International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.22 (SJIF-2017),e-ISSN:2455-2585
International Conference on
Recent Explorations in Science, Engineering And Technology (ICRESET'19)
Volume-5, Special Issue-March, 2019.

STEGANALYSIS OF IMAGES USING QRC

Bhavadharini K[1], Meganisha B[2], Suseendran S[3]

[1,2]Department of CSE, KGiSL Institute of Technology
[3]AP-Department of CSE, KGiSL Institute of Technology,

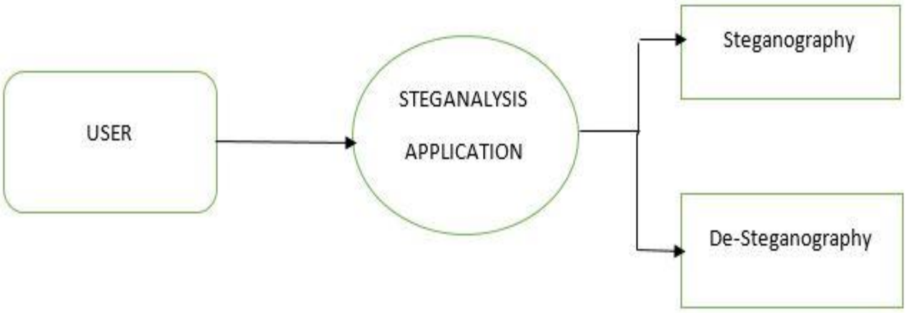
Abstract: - Steganalysis is an efficient technique used to hide any encrypted data behind an image or any other digital media to make them more secure. This image can be converted into a Quick Response Code which can make the encryption more powerful. It can be said as a combination of steganography and cryptography techniques into a single technique. The steganography can preserve the secrecy whereas the cryptography can prevent intrusion. The steganalysis can prevent intrusion and make data secure by maintaining the secrecy of data. This can be the solution to ensure the security of the data as it is concerned by implementing the steganography technique for images with the improvement on both image security & quality. This technique can prevent the data and media from the vulnerable attacks and other several threats. It uses more secure algorithms which are unbreakable when compared to its previous techniques.

Keyword: Steganalysis, QRC, Steganography,

I. INTRODUCTION

- 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.

- 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 QRCode which can be decrypted by any user-friendly device like desktop, Mobile, scanners etc.., It can support on any operating system like Windows, MacOS, blackberry, android etc.,



Several algorithms can be used to carry out the cryptographic techniques in steganalysis they are:

- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)
- Rijndael Algorithm etc.

EXISTING METHOD:

The existing system involves tedious process. The process does not combine steganography and cryptography. It cannot perform both cryptography and steganography at the same time and lacks many features. It cannot support various operating systems. The existing system is not portable and cannot run on other devices.

Drawbacks of existing methods:

The drawbacks of the existing methods are as follows:

- Take more processing time.
- There is lack of security for the data.
- Does not support all the versions and all the operating systems.
- More vulnerable to threats & attacks.
- Difficulty in detecting the intruders.
- Lack of media quality & robustness.

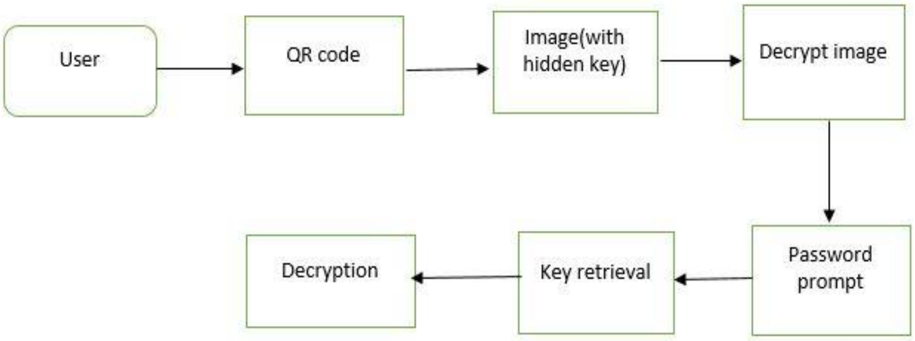
II. PROPOSED METHOD

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 QRCode which can be decrypted by any user-friendly device like desktop, Mobile, scanners etc.., It can support on any operating system like Windows, MacOS, blackberry, android etc.,

2.1 Advantages of proposed method:

The major advantages for proposed system is as follows

- Run across various devices.
- Support various operating systems.
- Portable & easy to carry the QR code anywhere.



Encryption & decryption in steganalysis

III. RIJNDAEL ALGORITHM

The Rijndael algorithm is a new symmetric block cipher that supports various 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 be same of those keys. Rijndael uses a various number of rounds, depending on key/block sizes, as follows:

- It perform 9 rounds if the key/block size is 128 bits
- It performs 11 rounds if the key/block size is 192 bits
- It perform 13 rounds if the key/block size is 256 bits

Rijndael is a substitution linear transformation cipher method. It does 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. Before the first round, a simple key addition layer is performed, which is for security. Thereafter, there are Nr-1 rounds and then the final round. The transformations forms a State when started but before completion of the entire process.

The State can be considered 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 XORed to the State. The key schedule helps the cipher key determine the round keys through key expansion and round selection.

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

3.1 Input Design

Input Design is the process of converting a description of the input into a computer-based system. This design is important to avoid errors in the input process and show the correct direction for getting correct information from the computer system.

It is achieved by creating user-friendly interface for the data enter and to handle big data. The goal of designing input is to make the data entry easy and to be free from errors. The data entry user interface is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

When the data is entered it will check validation. Data can be entered with the help of user interface. Appropriate messages are provided as when needed. Thus the objective of input design is to create an input layout that is easy to use.

3.2 Output design

A quality of output is one, which meets the requirements of the end user and presents the information clearly. In any system results, the processing are communicated to the users and to other system through outputs. In output design it is determined as how the information is to be displaced for immediate need and also the hard copy output. It is the most important one and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user's decision-making.

IV. ENCRYPTION & KEY GENERATION

The encryption is a part of cryptography which is applied in steganalysis. This can protect the files of the user with a specific key which serves as a purpose of security. The files which are to be protected are obtained from the user. The files which are obtained from the user are encrypted using rijndael algorithm and it results in the generation of the key as a result of the encryption. This key can be used as a part of decryption and also in the retrieval of image from the QR code.

4.1 Hiding the key

The steganography is the process of hiding any form of content behind a digital media. This is applied after cryptography in steganalysis. The key is a form of data which can be hidden behind any digital media like image. This is the part where the steganography and cryptography are combined.

The key which is obtained after the encryption of the image is hidden behind an image. The image into which the key should be hidden can be chosen by the user themself. This concept of hiding the key generated after the encryption of the selected file behind an image involves steganography.

4.2 Image to QR conversion

The image which now holds the hidden key called as "stego-image" is converted into a QR code for easy access and enhanced security. This helps the user to protect their data in a more secure way and QR code can be scanned easily. The reverse process of converting the QR into an image will result in decryption.

The conversion of image to a QR code is carried out in order to ensure the ease of access and portability. The QR code can be easily applied or scanned from any hand-held device. This ensures the security as the decryption only happens when the key is known by the user.

4.3 Extraction of key from the image

The resulting QR can be scanned to view the image from which the key can be extracted. The key should be extracted from the image by scanning the QR code and this process of extraction is termed as "De-steganography". This key can be used to decrypt the file and view the original contents of the file.

The extraction of key is done to retrieve the file that has been hidden behind the image. This is the reverse process of those initial key generation processes.

4.4 Decryption

The decryption process is the reverse of the encryption process. This process must be carried out in order to retrieve the original file which is encrypted and hidden. This helps the user to view their original file if the key is known.

The decryption is the part of cryptography which is applied in steganalysis in order to enhance the security of the content provided. The decryption can be done only by the user who knows the key.

V. CONCLUSION

The proposed system is very easy to implement and it does not involve in any loss of data. This does not reduce the quality of the image or the content of the file. It ensures the usage of the most secure algorithm which is easy to implement but hard enough to crack. The algorithm proposes various advantages and is widely used for higher security. The only disadvantage in steganalysis is that the file cannot be hidden behind the image directly instead it is encrypted and the key alone can be hidden.

VI. REFERENCES

[1] Rajani Devi.T "Importance of Cryptography in Network Security" International Conference on Communication Systems and Network Technologies IEEE 2013(462 - 467).

[2] N. F. Johnson and S. Jajodia, "Steganalysis: The Investigation of Hidden Information", IEEE Information Technology Conference, September 1998.

[3] J. Cummins, P. Diskin, S. Lau and R. Parlett, "Steganography and Digital Watermarking", School of Computer Science, the University of Birmingham, 2004.

[4] J. Watkins, "Steganography – Messages Hidden in Bits", 2008.

[5] W. Luo, F. Huang, J. Huang, Edge adaptive image steganography based on LSB matching revisited, IEEE Trans. Inf. Forens. Security 5 (2) (2010)201-214.

[6] Ge Huayong, Huang Mingsheng, Wang Qian, "Steganography and Steganalysis Based on Digital Image", IEEE Trans. International Congress on Image and Signal Processing, (2011) 252-255.

[7] Nur Hadisukmana, Yosua Kristianto "Steganography Software with Combination of Encryption Algorithms for Multimedia Files" First International Conference on Informatics and Computational Intelligence IEEE Dec2011 (100 - 105).

[8] Manoj Kumar Ramaiya ,Naveen Hemrajani, Anil Kishore Saxena "Security Improvisation in Image Steganography using DES" 2012 IEEE(1094 - 1099).

[9] Parag Kadam, Mangesh Nawale, Akash andhare, Mukesh Patil "Separable Reversible Encrypted Data Hiding in Encrypted Image Using AES algorithm and Lossy Technique" Proceedings of the 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering February 21-22 2013 IEEE.

[10] https://www.lri.fr/~fmartignon/documenti/systemesecurite/5-AES.pdf

[11] https://searchsecurity.techtarget.com/definition/Rijndael

[12] https://www.cs.mcgill.ca/~kaleigh/computers/crypto_rijndael.html

[13] https://ieeexplore.ieee.org/document/1289996