

A Survey on Private Message Sharing and Document Authentication Methods using QR codes

D.H. Patil¹, Sumit Sawant², Tushar Tamhane³, Ganesh Khedkar⁴

Professor, Dept. of IT, Rajarshi Shahu College of Engineering, Savitribai Phule Pune University, Pune, India¹

Student, Dept. of IT, Rajarshi Shahu College of Engineering, Savitribai Phule Pune University, Pune, India^{2,3,4}

Abstract: Quick response codes or QR codes are increasing their popularity as they appear in more places in the today's scenario. Quick Response Codes can be considered as physical hyperlinks that give the ability to users to access information, share messages and authenticate the documents. Apart from marketing, QR Codes have been also adopted in different areas such as the on-line payments. As the usage of QR codes is increasing day by day care must be taken while designing the QR code so that there aren't any issues regarding its security and privacy. In this paper we have studied various state of the art existing techniques of designing QR code along with their comparison with each other. Also various state of the art existing techniques of document authentication with their comparison with each other.

Keywords: QR Code, Image Processing, Feature Extraction, Digital Signature.

I. INTRODUCTION

Quick response codes or QR codes are basically a two dimensional bar codes which are used day by day due to the technological advancements [1]. These codes have plenty of applications. To name a few, these QR codes can be used for storing information (advertising, museum art description), web site redirecting, tracking and tracing (for transportation tickets or brands), Entity identification (passenger information, supermarket products), Uniform resource locator, Code payments, Virtual stores, Website login, Message sharing and document authentication. QR code is also known as matrix barcode. QR code was invented by Denso Wave in Japan while working for automotive industry. Due to the technological advancements there are plenty of QR codes which are being used in the market. As a result of which the demand for QR code scanners has also increased proportionally. The popularity of QR code is due to its robustness, easy to read feature, higher encoding capacity and small size.

Although it has many advantages but still has many downsides to be improved upon most common disadvantages are: It is easily accessible to anyone even if it is ciphered and it is very difficult to distinguish between the originally generated QR codes with its photocopy. So, in order to intrude the QR code, any third person can retrieve the information with the help of a standard QR code scanner. As far as message sharing and document authentication are concerned the security of the QR code is our highest priority. In order to overcome these shortcomings we have proposed a two level QR code with enhanced encoding technique. This enhancement is achieved by using textures patterns in place of black modules. These patterns are sensitive to the distortions created while printing and scanning process. Our proposed

technique also lays emphasis on storage capacity apart from security and privacy. Our proposed system consists of a public level QR code and a private level QR code. The public level QR code can be accesses with the help of any standard QR code scanner whereas the public level QR code cannot be accessed from any standard QR scanner. Hence it provides a level of security against any possible intrusion to greater extent. The first level keeps the strong characteristics of the QR code whereas the second level improves the storage capacity of the QR code. This paper is as follows: we start with the overview of QR codes and in the subsequent sections we will be mainly exploring the state of the art existing techniques along with the proposed technique. And at the end we will compare our technique with the existing techniques.

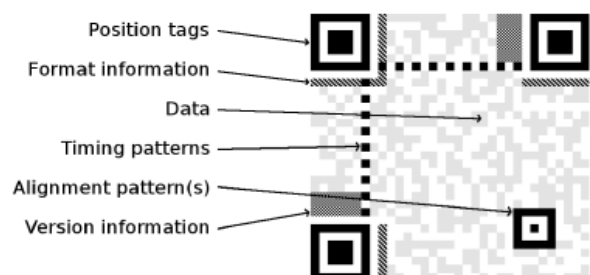


Fig. 1. QR Code.

II. VARIOUS APPROACHES FOR PRIVATE MESSAGE SHARING USING QR CODE

A. Contextual QR Code [2].

Contextual QR code is one of the most popular QR code used nowadays. Contextual QR code mainly uses the

attributes or contexts while designing QR code. It is basically a type of static QR code which is related to a particular context while designing a QR code. Contextual QR code can be generated by giving various contexts or parameters as input such as time, location, and IP address and device type for personalizing the output message by adding the name of the user or by changing the language and transfer user information and contexts along with the parameters to the server database. Contextual QR code is generated by taking user attributes into consideration. Contextual QR code mainly takes ubiquitous computing into consideration. Context aware QR code is capable enough to help filter information so that the relevant information under the right time at the right place is extracted. QR codes are used for context aware navigation. QR code also acts as a location source in which the physical location of the QR code is encoded inside a uniform resource locator. Context based QR code can also consider proximity apart from location. Proximity based QR codes can be very useful if the location of the user is very difficult to find. As far as private message sharing and document authentication is concerned contextual QR codes keeps a record of the various user attributes.

Very often, this change is related to privacy. For example, a privacy-aware proximity detection service determines if two mobile users are close to each other without requiring them to disclose their exact locations.

Contextual QR can be used to collect database of so called Wi-Fi “fingerprints”. Each fingerprint stores the description of the location and it also consists of the MAC addresses and the received signal strengths (RSSI) of nearby access points. This database could be used for Wi-Fi based positioning and historical records for fingerprints let us discover user’s behavioural patterns.

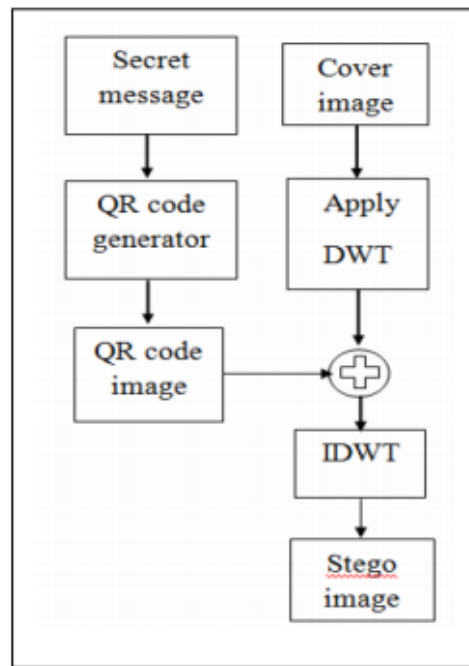
B. Code Steganography [3].

Steganography is basically the process of hiding data into a secret message. The QR code steganography hides the information or secret message into the QR code. The message to be hidden is termed as the secret message is used after encoding it with the help of error correcting bits. This error correction capacity of the QR code helps to perform the steganography of the QR code. The secret message in the QR code does not disturb the reading process of the QR code as such. The error capacity of the QR code Steganography is very low. In Steganography QR code, the maximum secret message length is equal to 1215 Bytes for QR code version 40 i.e.; V40. We can also embed an invisible watermark in the QR code which acts as the secret message. For such embedded invisible watermarks, discrete cosine transformation and discrete wavelet transformation are used [4].

Encoding algorithm:

- Step 1: Cover image is taken as an input.
- Step 2: Generate the QR code with the secret code.
- Step 3: Apply discrete wavelet Transformation.
- Step 4: Embed the QR code image on the cover image.

- Step 5: Apply inverse discrete wavelet transformation.
- Step 6: Steganographed QR code is generated.



Encoding Model.

Fig. 2. QR Code Steganography

C. Copy detection pattern QR code [5].

Copy detection pattern QR code is one of the most innovative and popular technique of QR generation. In this technique, with the help of secret key, password and random seed a maximum entropy image is generated which is used as a graphical QR code. This copy detection technique is most widely used for document authentication. The comparison of the original QR code along with the QR code present in the document is performed on the basis of which it is decided whether the document is authentic or not. After performing the comparison the difference is noted, and if the difference between these two QR codes is more than a threshold value then then we conclude that the document is not authentic and is tampered. In other words, the length of the message is given beforehand. This technique is even useful for removing the drawbacks created by performing the print and scan process, which distorts the original QR code.

III.COMPARATIVE STUDY OF VARIOUS APPROACHES FOR PRIVATE MESSAGE SHARING USING QR CODE

TABLE I COMPARISON TABLE

Sr. No	Storage Capacity(bits/inch)			
	Code Name	Public	Private	Total
1	Contextual QR code [2]	2953	0	2953

2	QR code stenography[3]	7089	1215	8304
3	Copy detection pattern[5]	7548	3102	10650

IV. VARIOUS APPROACHES FOR DOCUMENT AUTHENTICATION USING QR CODE

A. Image processing [7].

The image processing technique of document authentication using QR code is one of the most widely used document authentication technique. In this technique the main emphasis is laid on the signature verification with the help of QR codes. This technique provides a state of the art solution of skilled and semi-skilled forgeries by robust mechanism. This method provides dynamic information gathering as a result of which the performance is enhanced. This method is has very high accuracy. [7]

B. Feature Extraction [8].

In this technique, there are basically two phases of document authentication using QR codes. In first phase the input signature is acquired. The second phase consists of pre-processing, in which the various noises are removed and is further processed to pre-processing. In this technique, meaningful information will be extracted from pre-processed signature for classification. Afterwards, the features extracted in the previous stage are used to match the input signature shape and the training samples. The result is used to judge the authenticity of the input signature for reducing forgeries. Then the comparison of training data with features is performed. Then a threshold is set, and according to the threshold we will classify whether the document is authentic or not. But the results were not satisfactory as the extraction of exact signatures from testing data images produces error in verifying the signatures. [8]

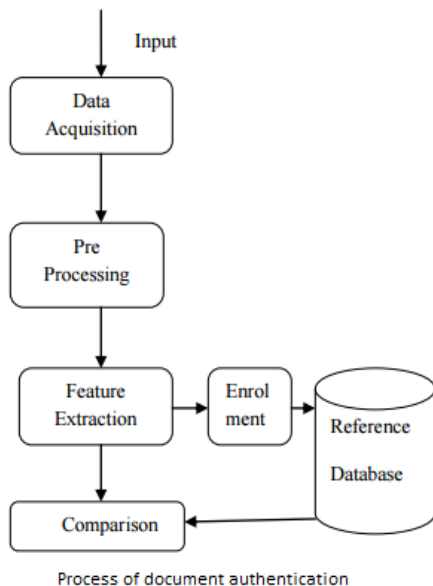


Fig. 3. Process of document authentication

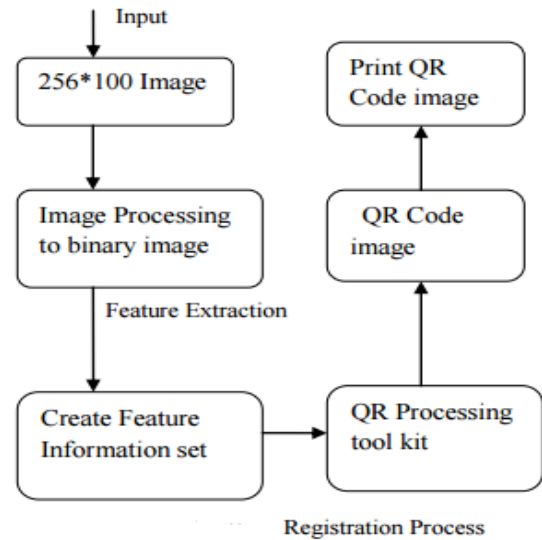


Fig. 4.Registration Process

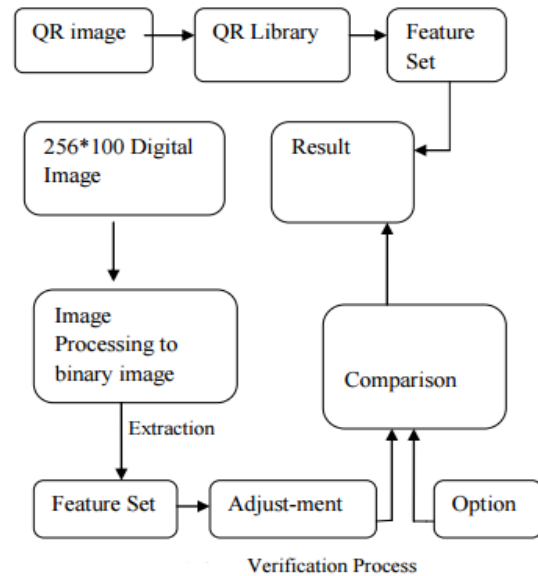


Fig. 5.Verification Process

C. Digital Signature [9].

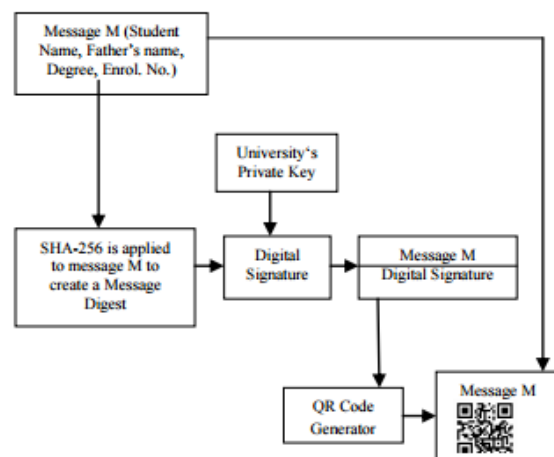


Fig 6 QR code generation using digital signatures

QR Code generation using Digital signature is one of the state of the art techniques for document authentication. Just as finger prints and hand written signatures are used to uniquely identify people for transactions and legal procedure, so digital signatures or digital thumbprints are commonly used to identify electronic entities for online transactions. A digital signature uniquely identifies the originator of digitally signed data and also ensures the integrity of the signed data against tampering or corruption.

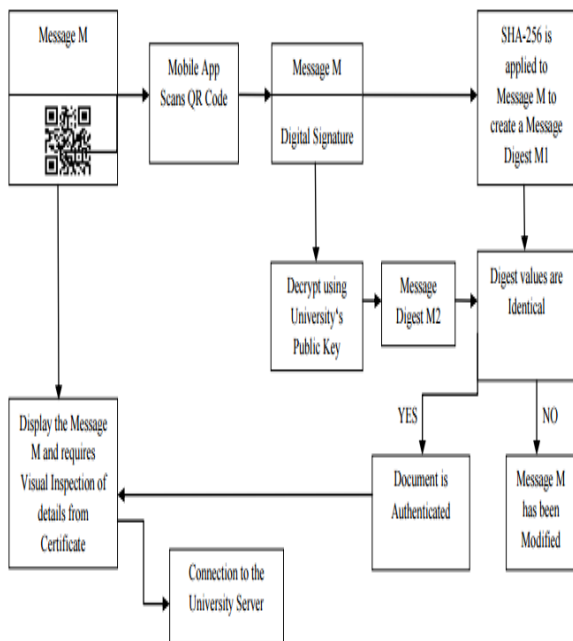


Fig.7 QR code scanning for document authentication

- 1) Input the message whose QR code is to be generated.
- 2) Find the message digest 5 checksum value of the message using SHA-256.
- 3) Use the Private Key to convert the message digest into digital signatures.
- 4) The input message along with the digital signature is fed to the QR code generator module.
- 5) The QR Code generator produces a QR Code by replacing the black modules.

V. COMPARATIVE STUDY OF VARIOUS APPROACHES FOR DOCUMENT AUTHENTICATION USING QR CODES

TABLE II COMPARISON TABLE

Sr. No	Document authentication using QR		
	Technique	Max Characters	Accur acy
1.	Image processing [7]	2953	71%
2.	Feature extraction [8]	4296	64%
3.	Digital Signature [9]	7089	75%

VI. CONCLUSION

In this survey paper we have compared various approaches for private message sharing such as Contextual QR code, QR code Steganography, Copy detection pattern QR code among these we have observed that Copy detection QR code has highest data storing capacity of storing 10650 bits/inch. As well as we have also compared various approaches for document authentication which are Image Processing, Feature Extraction, and Digital Signature in the context of QR code among these we have observed that Digital Signature has maximum accuracy of 75%.

REFERENCES

- [1] Information Technology—Automatic Identification and Data Capture Techniques—Bar Code Symbology—QR Code, ISO/IEC Standard 18004:2000, 2000.
- [2] J. Rouillard, "Contextual QR codes," in Proc. IEEE 3rd Int. Multi-Conf.Comput. Global Inf. Technol. (ICCGI), Jul./Aug. 2008, pp. 50–55.
- [3] T. V. Bui, N. K. Vu, T. T. P. Nguyen, I. Echizen, and T. D. Nguyen, "Robust message hiding for QR code," in Proc. IEEE 10th Int. Conf.
- [4] P.-Y. Lin, Y.-H. Chen, E. J.-L. Lu, and P.-J. Chen, "Secret hiding mechanism using QR barcode," in Proc. IEEE Int. Conf. Signal-Image Technol. Internet-Based Syst. (SITIS), Dec. 2013, pp. 22–25.
- [5] J. Picard, "Digital authentication with copy-detection patterns," Proc. SPIE, vol. 5310, pp. 176–183, Jun. 2004.
- [6] Iuliia Tkachenko, William Puech, Senior Member, IEEE, Christophe Destruel, Olivier Strauss, Jean-Marc Gaudin, and Christian Guichard, "Two-Level QR Code for Private Message Sharing and Document Authentication," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 3, MARCH 2016.
- [7] Amina Khatra, "Signature Verification Using Image Processing Techniques," International Global Research analysis (2277-8160) Volume 2 Issue 12, Dec 2013.
- [8] M. Jasmine, K. Murugesan, "Bank Cheque Authentication using signature" , International Journal of Advanced research in Computer science and software Engineering(2277 18x) volume 3, issue 5, May 2013.
- [9] Samit Biswas, Tai-hoon Kim, Debnath Bhattacharyya"Features Extraction and Verification of Signature Image using Clustering Techniques", International Journal of Smart Home, Vol 4 No. 3, July, 2010.
- [10] Hemant Saikia, Kanak Chandra Sama, " Approaches and issues in offline", International Journal of Computer Application (0975-8887) Volme42-NO16, March 2012.
- [11] Maykin Warasart, Pramote Kuacharoen" Paper based Document Authentication using Digital Signature and QR Code", International conference on Computer Engineering and technology vol. 40, 2012.
- [12] Donato Impedovo and Giuseppe Pirlo" Automatic Signature Verification: The State of the Art "IEEE transactions on systems, man, and cybernetics, vol. 38, no. 5, September 2008.

BIOGRAPHY

Dipali H. Patil is a Assistant Professor in Information Technology Department of Rajarshi Shahu College of Engineering, Tathawade, Pune. She received Master of Computer Science & Engineering degree in 2011. From Savitribai Phule University, Pune. Her Research interests are Artificial Intelligence, Computer Networks etc.