Diploma Student Project Synopsis

Department of Computer Science Engineering

Name of Students : 1.Mayur U

2.Jayanth N swamy

3.Mallikarjun

4.MadhuSudhan KV

Project Title *:* ***Image encryption***

Synopsis

BACKGROUND

Computer has become an essential device now a days. The main use of computer is to store data and send it from one location to other. The information that is shared must be transferred in a secured manner. To ensure secured transmission of information, data is encrypted to unreadable formats by an unauthorized person. Cryptography is the science of information security which has become a very critical aspect of modern computing systems towards secured data transmission and storage. The exchange of digital data in cryptography results in different algorithms that can be classified into two cryptographic mechanisms: symmetric key in which same key is used for encryption and decryption and asymmetric key in which different keys are used for encryption and decryption.

Images are broadly used in numerous processes. As a result, the safety of image data from unauthorized access is crucial at the hands of user. Image encryption plays a significant role in the field of information hiding. Image hiding or encryption methods and algorithms ranges from simple spatial domain methods to more complicated and reliable frequency domain. Image Encryption Using Rubik's Cube Based Algorithm is the process to transform the image securely so that no unauthorized user can be able to decrypt the image. Image encryption have applications in many fields including the internet communication, transmission, medical imaging etc.

First, in order to scramble the pixels of gray-scale original image, the principle of Rubik's cube is deployed which only changes the position of the pixels. Using two random secret keys, the bitwise XOR is applied into the rows and columns. These steps can be repeated until the number of iterations is not reached. Numerical simulation has been performed to test the validity and the security of the proposed encryption algorithm.

PROBLEM DEFINITION

Information Security is the most common word uttered by any man, any device or any peripheral since past two centuries. Protection from malicious sources has become a part of the invention or the discovery cycle. Myriad methods of protection are used ranging from a simple authentication password to most complex Cryptography. The advancements of digital revolution were not achieved without drawbacks such as illegal copying and distribution of digital multimedia documents. In order to provide data security and protection, different encryption methods must be used.

PURPOSE

This is the proposal for the design and development of software named as "Secure Image Encryption Using Algorithm Based On Rubik's Cube Principle". It applies special mathematical algorithm and keys to transform digital image into chiper code before they are transmitted and decrypts using application of mathematical algorithms and keys to get back the original data from the chiper code. The goal is to provide authentication of users and integrity, accuracy and safety of data resources.

OBJECTIVE

The main objective of our project is to provide security of the image-based data with the help of suitable key and protect the image from illegal copying and distribution

LITERATURE REVIEW

Evolution of Image Encryption and Decryption

First, we want to review the history of image encryption and decryption and how it came to be a subject of interest. Here, we have listed the significant encryption and decryption techniques used in each era and how they have changed throughout human history.

Historical Cryptography

The earliest known text containing cryptography came from Egypt in the form of hieroglyphics. These texts were dated to be as old as 4000 years old. Nobody knows why Egyptian used such encryptions but scientists assume it was done so as to show that they can write a language that is of higher level than common people or to make it look formal similar to modern day legal documents. In Greece, in about 500 B.C., Spartans used Scytale which was a device to send or receive secret messages. The device was a cylinder in which a narrow strip of parchment was wound and the message was written length-wise. Once it was unwound the strip was unreadable and could only be read with the help of a similar cylinder.2500 years ago not many people could read or write so this technique was quite effective but nowadays it could easily be deciphered. 2000 years ago, the earliest use of cryptography was seen and used by Julius Caesar. He devised a technique to send secret messages as at that time messengers were captured by enemies who could steal the message. But, Caesar would shift the texts by a specific number so that only the person who new the cipher code could decipher the texts, giving Julius Caesar a huge advantage against his enemies. In the 1400's, Leon Battista Alberti devised an encryption system using Cipher disk. This device allowed for many methods of substitution. In the 1500's, following the work of Alberti, Blaise De Vigenere created a cipher which came to be known as Vigenere Cipher. In the late 1700's, Thomas Jefferson devised a cipher system similar to the Vigenere cipher but with higher security. The encrypted message was present on the wheels and the ciphertext could have been any other plain text present in the wheel. Similar to Alberti, Jefferson never developed his encryption system. "During the early 1900's, the United States Army reinvented Jefferson's Wheel Cipher without any knowledge about Jefferson's invention. Jefferson was over a hundred years before his time.

Modern Cryptography

In the modern age of internet and technology data security is a huge field and an equally immense challenge as highly sensitive data are stored in the digital realm. Personal info such as bank information, social media accounts, etc. all are in threat from phishing, pharming and spyware. To counteract such threats many ingenious techniques have been developed including image encryption.

Some of the previous image encryption methods developed include chaotic systems, pixel position permutation and value transformation. Huang, C.K., Nien, H.H proposed a novel pixel shuffling method which used chaotic systems to generate chaotic sequences as encryption codes . Chen, G., Mao, Y., Chui, C.K. generalize a two-dimensional cat map to a 3D one for a real-time secure symmetric scheme . Guo et al. proposed a colour image encryption method using discrete fractional random transforms and Arnold transform in which DFRNT encrypts the intensity component while AT encrypts hue and saturation components . Zhu et al. proposed a permutation method to confuse and diffuse the grey-scale image at the bit level, which changes the position of the pixel and modifies its value also using the Arnold cat map to permute the bits and the logistic map to further encrypt the permuted image. Wang, Y., Wong, K.-W., Liao, X., Chen, G. in their research paper proposed image encryption algorithm combining permutation and diffusion where the original image is partitioned into blocks and then spatiotemporal chaos is applied to shuffle the block and generate pseudorandom sequence .

FUNCTIONAL REQUIREMENTS

Our system of Image Encryption application functional requires

- The application is able to ask user to input keys ‘kr’ and ‘kc’ for decryption process to take place.
- The application is able to send the keys through email provided by users after encryption.
- The process of both encryption and decryption is incredibly fast.
- The image file size is not significantly affected to prevent doubt for unauthorized user.
- The image is transmitted according to user preference safely after being encrypted.

SOFTWARE REQUIREMENTS

Here we specify the types of software that is used within the system.

1 Photoshop

2 Python 3.7

3 SQLite

4 Atom IDE

5 Microsoft Windows 10 OS

Conclusion:

This project can help to Encrypt and Decrypt images and videos in a video call or text messages.