# STEGANALYSIS OF IMAGES USING QRC

**Description:**

The Steganalysis of images using QRC is used to handle the security of the user information and it provides the ease of access for the files. This uses cryptography and steganography in combined form in order to encrypt the user file and hide them behind an image.

System gathers the files from the user that are to be encrypted and secured.

**Technology details:**

C#, .NET IDE: Microsoft Visual Studio, SQL.

**Existing system:**

* The existing system of steganography can be used only to encrypt one type of file and it cannot accept all other types.
* The text alone can be hidden inside the image which may provide less security and privacy.
* The steganalysis can be a useful and advanced technique which might prevent intrusion or hacking.

**Proposed system:**

* The steganalysis technique can be implemented to encrypt any form of file and hide its key behind an image.
* This image can be converted to QR Code which can be decrypted by any user-friendly device like desktop, Mobile, scanners etc..,
* It can support on any operating system like Windows, Mac OS, blackberry, android etc.,

**Future enhancements:**

This analysis using QRC can be applied in transmission of big data to overcome the shortfalls of digital media and its associated security techniques.

**Algorithm used:**

**RIJNDAEL ALGORITHM**

The Rijndael algorithm is a new generation symmetric block cipher that supports key sizes of 128, 192 and 256 bits, with data handled in 128-bit blocks - however, in excess of AES design criteria, the block sizes can mirror those of the keys. Rijndael uses a variable number of rounds, depending on key/block sizes, as follows:

* 9 rounds if the key/block size is 128 bits
* 11 rounds if the key/block size is 192 bits
* 13 rounds if the key/block size is 256 bits

Rijndael is a substitution linear transformation cipher, not requiring a Feistel network. It uses triple discreet invertible uniform transformations (layers). Specifically, these are: Linear Mix Transform; Non-linear Transform and Key Addition Transform. Even before the first round, a simple key addition layer is performed, which adds to security. Thereafter, there are Nr-1 rounds and then the final round. The transformations form a State when started but before completion of the entire process.

The State can be thought of as an array, structured with 4 rows and the column number being the block length divided by bit length (for example, divided by 32). The cipher key similarly is an array with 4 rows, but the key length divided by 32 to give the number of columns. The blocks can be interpreted as uni-dimensional arrays of 4-byte vectors.

The exact transformations occur as follows: the byte sub transformation is nonlinear and operates on each of the State bytes independently - the invertible S-box (substitution table) is made up of 2 transformations. The shift row transformation sees the State shifted over variable offsets. The shift offset values are dependent on the block length of the State. The mix column transformation sees the State columns take on polynomial characteristics over a Galois Field values (28), multiplied x4 + 1 (modulo) with a fixed polynomial. Finally, the round key transform is XOR ed to the State. The key schedule helps the cipher key determine the round keys through key expansion and round selection.

Overall, the structure of Rijndael displays a high degree of modular design, which should make modification to counter any attack developed in the future much simpler than with past algorithm designs.

**Input:**

* The input will be the files which the user desires to encrypt & the image behind which the files are to be encrypted.
* The password consisting of 8 characters must be given by the user such that it is known only to the developer and the user alone.
* The name of the file in which the encrypted file is to be stored must be specified.

**Output:**

* The output will be the QR Code which consists of the encrypted image behind it.
* This QR code can be given to the user such that it can be scanned to view the image behind which the file is hidden.
* The decrypted form of file can be known only id the password is specified.

**Process involved:**

1. The steganalysis application can be used to carry out the encryption and decryption.
2. The files to be encrypted is specified in the “attach files” text box.
3. The image behind which the file to be hidden is specified by clicking the “attach image” button.
4. The password must be specified in order to protect the file.
5. The alternate name of the file in which the encrypted file is to be stored is specified in the “output location” text box.
6. To encrypt the file “Encryption” button is clicked.
7. The QR code is automatically generated if the file is encrypted and the key is available.
8. The QR code can be scanned using any scanner software & it displays the link of the image.
9. The link is clicked in order to download the image.
10. The image can be attached in the Steganalysis application again to carry out the decryption process similar to encryption.
11. The password must be known in order to decrypt the files.