Hide and Seek: A New Way to Hide Encrypted Data in QR Code Using the Concepts Steganography and Cryptography

M. Manimekalai[1], R. Bakkiyalakshmi[2]

Professor Director and Head, PG Department of Computer Applications, Shrimati Indra Gandhi College, Trichy, India [1]

Research Scholar, Department of Computer Science, Shrimati Indra Gandhi College, Trichy, India [2]

Abstract: The art of information hiding has become an important issue in the recent years as security of information has become a big concern in this internet era. Cryptography and Steganography play major role for secured data transfer. Steganography stands for concealed writing; it hides the message inside a cover medium. Cryptography conceals the content of a message by encryption. QR (Quick Response) Codes are 2-dimensional bar codes that encode text strings. They are able to encode information in both vertical and horizontal direction, thus able to encode more information. Genetic Algorithm basic function is to be used to generate the key values that can be used to encrypt the message so the detection of the message is complicated. In this paper a novel approach is proposed for secret communication by combining the concepts of Steganography and QR codes. The suggested method includes two phases: (i) encrypt the message by using the key values that is generated using genetic algorithm (ii) Hiding the encrypted message inside the QR code. Experimental result shows that the enhanced design of secure algorithm can be created which ensure improved security and reliability.

Keywords: QR, Cryptography, Steganography, Genetic Algorithm, Encode.

I. INTRODUCTION

Cryptography and Steganography are well known and widely used techniques that manipulate information in order to cipher or hide their existence respectively. Steganography is the art and science of communicating in a way which hides the existence of the communication. Cryptography scrambles a message so it cannot be understood; the Steganography hides the message so it cannot be seen. Even though both methods provide security, a study is made to combine both cryptography and Steganography methods into one system for better confidentiality and security.

Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and the receiver have, and public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses. In Cryptography, a cipher message for instance, might arouse suspicion on the part of the recipient while an invisible message created with steganographic methods will not. In fact, steganography can be useful when the use of cryptography is forbidden: where cryptography and strong encryption are outlawed, steganography can circumvent such policies to pass message covertly. However, steganography and cryptography differ in the way they are evaluated: steganography fails when the "enemy" is able to access the content of the cipher message, while cryptography fails when the "enemy" detects that there is a secret message present in the steganographic medium. The disciplines that study techniques for deciphering cipher messages and detecting hide messages are called cryptanalysis and steganalysis. The former denotes the set of methods for obtaining the meaning of encrypted information, while the latter is the art of discovering covert messages. The aim of this paper is to describe a method for integrating together cryptography and steganography through some media such as image, audio, video, etc. Data hiding in a generated QR code image which is hided in a cover image using LSB technique. So, the process is the identification of the secret message hided in the input cover image. The secret message will be transferred from sender to receiver where they access it. The secret message could be in the form of text data. Here, the work is to embed QR code in color image by using data transmission and reception process. Hiding of information techniques would be continually introduced. Also the degrees of complexity are increased. Thus the future malware related traffic could be harder to detect.

II. RELATED WORK

[1] Mrs. G. Prema, S. Natarajan, "Steganography using genetic Algorithm along with visual Cryptography for Wireless Network Application", The proposed system provides the best approach for Least Significant Bit (LSB) based steganography using Genetic Algorithm (GA) along with Visual Cryptography (VC). Original message is converted

into cipher text by using secret key and then hidden into the LSB of original image. Genetic Algorithm and Visual Cryptography has been used for enhancing the security. [2] Fridrich J., Goljan M. And Du R, "Reliable Detection of LSB Steganography in Color and Grayscale Images", In this paper, we describe a new very accurate and reliable method that can detect LSB embedding in randomly scattered pixels in both 24-bit color images and 8-bit grayscale or color images. It is based on our previous work on lossless data embedding [3] J. Fridrich, M. Goljan and D. Hogea, "Steganalysis of jpeg images: Breaking the f5 algorithm", In this paper, we present a steganalytic method that can reliably detect messages (and estimate their size) hidden in JPEG images using the steganographic algorithm F5. The key element of the method is estimation of the cover-image histogram from the stego-image. This is done by decompressing the stego-image, cropping it by four pixels in both directions to remove the quantization in the frequency domain, and recompressing it using the same quality factor as the stego-image. [4] Chao-Shen Chen, Rong-Jian Chen, "Image Encryption and Decryption Using SCAN Methodology", In this project, we have used a algorithm for image encryption based on scan patterns that first shuffle the image completely and then exploit function xor. The algorithm trades off between speed and security, so that more complex key which shuffle the image completely results more security but it consume more time. Yet in most complexity mode the algorithm act fast. [5] Sozan Abdulla, "New Visual Cryptography Algorithm For Colored Image", The proposed algorithm is for color image, that presents a system which takes four pictures as an input and generates three images which correspond to three of the four input pictures. The decoding requires only selecting some subset of these 3 images, making transparencies of them, and stacking them on top of each other, so the forth picture is reconstructed by printing the three output images onto transparencies and stacking them together. The reconstructed image achieved in same size with original secret image.

III. METHODOLOGY

A. Genetic Algorithm

Genetic algorithm in cryptography can be used for generating the key. Key generation in cryptography is the most important part of encoding data. If the key is randomly chosen and non-repeating used than this cypher is called one time pad (or one time system). The one of the most used one time pad is in Vernam cipher. Vernam cipher is a stream cipher where plaintext is converted into cipher text by using XOR operation between plaintext and the key.

One of the possible methods of generating the key is described in the work. It consists of:

1. Generating binary population. For this step, pseudo random number generator can be used.
2. Selection. Where the two parents will be chosen for reproduction.
3. Crossover. From parents by using crossover operator we gain child.
4. Mutation. After crossover we applied mutation operator.
5. Fitness function. If value from fitness function is satisfactory random chromosome is selected as the key else process is repeated.
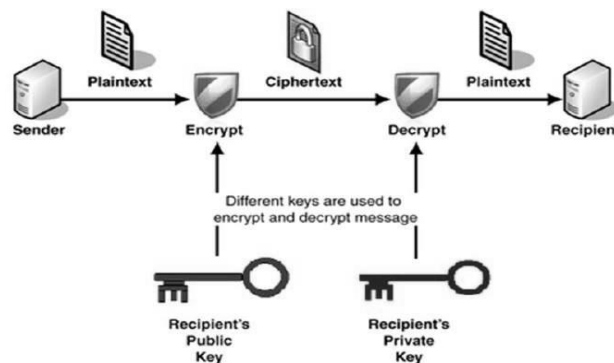
B. QR Code Steganography

Steganography is the art and science of writing secret messages in such a way that aside from the sender and the intended receiver, no one even suspects the existence of the secret message. Notice that steganography goals are in contrast to the goals of cryptography because encrypted messages or images attract attention. In steganography, the mere suspicion of a hidden message existence is sufficient to declare the failure of the scheme, even if the hidden message cannot be deciphered. QR codes have been previously used to exchange encrypted content, but there is no such research that uses them for steganography in the same fashion as this research. Being able to hide secret messages within general QR code symbols creates endless possibilities for discreet communication through QR codes. The idea behind this research is to show how to communicate a secret message between the sender and the receiver using QR codes without arousing any suspicion. Additionally, we show two ways to extract the secret message from the QR codes: first, using a private shared key between the sender and receiver, and second, without a shared key. For the purpose of this experiment, we show how person A (Adam) will communicate a secret message with person B (Bob).
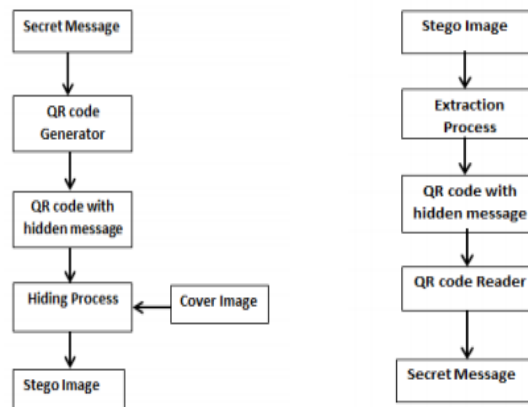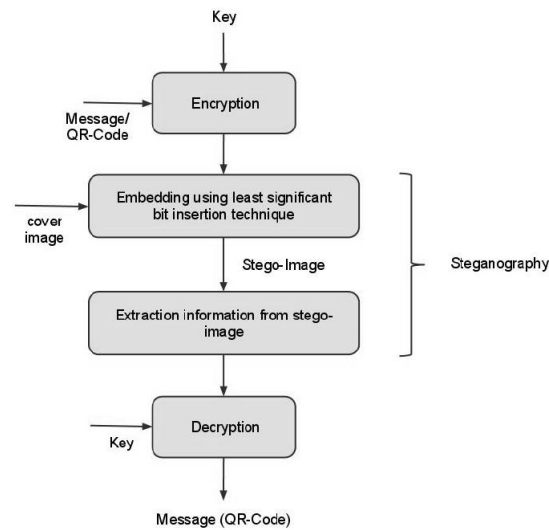
IV. CONCLUSION

This process has believe that by proposing the block-based encryption and decryption algorithm, it will help to reduce the relationship among image elements by increasing the entropy value of the encrypted images as well as lowering the correlation. Here in this paper a survey of all the existing Image Steganography techniques are discussed with their various advantages and limitations. Hence on the basis of their various advantages and limitations a new and efficient Image Steganography is implemented in future.

V. FUTURE ENHANCEMENT

Due to the rich availability of choices and the masking features offered by the massive utilization in Internet, malware developers could find the highest potential in network steganography. So, the future work will be possible to make deeper analysis in order to understand the steganography process of hider man and masker. The research can be expanded by doing analysis of steganography process of other tools in the audio and video media file. Identifying the maximum capacity of information that can be hidden in an image using a particular steganographic tool has to be modeled.

REFERENCES

[1] Mrs. G. Prema, S. Natarajan, "Steganography using genetic Algorithm along with visual Cryptography for Wireless Network Application", International conference on information communication and embedded systems (ICICES), 2013.

[2] Fridrich J., Goljan M. And Du R, "Reliable Detection of LSB Steganography in Color and Grayscale Images", Proceedings of Workshop on Multimedia and Security, Ottawa, pp. 27-30, , October 5 2001.

[3]   J. Fridrich, M. Goljan and D. Hogea, "Steganalysis of jpeg images: Breaking the f5 algorithm", In Proc. Of the ACM Workshop on Multimedia and Security, 2002.

[4] Chao-Shen Chen, Rong-Jian Chen, "Image Encryption and Decryption Using SCAN Methodology", Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06), 2006.

[5] Sozan Abdulla, "New Visual Cryptography Algorithm for Colored Image", Journal of computing, volume 2, issue 4, April 2010.