IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Vol. 10, Issue 4, April 2023

DOI: 10.17148/IARJSET.2023.10420

IMAGE SECURITY ENHANCEMENT USING CRYPTOGRAPHY

Chaitanya Shivaraju[1], Deepa G[2], Deepthi N K[3], Mythreyi U[4],

Prof. Manoj Kumar S[5]

Student, Computer Science and Engineering, K. S. Institute of Technology, Bangalore, India[1-4]

Assistant Professor, Computer Science and Engineering, K. S. Institute of Technology, Bangalore, India[5]

Abstract: In the recent years, the trends in technology have come up with a solution to share digital media in an easier and rapid manner which leads to the use of media in an illegitimate manner. In order to make this problem less severe, various cryptographic techniques can be used to secure the digital media by encrypting them. The following article presents a technique that enables the implementation of image security through the combination of different techniques namely Chaos based encryption and XOR based encryption and decryption.

Keywords: Cryptography, XOR based encryption and decryption, Chaos encryption, image security.

I. INTRODUCTION

This project aims at creating a web application for Encrypting the images at the sender side and sending that to the receiver who then decrypts it using the same application. Nowadays hackers and other intruders tend to snoop over the images which are sent online and try to manipulate them or misuse them. This causes insecurity for the personal or private images that are being shared.

The best solution that can be provided is by using the various techniques and algorithms for the Encryption and Decryption of the images . Cryptography is the action and study of algorithms and different techniques that ensure secure communication in the existence of adversarial behaviour. Cryptography is generally all about assembling and analysing entente that prevent any unauthorised or anonymous people viewing the private images and text. Only the sender who is sending the image and the receiver i.e. to whom the message is sent will be able to view the image .This prevents any unauthorised users to view these images.

There are three types of Cryptography namely symmetric key algorithm, asymmetric key algorithm, hash functions.

A. Symmetric-key algorithms

Uses single key for Encryption and Decryption of images Both these processes use the same key. It is one of the easiest type of Cryptography.

Examples:

1. Advanced Encryption Standard
2. Data encryption standard
3. Caesar Cipher

B. Asymmetric-key algorithms

Uses two keys for the encryption and Decryption. The keys are one private key and other is public key. If public key is used for Encryption then private key has to be used for Decryption or vice versa. The private key must not be shared between the sender and the receiver .Public key can be derived from private key.

Examples:

1. Elliptical Curve Cryptography
2. Diffie-Hellman
3. Digital Signature Standards

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Vol. 10, Issue 4, April 2023

DOI: 10.17148/IARJSET.2023.10420

C. Hash functions

It is a method of transforming the string into stabled length string. It protects the data or image in such a way that the original image cannot be recovered. It is irreversible and one way.

Examples:

1. MD5 [Message digest Algorithm-5]
2. SHA-1
3. Whirlpool
4.

In Cryptography after the Encryption takes place the original image will be transformed to cipher image by applying the encryption techniques and algorithms and the cipher image will be transformed into original image after the decryption using the same techniques and algorithms..

II. RELATED WORK

A. "Image Encryption using Block Permutation and XOR Operation"

This paragraph describes a proposed method for encrypting images using a combination of permutation and XOR operations. The original grayscale image is first divided into blocks of size NxN. Random numbers are generated using a random function to permute the pixels in each block, which are then merged to create a single image. Another set of random numbers is generated using LFG (Linear Feedback Shift Register), and these are XORed with the pixel values of the shuffled image to produce the encrypted image.

The original image and the Random numbers are put as an input to the system where the division into the blocks are formed due to division and further these blocks are shuffled and then the resulting Scrambled image is obtained which undergoes the XOR operation with lagged Fibonacci generator.

B. "Image Encryption Using Random Scrambling and XOR Operation".

This paper uses the algorithm which describes the process of encrypting an image before transmitting it to another end. The input is a grey scale image of a certain size and bit depth. The image is then decomposed into bit-plane images, which represent each pixel's binary value. For each bit-plane image, a 1-dimensional vector is created to simplify the encryption process. This transformation of the image into vectors allows for the application of various encryption techniques. The output is the encrypted image, which will be transmitted to the receiver securely.

Coming to the decryption of the respective cipher image the encryption using the XOR operation then the decomposition into 1bit plane images is done. The transformation of the bit plane image X into a 1-D vector V. Anti-scrambles the 1-D vector and the merge the anti-scrambled bit plane images according to their original level is taken place the obtain the original image X id being obtained.

C. "A novel image encryption scheme based on hyper-chaotic system and DNA sequence operation" .

The proposed encryption scheme uses a hyper-chaotic system to generate the pseudo-random sequence and a DNA sequence operation to perform the encryption. The scheme is based on three stages: (1) hyper-chaotic sequence generation, (2) DNA sequence operation, and (3) diffusion and confusion process. In the first stage, a 4D hyper-chaotic system is utilized to generate the pseudo-random sequence. In the second stage, a DNA sequence operation is employed to permute the positions of the pixels in the image. In the third stage, a diffusion and confusion process is applied to the permuted image to further enhance the security.

D. "A New Image Encryption Scheme Based on Chaotic Maps and Lifting Wavelet Transform"

The proposed encryption scheme uses chaotic maps and lifting wavelet transform to provide the randomness required for the encryption. The scheme consists of two stages: (1) chaotic map-based permutation and (2) lifting wavelet transform-based diffusion. In the first stage, a chaotic map is used to permute the positions of the pixels in the image. In the second stage, a lifting wavelet transform is applied to the permuted image to diffuse the information. The scheme uses two chaotic maps to provide the randomness required for the encryption. The security of the scheme is evaluated using various statistical tests.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Vol. 10, Issue 4, April 2023

DOI: 10.17148/IARJSET.2023.10420

III. PROPOSED SYSTEM

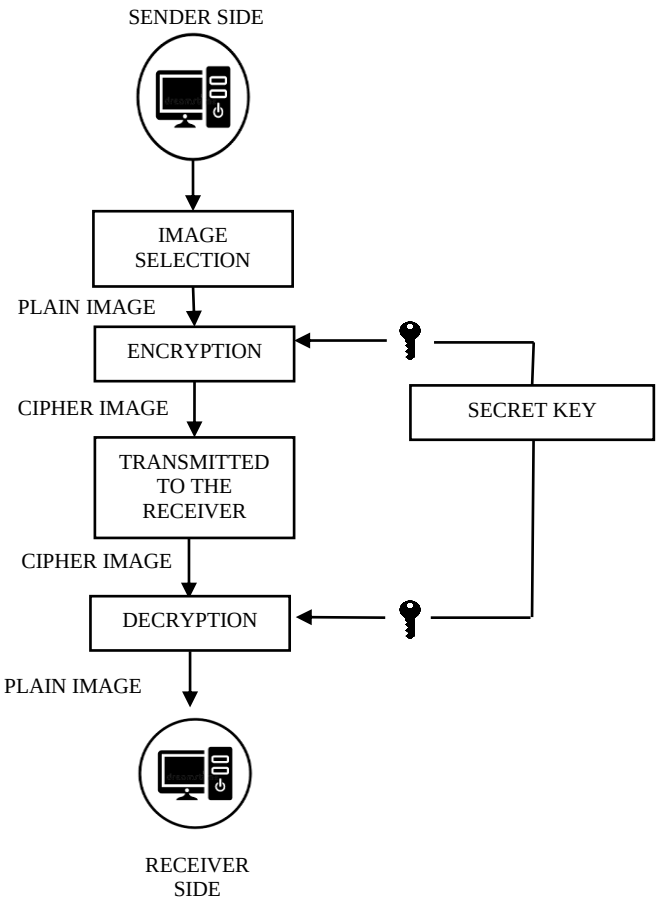

Fig. 1 Proposed System

The methodology (Fig 1 and 2) given shows the flow of how our project actually works .This project aims at creating a web application for Encrypting the images at the sender side and sending that to the receiver who then decrypts it using the same application. The sender selects the image to be encrypted and the sender can encrypt images of different format.

IV. IMPLEMENTATION

The image that is to be transmitted is selected by the user and who then uploads it into the web application.The first stage of encryption takes place.A random key is generated as a symmetric secret key. This stage then converts the image into byte array and each pixel obtained after conversion is XORed with the symmetric key.

The encrypted image obtained is passed to the second round of encryption which is performed using the chaos technique. With the chaos technique the pixels of the image is decomposed and decorrelated to generate the cipher image. This cipher image is transmitted to the intended receiver who then uses the same web application to retrieve the original image

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Vol. 10, Issue 4, April 2023

DOI: 10.17148/IARJSET.2023.10420

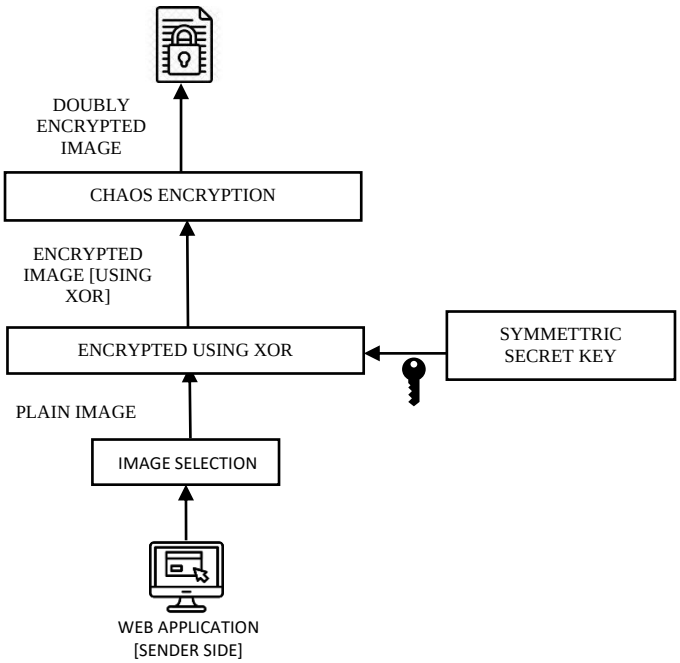

Fig.2 Encryption Process

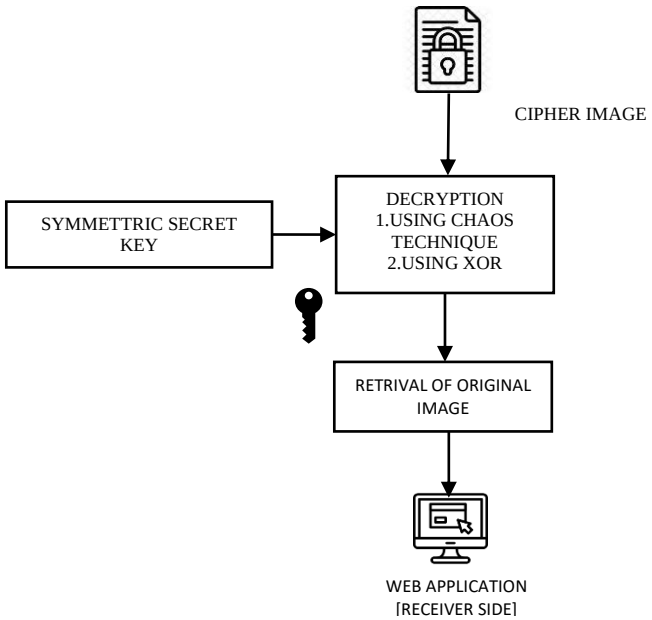

Fig. 3 Decryption Process

During the decryption process the user uploads the encrypted image along with the symmetric key. Upon providing the correct key with the decrypted image , the original image is first decrypted using the chaos technique and later decrypted using the XOR technique to retrieve the original image. If an incorrect key is provided with the encrypted image the image , the user will not be able to retrieve the original image.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Vol. 10, Issue 4, April 2023

DOI: 10.17148/IARJSET.2023.10420

V. RESULTS

After successful encryption of the image , the encrypted image is returned along with a secret key . The cipher image that is generated can be transferred to the intended user via any platform. Now the receiver uses the same website to upload the cipher image that the sender sends along with the key to obtain the original image.

The result of the implementation is as follows

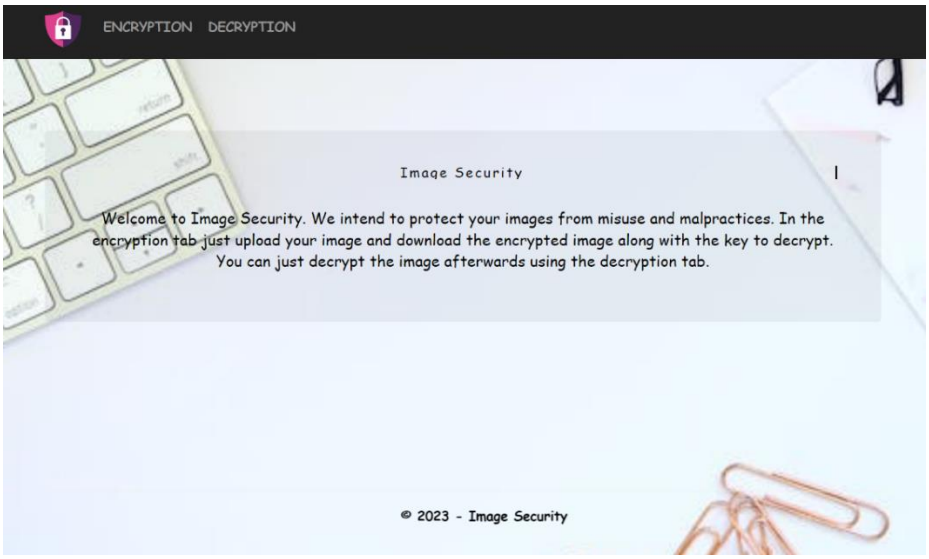

Fig. 4 Home page

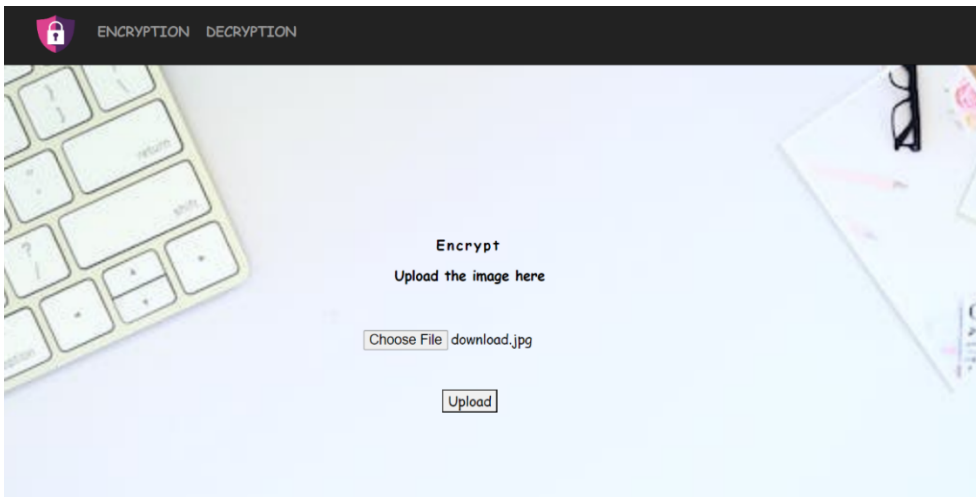

Fig. 5 Encryption

Fig. 6 Original image that is to be encrypted

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Vol. 10, Issue 4, April 2023

DOI: 10.17148/IARJSET.2023.10420

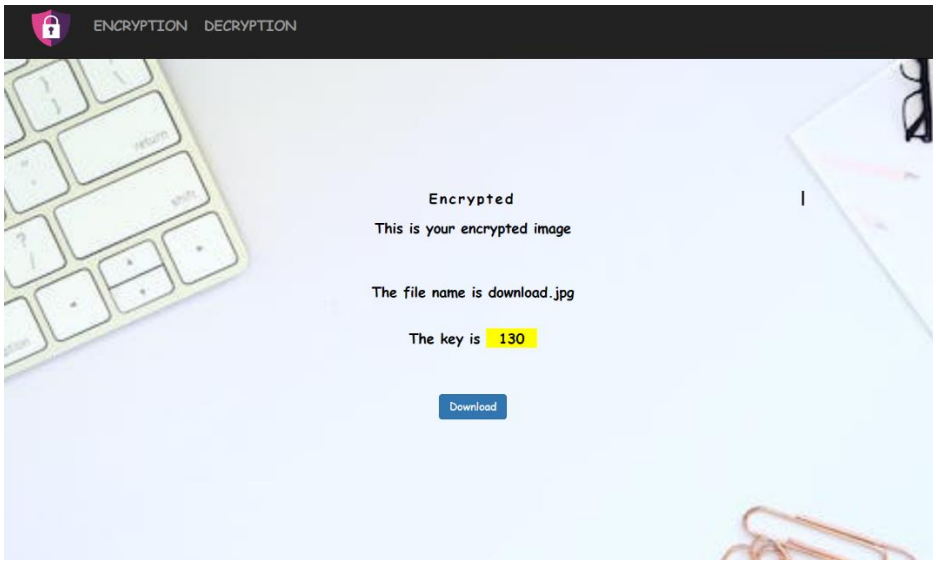

Fig. 7 Encrypted image and secret key generation

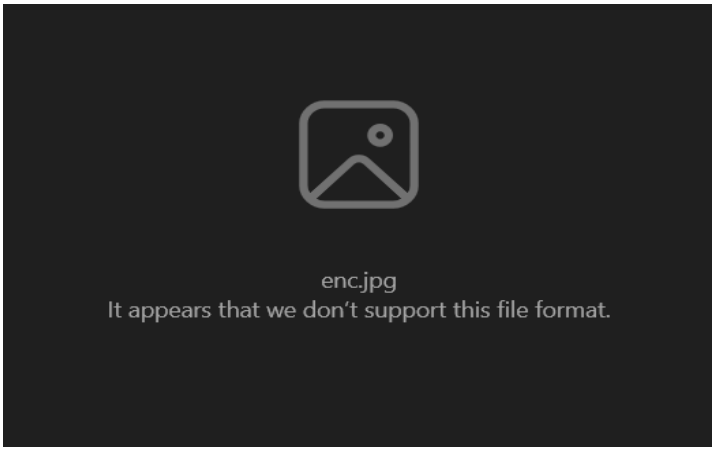

Fig. 8 Encrypted image

Fig. 9 Decryption

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Vol. 10, Issue 4, April 2023

DOI: 10.17148/IARJSET.2023.10420

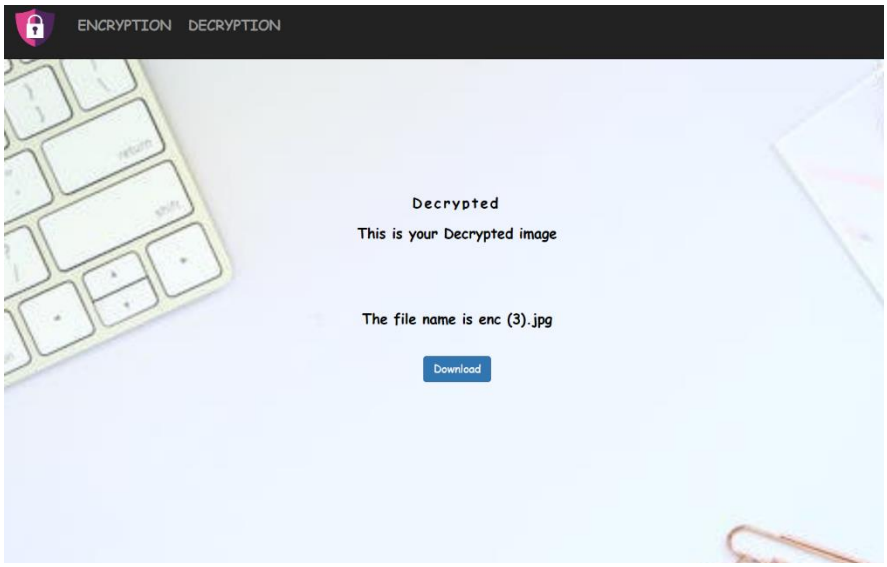

Fig. 10 Retrieval of original image upon providing the correct key with the encrypted image.

Fig. 11 Decrypted image upon providing correct key

VI. CONCLUSION

Any images including the scanned copies, have grown in importance as a means of information transmission and storage in the internet. The major concern is to provide high security and safe transmission over the internet . Due to their simplicity and convenience, digital picture have emerged as the crucial data transmission formats in the network. As a result, everyone has given the security protection of digital photos a lot of thought. Particularly against the backdrop of the recent deterioration in network security, information sharing and transmission based on digital images frequently encounter issues such as misuse of the data being shared. By using our application the above mentioned issues can be resolved.

The project “Image security enhancement using cryptography” provides security for the image by encrypting it using the techniques like double random phase technique, chaos method and XOR method . These algorithms provide security and multiple barriers for unauthorized users. A key is generated during the XOR operation which increases the security for these images as the hackers trying to decrypt the image using the wrong key cannot obtain the original image which was encrypted. Symmetric key is used for encryption and decryption. The advantage of using a symmetric key is that it is faster to decrypt the image compared to an asymmetric key.

ACKNOWLEDGEMENT

We cordially thank **Prof**. **MANOJ KUMAR S** for his valuable, constructive suggestions and constant support during the planning and development of the project. His willingness to give his time so generously has been very much appreciated. We would also like to thank all the professors of KSIT for their continuous support and encouragement.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Vol. 10, Issue 4, April 2023

DOI: 10.17148/IARJSET.2023.10420

REFERENCES

[1]. Nagham Hamid, Abid Yahya, R. Badlishah Ahmad & Osamah M. Al-Qershi, “Image Steganography Techniques: An Overview” In International Journal of Computer Science and Security (IJCSS), Volume (6) , Issue (3) , 2012.

[2]. Munesh Kumar, Gaurav Yadav, Ashish Kumar Keshari, Sandhya Katiyar , ”Image Processing using Steganography” in International Journal of Engineering Science and Computing, April 2017.

[3]. Unsub Zia, Mark McCartney, Bryan Scotney, Jorge Martinez, Mamun AbuTair, Jamshed Memon, Ali Sajjad,” Survey on image encryption techniques using chaotic maps in spatial,transform and spatiotemporal domains” in International Journal of Information Security (2022).

[4]. Hailan Pan, Yongmei Lei and Chen Jian ,“Research on digital image encryption algorithm based on double logistic chaotic map” EURASIP Journal on Image and Video Processing volume 2018 , Article number : 142 (2018).

[5]. Kazuya Nakano , Hiroyuki Suzuki, “Analysis of single phase based on double random phase encoding using phase retrival algorithm”, 2020.

[6]. Gaurav Kumar Soni, Himanshu Arora and Bhavesh Jain, "A Novel Image Encryption Technique Using Arnold Transform and Asymmetric RSA Algorithm", In. Springer International Conference on Artificial Intelligence: Advances and Applications 2019, Algorithm for Intelligence System, 89-90 (2020) BIOGRAPHIES .