I-Share: A secure way to share images

Madhura Shahasane[1], Sarita Yadav[2]

[1,2] Pillai HOC College of Engineering & Technology, Rasayani

---***---

Abstract - *Nowadays, information security is becoming more important in data storage and transmission. In the ever-shifting landscape of cyber threats and attacks, sharing images over the network becomes insecure. For this, various techniques were applied in order to encrypt and decrypt the images. An image encryption method makes information unreadable. As a result no attacker or eavesdropper, including server administrator and others cannot have access to original data or any other type of transmitted information through network, such as Internet. The objective of this project is to propose a real time image encryption standard using Quick Response (QR) code in an Android framework .The QR code acts as a smart container and keeps the speckle noise far away from the image. The QR code based noise-free optical encryption scheme can be combined with optical information authentication to obtain enhanced security level.*

Key Words: **Decryption, DRPE, Encryption, QR code, Speckle noise**

1. INTRODUCTION

Nothing is completely secure. Locks can be picked, safes can be broken into, and online passwords can be guessed sooner or late. Modern security is battling between high security and low friction. Security plays a vital role to secure data or the information that's deals with user's personal bank account. Due to rapid development of internet and wide use of multimedia the digital information can be communicated among various people. Security provided to images like blue print of company projects, secret images of concern to the army or of company's interest, using image encryption is beneficial. The need for security of information is increasing due to threats and attacks from attackers and intruders. To overcome these threats, we need new security method Optics field has revolutionized the defence, medical and broadcasting system.

Optical technologies have been widely explored to encrypt sensitive information. One major advantage of optical processing is the speed of processing large amounts of information. In addition, optical security can employ numerous parameters for encryption including wavelength, phase information, spatial frequency or polarization of light. In the encryption and decryption protocol we prefer Double Random Phase Encoding due to its common knowledge among the researchers in the field. QR Code (from Quick Response Code) is the trademark for a two-dimensional code first designed for vehicle industry. QR code is most popular due to its stability and readability. The code consists of black square dots arranged in a specific square pattern on a white background. The QR code contain the data that can be numeric, alphanumeric, byte/binary, etc. or through supported extensions, virtually any kind of data. In japan 1994 Denso Wave invented the QR code to track vehicles during vehicle manufacturing process. It has since become one of the most popular types of two-dimensional barcodes.

2. LITERATURE SURVEY

Image is also an important part of information. Therefore it is very important to protect image from unauthorized access. There are so many algorithms available to protect image from unauthorized access which is described below:

Image Encryption Using Affine Transform and XOR Operation: It's a two phase encryption and decryption algorithms that is based on rearranging the image pixels using affine transform and encrypting the resulting image using XOR operation. Redistribute the pixel values to different location using affine transform technique with four 8-bit keys. The transformed image then divided into 2 x 2 pixels blocks and each block is encrypted using XOR operation by four 8-bit keys [3]. The total key size used in algorithm is 64 bit. Amitava Nag results proved that after the affine transform the relations between pixel values was significantly decreased.

Image Encryption and Decryption Using Blowfish Algorithm in Matlab*:* Encryption and decryption of images using a secret-key block cipher called 64-bits Blowfish [6] is considered to increase security and to improve performance. This algorithm is used as a variable key size up to 448 bits. It employs Feistel network which iterates simple function 16 times. The blowfish algorithm is safe against unauthorized attack and runs faster than the popular accessible algorithms. The proposed algorithm is designed and realized using MATLAB. Hence if the number of rounds is increased then the blowfish algorithm becomes stronger. Since Blowfish does not have any known security weak points so far it can be considered as an excellent standard encryption algorithm.

Optical encryption using double random phasing encoding:

The double-random-phase encryption (DRPE) [11] is a very popular optical encryption method due to its simplicity. Moreover, it is robust against many different attacks in practical use such as the brute-force attack and chosen plain-text attacks by simply updating the encryption keys.

3. EXISTING SYSTEM

DRPE System

- The universal use of multimedia and communication system have risk of various cyber-attacks and there on and the resulting theft of private data from secured systems have led to the śdemand for ever improving security techniques

- Technique such as steganography and watermarking have been proposed in which data is hidden and the other hand, data can be encrypted making it difficult to access without some key.

- Often both processes hiding and encryption is been employed in the system. Among these a technique is Double Random Phase Encryption using optical processor.

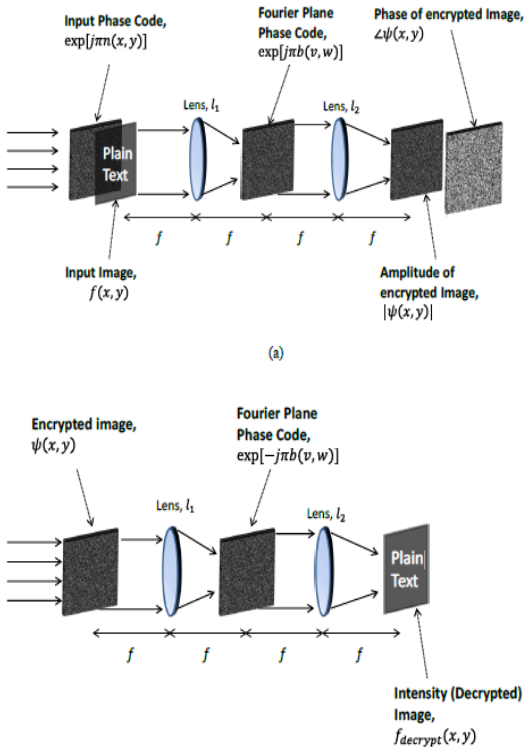

Fig: Double Random phase encoding process

- The DRPE turns an intensity image into an unreadable format by using two randomly distributed phase keys that are employed at spatial and Fourier domains respectively. The resulting encrypted data is complex and it cannot be decoded easily without decrypted it using the correct phase keys.

- In addition to this there are various extensions to DRPE such in Fresnel domain, the Hartley transform. Since the conventional encryption techniques has shown to be vulnerable for phase retrieval based attacks such as Chosen Cipher text attacks (CCA), Cipher text only attacks and Known plaintext attack.

4. PROPOSED SYSTEM

This paper tends to the security issue of giving a crucial picture encryption instrument for execution of a safe correspondence framework a correspondence foundation that can give a solid picture security over people in general system. The problem in encrypting the images with the optical encryption method DRPE is that it is vulnerable to the cipher text attack and known plaintext attack and also the speckle noise is added in the original image data while encryption.

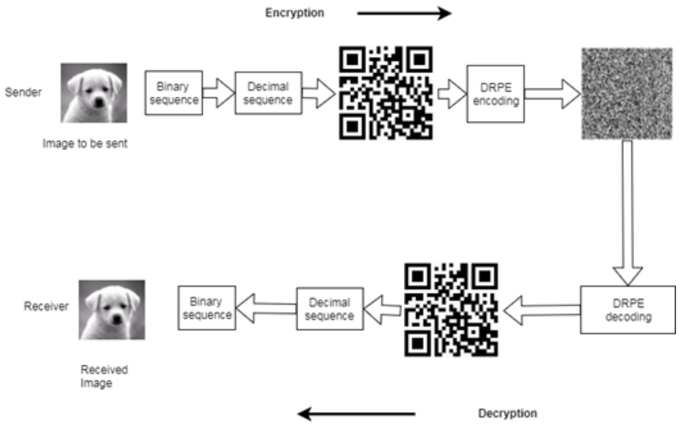

Fig. Flow of proposed algorithm

What is QR code?

QR code stands for quick response code which is the type of matrix barcode.it has number of features like large capacity data encoding, digit and dirt resistant, 360 degree reading and flexibility of an application. The QR code technology rapidly came to popularity due to its use in smartphone. The text, images, URL can be stored in the form of QR code

'I-share'-secure way to share images is an android based application that has been designed using many models and different algorithms. The system aims at secure transfer of image data over a public network such as an internet. To design the system for encrypting images following steps are required:

1. The binary data in either a BMP file or a JPEG file can be directly read out and cascaded as a single long binary number sequence.

2. In the next step, the binary number sequence is converted to be a decimal integer sequence. The rule is as follows. First, decimal number 0–7 is corresponding to a three-digit binary sequence, for example, 0 corresponds to "000" and 7 corresponds to "111". Decimal number 8 and 9 corresponds to four-digit binary sequence "1000" and "1001".

3. There is a maximum data storage limit for one single QR code, depending on the QR code version (code size). For

example, a version 1 QR code (size: 21×21 dots) with low level error correction can store at most 41 decimal integer numbers.

4. As a result, it is necessary to cut the decimal sequence into a number of segments and each segment is employed to generate an individual QR code. The gray scale image is therefore represented by multiple QR codes. As stated above, the generation of QR codes are under numeric mode.

The generated QR codes will go through optical encryption/decryption procedures. When the decrypted QR codes are obtained, they can be read by any conventional QR code reader and the integer sequence can be retrieved from each code. Multiple integer sequences can be assembled into one integer sequence, which will be later transformed into a binary sequence based on an opposite way of the rules stated in step 2. Finally, the binary sequence is converted back to an image file representing the final decrypted image.

5. CONCLUSIONS

In this sense, we believe this novel application merging the QR code to the optical encryption revitalizes the traditional optical encrypting methods. According to our criterion, technique represents an advance in presenting a practical tool, which can be massively used, and solving the drastically issue of the ever present speckle noise altering the outcome.

Future work may include various types of encryption and security strategies, storing various parts of encrypted and data followed by compression in the QR code.

REFERENCES

[1] W. Chen, X. Chen, Space-based optical image encryption, Opt. Express 18 (26)(2010) 27095–27104.

[2] G. Situ, J. Zhang, Double random-phase encoding in the Fresnel domain, Opt. Lett.29 (14) (2004) 1584–1586.

[3] X. Wang, W. Chen, X. Chen, Optical information authentication using compressed double-random-phase-encoded images and quick-response codes, Opt. Express 23(5) (2015) 6239–6253.

[4] X. Peng, P. Zhang, H. Wei, B. Yu, Known-plaintext attack on optical encryption based on double random phase keys, Opt. Lett. 31 (8) (2016) 1044–1046.

[5] L. Chen, D. Zhao, Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms, Opt. Express 14 (19) (2006) 8552–8560.

[6] Amitava Nag et al (2011)”Image Encryption Using Affine Transform and XOR Operation”, International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN).

[7] Pia Singh et al (July-2013) "Image Encryption and Decryption Using Blowfish Algorithm in Matlab," International Journal of Scientific & Engineering Research, vol. 4, Issue. 7.

[8] Liang Zhao et al (2012) “On the security analysis of an image scrambling encryption of pixel bit and its improved scheme based on self-correlation encryption”, Communications in Nonlinear Science and Numerical Simulation, Vol. 17, No. 8, pp3303-3327.