IMAGE SECURITY ENHANCEMENT USING CRYPTOGRAPHY

Chaitanya Shivaraju[1], Deepa G[2], Deepthi N K[3] , Mythreyi U[4],Prof. Manoj Kumar S[5]

[1] Chaitanya Shivaraju, Computer Science and Engineering, K.S. Institute of Technology, Bangalore, India
[2] Deepa G, Computer Science and Engineering, K.S. Institute of Technology, Bangalore, India
[3] Deepthi N K, Computer Science and Engineering, K.S. Institute of Technology, Bangalore, India
[4] Mythreyi U, Computer Science and Engineering, K.S. Institute of Technology, Bangalore, India
[5] Prof. Manoj Kumar S, Computer Science and Engineering, K.S. Institute of Technology, Bangalore, India

---***---

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 three different techniques namely Double random phase encoding, Chaos based encryption and steganography methods.

***Key Words*:** Cryptography, Double Random Phase, Steganography, Chaos encryption, image security.

1. 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.

1.1 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:

- Advanced Encryption Standard
- Data encryption standard
- Caesar Cipher

1.2 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:

- Elliptical Curve Cryptography
- Diffie-Hellman
- Digital Signature Standards

1.3 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:

- MD5 [Message digest Algorithm-5]
- SHA-1
- Whirlpool

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.

2. RELATED WORK

2.1 Based on Steganography technique

Steganography is a security technique that is used to conceal data inside cover media so that the secret data placed cannot be seen. Images, sounds, or videos can be used as the cover object. The steganography term is extracted from Greek word “covered writing”. They are famous for being a non-causal medium because it is possible to access any random image pixel. Additionally, the concealed data can continue to be unnoticeable to the naked eye. However, the methods of image steganography will take advantage of "gaps" in the Human Visual System (HVS)[1].

There are several techniques to conceal information or transmit it in a private way through different means. In the fifth century BCE, King Darius imprisoned the dictator Histiaeus in Susa. Histiaeus sent an ambiguous message to his son-in-law Aristagoras, who was at Miletus, by shaving a slave's head and tattooing the word on his scalp. When the slave's hair had

grown long enough to cover the tattoo, he was sent to Miletus with the message. [1]
In order to translate Arabic manuscripts on secret writing into English, which are supposed to have been penned around 1200 years ago, a project has been launched in Saudi Arabia. These manuscripts have been found in Germany and Turkey, among other places. [2]

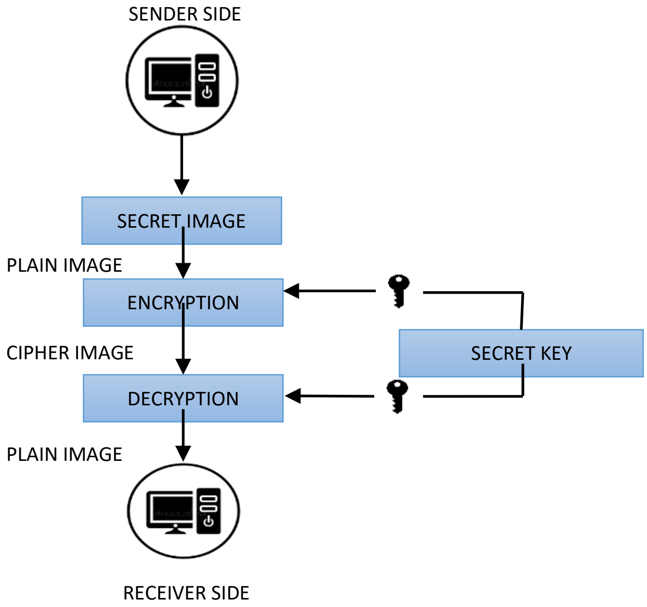
2.2 Based on chaos technique

Cryptography is described as a balanced fusion of the science of cryptography and chaos theory. Present the data bits of the message to be valid are arbitrarily ordered, and the picture's pixel bits are also made attractive, making the example challenging to comprehend.[3]
Five chaos-based algorithms and ten common photo encryption methods have each been looked at. To evaluate them, various assessment measures, such as statistical, differential, and quantitative attack analysis, were used. MATLAB 2015 was used to conduct the experiments and assess their effectiveness. The results demonstrated that statistical assaults could not be used against chaotic methods. Monjul Saika et al. gave a brief summary of chaotic map-based picture encryption in the spatial domain. The authors argued that chaos-based picture encryption is perfectly suited for encryption procedures because of their great sensitivity to beginning conditions. [4]
In order to encrypt and protect digital images, American researcher Fridrich suggested a chaotic encryption technology and technique based on two-dimensional Baker mapping. It is the first chaotic encryption method to be used and implemented in the context of digital image encryption.[5]

2.3 Based on Double Random phase technique

Numerous studies have been done on optical cryptosystems, which have advantages over discrete mathematics-based cryptography . For instance, when obtaining the image of the object, optical encryption techniques might encrypt the information of the object. Furthermore, ultrahigh-speed parallel processing can be used for optical encryption. A basic and straightforward optical cryptosystem is double random phase encoding (DRPE) . It has been expanded to include a variety of kinds, including phase-only DRPE , fractional DRPE, Fresnel DRPE , colour image DRPE , extended model of DRPE and incoherent DRPE. A symmetric-key cryptography method is DRPE. Two random phase detectors and a 4-f correlator are part of the optical setup for the DRPE. It masks, specifically one in each of the Fourier and spatial planes. As the system's symmetric key picture, the mask in the Fourier plane is employed. The phase key images of DRPE include some redundancy between encryption and decryption, whereas the symmetric key used in cryptography is one-of-a-kind. Even if the DRPE key contains some incorrect phase values, it is still possible to retrieve the plaintext pattern with tolerable noise. Multiple keys can therefore obtain a plaintext pattern in DRPE. It is crucial to understand the proportion of these keys to all key patterns QNN, which are defined by the phase quantization level, Q, and the image size, NxN pixels. The phase key image's characteristics have been examined in earlier works . Small images and few phase quantization levels were used in studies based on key-space analysis to examine the attributes of all phase keys . Additionally, a statistical method was used to examine the characteristics of big phase key images .[6].

3. PROPOSED SYSTEM



3.1 Proposed System

The methodology (Fig 3.1) 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. The sender can set a time limit within which the receiver have to decrypt the image. The receiver on opening the application within the time limit can decrypt the image. If the receiver doesn't not decrypt the image within the time limit the image will be discarded.

4. CONCLUSIONS

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.

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.

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] C Pradhan,V Saxena,A K Bisoi,”Non-Blind Digital Watermarking Technique using OCT and Cross Chaos Map”, International Conference on Communication,Device and Intelligent Systems IEEE,2018,pp.282-285.

[4] 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)

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

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

[7]] H. Yang, Q. Zhou, M. Yao, R. Lu, H. Li, and X. Zhang, “A practical and compatible cryptographic solution to ADS-B security,” IEEE Internet Things J. 6(2), 3322–3334 (2019).
[8] R. Ranjith Kumar,S. Jayasudha & S. Pradeep “Efficient and secure data hiding in encrypted images: A new approach using chaos” Published online: 15 Nov 2016

[9] Dr. Himanshu Arora, Mr. Manish Kumar and Mr. Sanjay Tiwari, "Improve Image Security in Combination Method of LSB Stenography and RSA Encryption Algorithm", International Journal of Advanced Science and Technology, Vol-29, No-8, 6167-6177, (2020).

[10] 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 (Optional not mandatory)