A THREE TIER ARCHITECTURE FOR DOCUMENT AUTHENTICATION

Reshma Totare, Nikita Doke, Snehal Varude, Kumudini Ponde, Prasidha Godhane

Abstract:
As we know QR (Quick Response) codes becoming the major transition routes for the authentication of the applications and the process. Quick response codes are most reliable and fastest way of authentication in today's world. These authentications can be used in implicit or in an explicit way to ensure the security instead of passwords. Many quick response code authentications are single tier, where they involve only QR codes and this may be the reason for lower security in many paradigms. So, to overcome this some two tier QR code authentication systems are existed where secret passwords are being hidden in the QR codes to provide double security for authentication. So, to enhance this process proposed methodology presents three tier security of QR code authentication where a document is encrypted using Reverse circle cipher encryption algorithm with a random key. This key is catalysed by RSA asymmetric algorithm. A Reversible data hiding technique is used to store these two deferent keys in two QR code Strings for their respective least Signiant bits. These QR code Strings are created by using the random pattern evaluation method. And whole model provides tuned security for the data authentication in three tier level.

Index Terms: QR Code, Document Authentication, Encoding and Decoding

1. Introduction
1. QR Code?

QR Code (Quick Response Code) is a 2D matrix barcode designed in 1994 in Japan for automotive industry of Japan. It provides easy information access using a Smartphone. A barcode contains information about the product to which it is added which is machine readable. QR code lets in to encode 4000 characters in a 2D barcode. Numeric, Alphanumeric, kanji and byte/binary are the four approved standard encoding modes utilized by QR code to electively save and keep records. A QR code is used in deferent scenario for deferent purpose like to open a URL, to save a contact, text to the user, product tracking, time tracking, item identification, document management etc. QR code is the registered trademark of “Denso Wave Incorporated”.

QR code is the combination of black squares in a square grid on a white background. It is read by the imaging device like camera and Reed Solomon error correction is used to process QR code till the code is appropriately identified. The information is contained in QR code is then obtained from patterns contain inside given String vertical and horizontal components. The content present inside QR code is not changed once generated. The most familiar type of QR code is Static QR codes, which is used to circulate information to common pubic. They are frequently shown on advertising material in newspaper, television and magazines. The information in static QR code is tracked by code creator as QR code is scanned. Dynamic QR codes also called Unique QR Code provide more functionality than Static QR code. This type of QR code contains some specific information like email address and scanner name and it is used more often for personalized marketing.

II. Document Authentication?

Authentication is the process to verify and prove the legality of documentary and physical evidence. It involves verifying the legality of individual documents or website with digital signature. An authentication of physical evidence like drugs, documents, jewels, goods etc, is the major concern in a world of global trade.

Paper documents are the important and basis of today's business transaction and administrative process. So, the authentication of printed papers which contain the signature and seal of one and more individual is very important. Document authentication is the process to confirm the genuineness and the legality of a document, to make it valid and legal. It proves that the seal and signature present on providing document is legal and genuine.

Forgery of a printed document is common in today’s world. The conventional solution to prevent document forgery like watermarking or use of special papers in printing is not cost effective. Document authentication is exceedingly esteemed research area, and lots of methodologies are studied to improve the authentication method and to enhance forged document detection technique. The technique investigates the viability of embedding certain facts about published documents for verification purposes. Such information will be separated from the content material of documents, which is divisible into two: the context, which includes the text, figures and shapes and the visible attributes of the report which include its colour and design.

III. Motivation

As we know QR (Quick Response) codes becoming the major transition routes for the authentication of the applications and the process. Quick response codes are most reliable and fastest way of authentication in today's world. These authentications can be used in implicit or in an explicit way to ensure the security instead of passwords.

2. Literature Survey

I. Thach V. Bui, Nguyen K. Vu, Thong T.P, Nguyen Isao Echizen and Thus D. Nguyen proposed a robust scheme to have hidden private message in the QR code. Their method is safe against a bit changed attack and easily handles more error in comparison to normal technique. In their proposed technique length of the message is smaller than the previous technique which depends on bit algorithm. They use Reed Solomon codes to encode private message before implanting the end result into a QR code.

II. Ching-Yung Lin and Shih-Fu Chang presents the prototype for the print and scan method. They considered geometric distortion and pixel value distortion for their prototype. They present the features of discretized and rescanned String in frequency and spatial domains and analyse the Discrete Fourier Transform coincident changes.
III. Tobias Langlotz and Oliver Bimber present an innovative method for optical data alteration between mobile device and public displays depend on unsynchronized 4D barcodes. They assume that no absolute (electro-magnetic or other) connection between the devices can exist. The mobile phone having camera utilizes to record 2D colour barcode which is displayed on screens. This allows transferring data optically amid both devices. Their method increases the abstracts throughput and the power of the barcode recognition, although no actual synchronization exists.

3. Techniques
I. Key generation

Description and Priority
Input-Instance String
Priority (High
Stimulus/Response Sequences
Stimulus: Hash Key generation
Response sequence: character selection

II. RCC

Description and Priority
Input-String Text
Priority (High
Stimulus/Response Sequences
Stimulus: Block creation
Response sequence: Character Rotation

Functional Requirements Data encryption.

III. QR Code image generation

Description and Priority
Input-Instance numbers
Priority (High
Stimulus/Response Sequences
Stimulus: Initial Pattern
Response sequence: Block formation

Functional Requirements QR code image creation.

IV. Encoding

Description and Priority
Input-QR code image and authentication key
Priority (High
Stimulus/Response Sequences
Stimulus: LSB bits
Response sequence: Data hiding

Functional Requirements
Encoded image.

4. System Architecture

Description:
I. Document Content: Document Content in String
II. Hash Key: Generate a md5 Hash Key for the String
III. Random Characters: Select Random Characters from the md5 Hash Key
IV. RSA: Create Public and Private Key
V. RCC: Encrypt the File using Public Key
VI. Random Pattern Analysis: Analysis the Random Pattern For the QR
VII. Code
VIII. Data Encoding: Hide Public and Private Key into QR code Image

5. Applications

Visual Cryptography technology can decode concealed images based purely on human Visual systems, without any aid from Cryptographic calculation. This good property gives birth to a wide range of encryption utilization. In this section, we will deal with how VCS is used in Applications such as E-Voting System, Financial documents and Copyright Protections.

I. Electronic-Balloting System

These a day’s utter most of the Voting is managed with Computer Systems. These Voting Machines expected voters to faith them, without giving testimony that they recorded each vote accurately. One way to solve this difficulty is to issue receipts to Voters to ensure them their votes are counted.
II. Encrypting financial documents

The VCS principle can also be practiced in transmitting confidential financial documents over Internet. VCRYPT is an example of this category of system being discover by Hawkes et al. VCRYPT can encode the original drawing document with a enumerate (k, n) VCS, then send each of the encoded n shares separately by Emails or FTP to the recipient.

6. Future Work

As the future scope proposed model can be enhanced to work in efficient web paradigm and in mobile applications. This can be used to provide live password authentication schemes to ensure the more security of the passwords and OTPs. Proposed model can be developed as the readymade API which helps the other developers too to build their system of stag analysis.

7. Conclusion

The proposed methodology successfully encrypts the given text by using the random keys which are initially created by the random number generation technique. This process is catalysed using the MD5 hashing algorithm for the instance attributes. These keys are powered with the RSA algorithm of asynchronous paradigm to provide more security in the key generation process. The Encryption process is enhanced and improved using the Reverse circle cipher algorithm by rotating the characters on each substitution of the blocks. A strong steganography process is being used to maintain the security using reversible data hiding technique inside the QR image. This QR image is being generated with the unique high-level combination of the random blocks of size 7 X 7.

The Whole process is tried and tested under many experiments for encryption and authentication, Experiments are found that proposed methodology outperform in maintaining a strict and secure way of three tier document authentication using the QR code images and RCC scheme. As our system is yielding.

8. Reference