ISSN 2395-1621

Authenticate Message Hiding in QR Code Using AES Algorithm

[#1]Shraddha Bhavar, [#2] Juily Jadhav, [#3] Nikita Kulkarni, [#4] Krutika Patil

[#3]nikitakulkarni579@gmail.com

[#1234]Students, Department of Computer Engineering, JSPM NTC, Pune

ABSTRACT

Quick Response Code that is QR code is widely used in daily life in recent years because it has high capacity encoding of data, damage resistance, fast decoding and other good characteristics. Since it is popular, people can use it to transmit secret information without inspection. The development of steganography in QR code leads to many problems arising. How to keep the original content of QR code and embed secret information into it are the one main challenge .In this project we are using the AES algorithm for the encryption and decryption of data and LSB used for the steganography .We also conduct our solution by analysing the complexity, security of the secret message.

***Keyword*: QR code, Steganography, AES algorithm , LSB matching algorithm.**

ARTICLE INFO

Article History

Received 21st March 2016

Received in revised form :

23rd March 2016

Accepted : 25th March 2016

Published online :

28th March 2016

I. INTRODUCTION

The existing system is based on Reed Solomon Codes and List Decoding which are more vulnerable to attacks and used bit technique to store message in the QR code. In proposed system we adding more security to the message hiding technique in QR code by using AES encryption algorithm and LSB matching algorithm. A key functionality is also to be provided to add more security to the secret data. Even the amount of data that can be stored in the QR is increased. LSB matching is basically used for steganography in the QR code. LSB matching enhances the secret message hiding quality of the QR code.

The process of hiding secret message using QR code by a key. The aim of ‘Secret Message hiding in QR code’ is with the help of cover message hidden message can be send or receive in QR code by user who has the application.

The process of hiding secret message using qr code by a key. the aim of ‘secret message hiding in qr code’ is with the help of cover image hidden message can be send or receive in qr code by user who has the application.

II. PRELIMINARIES

Area of our project is Image Processing. We are using QR code to hide the secret message which is covered by a cover message or image. The secret message can be decrypt only after using a key into the application.

A. QR Code

QR code is a type of matrix barcode (or two-dimensional barcode)[11]. A barcode is a machine-readable optical label that contains information about the item to which it is attached. A QR code uses four standardized encoding modes (numeric, alphanumeric, byte/binary, and kanji) to efficiently store data; extensions may also be used. The QR Code system became popular outside the automotive industry due to its fast readability and greater storage capacity compared to standard barcodes. Applications include product tracking, item identification, time tracking, document management, and general marketing.[11][9]

B. Steganography

Steganography is the process of concealing a file, message, image, or video within another file, message, image, or video.

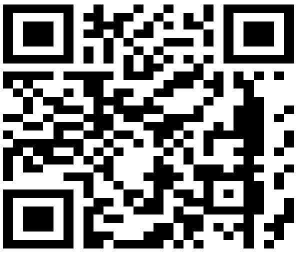

Fig.1 QR Code

III.PROPOSED SOLUTION

It is a desktop application through which we can send and receive the secret message. This message will be in encoded form and to decode this message one key will be provided to the receiver. Using this public key the user can decode the secret message. The secret message is hidden behind the QR image. That means when we scan the QR code we only get the normal message and when we place this QR image into the application it asks for the key. And when the key is entered we can get the secret message.

But it's important for the receiver to have the public key to decode the secret message. AES is a symmetric algorithm so we need to use the same key for encryption and decryption. Sender sends the key manually through SMS to the receiver.

A. AES

The Advanced Encryption Standard the AES is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data. The origins of AES date back to 1997 when the NIST announced that it needed a successor to the aging Data Encryption Standard (DES) which was becoming vulnerable to brute-force attacks. This new encryption algorithm would be unclassified and had to be "capable of protecting sensitive government information well into the next century. "It was to be easy to implement in hardware and software, as well as in restricted environments (for example, in a smart card) and offer good defences against various attack techniques.[9]

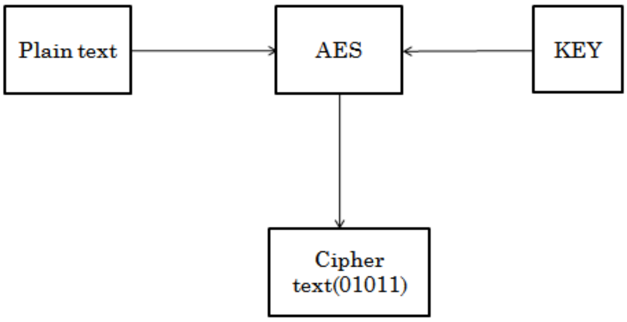

Fig. 2.AES diagram.

B.LSB

The least significant bit (LSB) is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. The LSB is sometimes referred to as the right-most bit, due to the convention in positional notation of writing less significant digits further to the right. It is analogous to the least significant digit of a decimal integer, which is the digit in the ones (right-most) position. It is common to assign each bit a position number, ranging from zero to N-1, where N is the number of bits in the binary representation used. Normally, this is simply the exponent for the corresponding bit weight in base-2. Although a few CPU manufacturers assign bit numbers the opposite way (which is not the same as different endianness), the term least significant bit itself remains unambiguous as an alias for the unit bit. By extension, the least significant bits (plural) are the bits of the number closest to, and including, the LSB. The least significant bits have the useful property of changing rapidly if the number changes even slightly. For example, if 1 (binary 00000001) is added to 3 (binary 00000011), the result will be 4 (binary 00000100) and three of the least significant bits will change (011 to 100). By contrast, the three most significant bits (MSBs) stay unchanged (000 to 000).

IV. MOTIVATION OF THE PROJECT

The process of hiding secret message using QR code by a key. The aim of secret Message hiding in QR code is with the help of cover message hidden message can be send or receive in QR code by user who has the application

1. Security: It secure the secrete message in QR code using AES algorithm.
2. Data Storage: It increases the storage efficiency of the QR code.
3. Data Loss: The cover message does not get affected after encrypting the secret message in QR code.

V.SYSTEM ARCHITECTURE

User can scan the QR code which he gets through the email. And he will get the normal massage. But if he wants the secret massage and he has the secret key which is sent through SMS then user upload the QR image into the application and provide the secret KEY to it. After giving the secret KEY user can get the secret massage. Only using KEY user can get the secret massage.

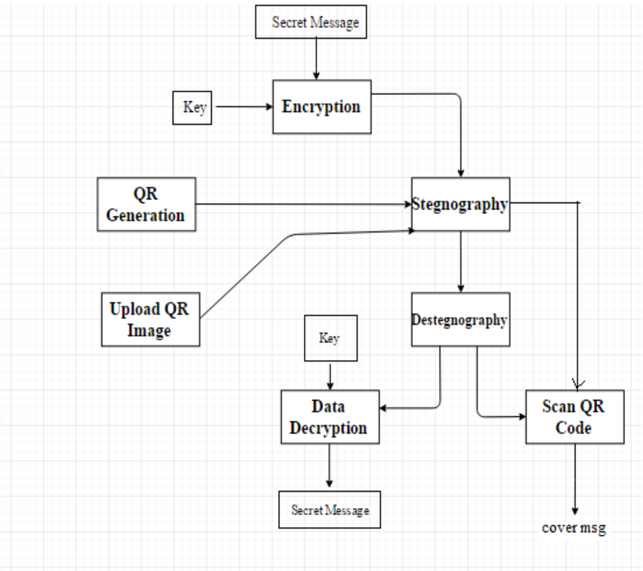

Fig 3. System Architecture

V. STATEMENT OF SCOPE

Scope of this project is to hide the secret message in the QR code which already has a cover message in it. This will generate secret communication between any those users having the application and key. But the user who doesn't have this application can scan the QR code and also able to read the cover message.

VI.MAJOR CONSTRAINTS

The major constrain of this project is to send and receive private massage using publicly available QR code.

VII. CONCLUSION

QR code is used to link directly to the URL , Its also used to hold some record or data in it. The size of QR code is very small so data storage in it is limited .Hiding message in this QR code which is already has limited storage area is very difficult. . In proposed system we add more security to the message hiding technique in QR code by using AES encryption algorithm and LSB matching algorithm. A key functionality is also to be provided to add more security to the secret data. Even the amount of data that can be stored in the QR is increased. LSB matching is basically used for steganography in the QR code. LSB matching enhances the secret message hiding quality of the QR code.

ACKNOWLEDGMENT

It gives us great pleasure in presenting the Paper on 'Authenticate Message hiding in QR code using AES algorithm'.We would like to take this opportunity to thank our internal guide Prof. D. S. Uplaonkar for giving us all the help and guidance we needed. We are really grateful to them for their kind support. Their valuable suggestions were very helpful. We are also grateful to Prof. R. H. Kulkarni , Head of Computer Engineering Department and Project coordinator Prof. S. S. Shinde , RSSOER for their indispensable support, suggestions.

REFRENCES

[1] Thach V. Bui, Nguyen K. Vu, Thong T.P. Nguyen, Isao Echizen† and Thuc D. Nguyen Robust Message Hiding for QR Code Faculty of Information Technology University of Science, Ho Chi Minh City, NationalInstitute of Informatics, Tokyo, Japan.

[2] Chen, Wen-Yuan, and Jing-Wein Wang. Nested image steganography scheme using QR-barcode technique. Optical Engineering 48, no. 5(2009): 057004-057004.

[3] Chung, Chin-Ho, Wen-Yuan Chen, and Ching-Ming Tu. Image hidden technique using QR-barcode. In Intelligent Information Hiding and Multimedia Signal Processing,2009.IIH-MSP'09.Fifth International Conference on, pp. 522-525. IEEE, 2009.

[4] Huang, Hsiang-Cheh, Feng-Cheng Chang, and Wai-Chi Fang. Reversible data hiding with histogram-based difference expansion for QR code applications. Consumer Electronics, IEEE Transactions on 57, no. 2 (2011): 779-787.

[5] wISO/IEC 18004:2006. Information technology – Automatic identification and data capture techniques – QR Code 2005 bar code symbology specification.

[6] Soon, Tan Jin. QR code. Synthesis Journal (2008): 59-78.

[7] Beelen, Peter, and Kristian Brander. Key equations for list decoding of Reed Solomon codes and how to solve them.Journal of Symbolic Computation 45, no. 7 (2010): 773-786.

[8] Bui, Thach V., Binh Q. Nguyen, Thuc D. Nguyen, Noboru Sonehara, and Isao Echizen. Effective Fingerprinting Codes for Database.In Signal- Image Technology & Internet-Based Systems (SITIS), 2013 International Conference on, pp. 655-659.IEEE, 2013.

[9] Fei Shao, Zinan Chang, Yi Zhang. "AES Encryption Algorithm based on the high performance computing of GPU". Communication software and networks, 2010.ICCSN'10 Second International Conference.

[10] Neeta D,Snehal.K,Jacobs.D."Implementation of LSB stegnography and its evaluation for various bits".Digital Information Management,2006 First International Conference.

[11]https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[12] Lin, Pei-Yu, Yi-Hui Chen, Eric Jui-Lin Lu, and Ping Jung Chen. Secret Hiding Mechanism Using QR Barcode. In Signal-Image Technology &Internet-Based Systems (SITIS), 2013 International Conference on, pp.22-25. IEEE, 2013