**Valid QR Codes Using Steganography and Cryptography Messages**

**ABSTRACT: -**

Steganography is considered the first line of defense in information security as it hides a secret message (payload) inside an innocent looking le (container) to transfer the payload under the adversary's nose without noticing it. Steganographic systems only use the container to hide the payload. In this paper, we present a steganographic system that uses the container not only to hide the payload, but also to give misleading information to the adversary. To achieve this goal, we use quick response (QR) code as a container. QR codes generated by our proposed system can carry its ordinary message in addition to the payload. Anyone can read the message, but the payload can only be obtained using a secret key. The message and the payload are unrelated; i.e. any message can be generated regardless of the payload and vise versa. We can take advantage of that by generating a message that gives misleading information to the adversary. We test the proposed system and show that the generated QR code is (valid) i.e indistinguishable from an ordinary QR code which makes it look innocent and less susceptible to an adversary's attack. Moreover, it is space-efficient, has an acceptable level of noise immunity and is prone to steganalysis attacks.

|  |  |
| --- | --- |
| **EXSISTING SYSTEM** | **PROPOSED SYSTEM** |
| * However, the existing work only provides in their system, a database is constructed by a group of chosen images, and these images are indexed in the database by generating hashing sequences for these images. * The payload is divided into segments. An image is sent if its hashing sequence is matching with the segment. * Their system is robust to luminance changing and noise. | * In this paper, we present a steganographic system that uses the container not only to hide the payload, but also to give misleading information to the adversary. * To achieve this goal, we use quick response (QR) code as a container. QR codes generated by our proposed system can carry its ordinary message in addition to the payload. Anyone can read the message, but the payload can only be obtained using a secret key. The message and the payload are unrelated; i.e. any message can be generated regardless of the payload and vice versa. * Embedding the payload in the QRcode without affecting its image quality and its message. Securing the payload against an adversary. |
| **EXISTING ALGORITHM**  Multi-level Encryption Algorithm (MLEA), | **PROPOSED ALGORITHM:-**  Stegnalysis QR Payload Embedding and Extraction (SQPEE) |
| **ALGORITHM DEFINITION:-**  After that, the message is encrypted using a multi-level encryption algorithm (MLEA), then the encrypted payload is concealed in the host image using an adaptive LSB substitution. Their system achieves a reasonable balance between quality and security. | **ALGORITHM DEFINITION:-**  The proposed system consists of two parts: the payload embedding and the payload extraction. The owchart of embedding the payload in the QR code. The QR code can be generated by any QR code software.  The message is independent from the payload. It can be chosen as an innocent message such as a food label, or it can be chosen as a misleading message to the adversary. The role of the encryption algorithm is to randomize the payload in a way that makes the probability of the pixels' values |
| **DRAWBACKS:-**   * Providing less security * Because of less security may be a data leakage. | **ADVANTAGES:-**   * Providing more security * We can take advantage of that by generating a message that gives misleading information to the adversary. * More space-efficient |

**MINIMUMSYSTEM REQUIREMENTS**

**HARDWARE REQUIREMENTS**

* PROCESSOR : DUAL CORE 2 DUO.
* RAM : 2GB DD RAM
* HARD DISK : 250 GB

**SOFTWARE REQUIREMENTS**

* FRONT END : J2EE (JSP, SERVLET)
* BACK END : MY SQL 5.5
* OPERATING SYSTEM : WINDOWS 7
* IDE : ECLIPSE