frames and sound simultaneously. Finally, we can also create an app which can contain all of the above activities, with two people having the app; one will become the sender and other the receiver at a time, based on the requirement of either of two.

6. CONCLUSION

This algorithm is developed based on the principle of Rubik's cube to scramble image pixels. To confuse the relationship between encrypted and original images, a key is used to apply the XOR operator to odd rows and columns of the image.The same key is flipped and applied to the even rows and columns of image. It is also efficient for fast encryption and decryption which is appropriate for real-time Internet encryption and transmission application.

7. REFERENCES

[1] A Survey of Image Encryption Algorithms Manju Kumari ,Shailender Gupta , Pranshul Sardana 3D Research Center, Kwangwoon University and Springer-Verlag GmbH Germany, part of Springer Nature 2017.A new efficient and configurable image encryption structure for secure transmission

[2] Walid I. Khedr, Springer Science+Business Media, LLC, part of Springer Nature 2019.

[3] A Novel Hyperchaotic Image Encryption Scheme Based on DNA Encoding, Pixel-Level Scrambling and Bit-Level Scrambling, Shuliang Sun, IEEE

[4] Color Image Encryption for Secure Transfer over Internet: A survey Farzana Kabir , Jasmeet KaurInternational Research Journal of Engineering and Technology (IRJET).

[5] Secure sharing of outsourced data in cloud computing with comparison of different attribute based encryption schemes : A review",Vurukonda,N.&Thirumala Rao,Journal of Advanced Research in Dynamical and Control Systems,2017

[6] Super-Resolution Image Reconstruction Using Dual-Mode Complex Diffusion-Based Shock Filter and Singular Value Decomposition,Suryanarayana,G.&Dhulli ,R,Circuits, Systems, and Signal Processing,2017

[7] Shape Based image retrieval using lower order Zernike moments,Sucharitha,G.&Senapati, R.K,International Journal of Electrical and Computer Engineering,2017

[8] Reversible Image Watermarking technique using LCWT and DGT,Bennilo Fernades,J., Sivakannan,J,International Journal of Engineering and Technology(UAE),2018

[9] A Study on Wavelet transform using image analysis,Basha,C.Z.,Sricharan,K.M, International Journal of Engineering and Technology(UAE),2018

[10] Ultrafast Optical message encryption-decryption system using semiconductor optical amplifier based XOR logic gate,Agarwal,V.,&Pareek,P.,&Agarwal,M.,Proceedings of the International Conference on Numerical Simulation of Optoelectronic Devices,2018

[11] Identification of cervical spondysis disease on spinal cord mri image using convolutional neural network-long short-term memory(Cnn-lstm) technique, Ahammad,S.H., Rajesh,V., Indumathi,U.,&Charan,Journal of International Pharmaceutical Research,2019

[12] An adaptive noise removal framework for medical Images,Anusha,A.,&Vijayasaradhi,T., Journal of Computational and Theoretical Nanoscience,2019

[13] Achieving Confidentially and effective access Control of cloud data using cipher text policy based attribute based encryptionMane,P.M.,&Rani,C.M.S,Journal of Computational and Theoretical Nanoscience,2019

[14] Fusion of visible and infrared images via saliency detection using two-scale image decomposition, Naidu A.R., Bhavana D., Revanth P., Gopi G., Kishore M.P., Venkatesh K.S. International Journal of Speech Technology,2020

[15] Reversible Image Steganography Using Dual-Layer LSB Matching, Sahu A.K., Swain G., Sensing and Imaging,2020

[16] Cloud data search and verification using order preserving encryption, Shankar R., Janardhanarao S., Inthiyaz S., Shameem S., International Journal of Emerging Trends in Engineering Research,2020

[17] Recent advances in subsurface analysis with quadratic frequency modulated thermal wave Imaging,Subhani,S.,Suresh,B.,Journal of Theoretical and Applied Information Technology,2017

[18] Secure message exchange using text to image encoding,Barik,S.,Manikanta Sai,J.,Prasaannanjaneyulu Reddy,C., International Journal of Emerging Engineering,2018

[19] A multi keyword searchable attribute-based encryption technique for data access control in cloud storage, Mane P.M., Chetty M.S.R., International Journal of Advanced Trends in Computer Science and Engineering,2020