ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

Secure Two-Level QR Code for Hybrid Document Sharing and Authentication Using Steganography

Gaurav Suresh Yadav, Sanchit Shivajirao Walke, Dhanashree Sambhaji Wadile, Yogesh Shriniwas Rapelli,

Prof R.S.Paswan.

Department of Computer Engineering, Pune Institute of Computer Technology, Pune, India.

ABSTRACT: The QR code was intended for storage data and fast reading applications. The proposed QR code authentication two-level storage is used for to verify original content in QR code. Our proposed work uses public and private storage level of document storage. In the public level similar standard QR code storage level is elaborated; which can be readable to any QR code scanner device. The private level is constructed by replacing the black modules by specific textured patterns. It consists of information encoded using q-ary code with an error correction capacity. Q-array code will increase the storage capacity of the QR code, but also to verify the original document from a copy. This authentication is due to the sensitivity of the used patterns to the print-and-scan process. The novel approach in the pattern recognition method that applied to read the second-level information can be used both in a private message sharing and in a document authentication scenario. Third, the reversible capability inherited from our scheme provides performance which allows recovery of the source texture pattern. We introduce texture synthesis process into steganography for hiding secret in image. The outcomes about demonstrate a perfect restoration of private data. It additionally features the likelihood of utilizing this new rich QR code for document authentication.

KEYWORDS: QR code, two storage levels, Private message, Document authentication, Pattern recognition, Print-and-scan process, Secret Sharing

I. INTRODUCTION

Today graphical codes such as EAN-13 barcode, Quick Response (QR) code, DataMatrix, PDF417, are periodically used in our daily lives. These codes have a vast number of applications including: information storage (advertising, museum art description), redirection to web sites, track and trace (for transportation tickets or brands), identification (flight passenger information, supermarket products) etc. The QR code was invented for the Japanese automotive industry by Denso Wave1 Corporation in 1994. The most important characteristics of this code are small-scale printout size and high speed reading process. Today, 40 QR code versions are available with different storage capacities. The smallest QR code version (version V1) has a 21 × 21 module size. It can store 152 bits of raw data at the lowest correction level. The biggest QR code version (version V40) has a 177 × 177 module size. It can store a maximum of 7089 bits of raw data at its lowest correction level. A QR code encodes the information into binary form. Each information bit is represented by a black or a white module.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

Specific QR code structure

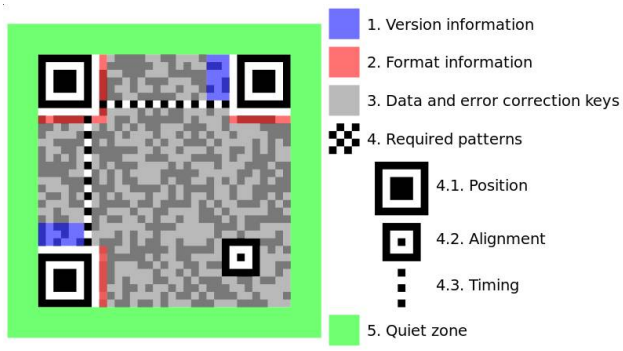

Fig. 1 Specific QR Code Structure.

As represented in Fig. 1, the QR code has a unique structure for geometrical correction and high speed decoding. Three position tags are used for QR code detection and orientation correction. One or more alignment patterns are used to code deformation arrangement. The module get it together is set by timing patterns. Furthermore, the format information areas contain error correction level and mask pattern. The code version and error correction bits are stored in the version information areas.

The popularity of QR codes is primarily due to the following features:

- QR code robust to the copying process,
- It is easy to read by any device and any user,
- It has high encoding capacity enhanced by error correction facilities,
- It is in small size and robust to geometrical distortion.

However, those undoubted advantages also have their counterparts:

i. Information encoded in a QR code is accessible to every user smoothly, even if it is encoded.
ii. It is difficult to classify primary content from duplicate file content due to print and scan feature.
iii. It is impossible to discriminate an originally printed QR code from its copy due to their insensitivity to the Print-and-Scan (P&S) process

II. LITERATURE SURVEY

The paper [1] refers the authentication problem of real-world goods on which 2D bar-codes (2D-BC) were printed and we take the challengers view. The challengers are assumed to have access to noisy copies of an original 2D-BC. A simple estimator of the 2D-BC is depends on copies averages is proposed, letting the challengers print a fake 2DBC with as original by the system detector. Performance of the estimator in terms of error probability at the detector side is then derived with respect to Nc and compared with experimental results on real 2D-BC. It is shown that the adversary can produce a fake that successfully fools the detector with a reasonable number of genuine goods. Advantage: Create a fake 2D-BCs declared as genuine by the detector. Disadvantage: Require additional noise to generate fake barcode. Generating fake 2D QR code declared as original by QR code reader.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

The proposes method in paper [2] for Hiding secret information based on bit technique is so fragile to modification attack. Storing secret data based on bit technique is so yield to modification attack. If an attacker change any bit of hidden bits, it is impossible to recover the secret information. So from this paper, we refer a scheme based on Reed- Solomon codes and List Decoding to overcome this problem. We also conduct our solution by analyzing the complexity, security, and experiment. Advantage: For attacker difficult to find original data Reed-Solomon codes and List Decoding to overcome this problem. In this paper, refer Reed-Solomon codes for encoding content in QR code.

The paper [3] represents no direct connection between devices can exist. Time-multiplexed, 2D colors barcodes are show on screen & recorded with camera embed mobile phones. A Proposed method gives optical data transfer between public displays and mobile devices based on unsynchronized 4D barcodes. We consider that no direct connection between the devices can exist. Time-multiplexed, 2D color barcodes are displayed on screens and recorded with camera equipped mobile phones. This allows transmitting information optically between both devices. Advantage: Maximizes the data throughput and the robustness of the barcode recognition. In this paper, refer Time-multiplexed, 2D color barcodes.

We show properties of the discredited, rescanned image in both the spatial and frequency domains, and then further analyze the changes in the Discrete Fourier Transform (DFT) coefficients. Based on these properties, we show several techniques in paper [4] for extracting invariants from the original and rescanned image, with potential applications in image watermarking and authentication. Advantage: Authentication by image watermarking. Disadvantage: Uses watermarking based authentication. In this paper, Discrete Fourier Transform coefficients and image based authentication is used.

The paper [5] describes the proposed scheme can conceal the secret data into the cover QR code without distorting the readability of QR content. That is, general browsers can read the QR content from the marked QR code for the sake of reducing attention. Only the authorized receiver can encrypt and retrieve the secret from the marked QR code. The secret payload of the designed scheme is adjustable. The scheme can convey larger secret into a QR code according to the selection of the QR version and the error correction level. Advantage: Only the authorized receiver can encrypt and retrieve the secret from the marked QR code. Secret hiding mechanism used for QR code by encrypted payload.

Existing system based on searching relational values between P&S unuseful patterns and related patterns. The storage capacity can be magnificently increased by code alphabet q or by increasing the textured pattern size. Existing system results show a restoration of private information. It also highlights the possibility of using this QR code for document authentication.

In this work, private level constructed by replacing black modules by specific texture pattern. For this existing work uses rich graphical code. Private message are embedded by adding distortion in print and scan technique. These rich graphical codes increase significance by improving aesthetic view of QR code.

Advantage**:**

1. Increase storage capacity of qr code along with differentiate original document.

Disadvantage:

1) Data stored in a QR code is can be easily readable to camera containing, although it is not plain text and therefore is only readable to authorized user ,likewise watch and read. It is impossible to classify an originally document in QR code from its copy due to their insensitivity to the Print and Scan process.

III. PROPOSED SYSTEM APPROACH

The proposed two-level QR (2LQR) code contains of: a first level open for any standard QR code reader, hence it keeps the solid qualities of the QR code; and a second level enhances the limits and attributes of the underlying QR code.

Proposed system uses two levels QR for data hiding. This 2LQR code has following levels

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

1. Public level
2. Private level.

The public level QR code can read text or document easily with reader, but the private level needs a specific device with encoded data. This 2LQR code can be used for private message sharing or for authentication mechanism. The private level is created by replacing black modules with textured patterns from cover image. These textured patterns are considered as black modules by standard QR code reader. So that private level is hidden to QR code readers. Proposed system for private level does not affect in anyway the scanning public data of the public level. The proposed 2LQR code increments the storage capacity of the standardized QR code due to its supplementary reading level. The storage capacity of the two-level QR code can be improved by incrementing the number of textured patterns used or by reducing the textured pattern size.

The use of cover image to hide data, our algorithm hides the source texture image and embeds secret data through the process of texture synthesis. This allows us to extract secret data and the source texture from a steganography.

Advantage:

1. Secure encoding of messages or files.
2. Two level user authentication
3. Text steganography for message/file encoding
4. Stego synthetic texture for QR code hiding

IV. SYSTEM DESIGN

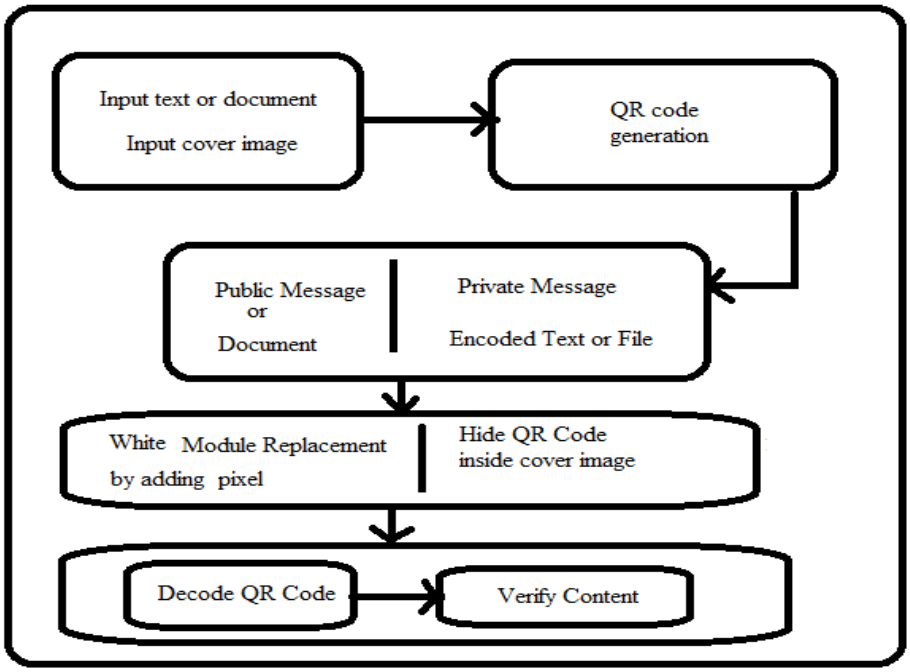

Fig.2. Proposed System Architecture

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

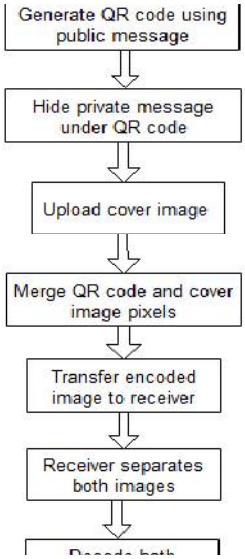

Fig. 3 Flow Chart Diagram

Fig. 3 shows implementation steps of user in project

1. User must have registration first in application.
2. After activation of user account, he/she can login first.
3. Enter Public Message and Private Message for secret data sharing.
4. Generate QR code image with hide public message.
5. Apply Steganography on cover image with hide private message
6. Upload Cover image
7. Merge QR and Cover image pixels
8. Transfer generated image to another user
9. Receiver get merged image and separate into QR and Cover image
10. Decode in reverse process and extract original public and private message
11. Logout

Private Message Storing:-

Let $R = A[x]/(x^n-1)$ be a polynomial ring over a Galois field $A = GF(q)$. The cyclic code C elements are defined with polynomials in R so that the codeword $(c0, c1. . . cn-1)$ maps to the polynomial $c0 + c1x + \cdots + cn-1x^{n-1}$, and the multiplication by x corresponds to a cyclic shift. The code C is generated by a generator polynomial $g(x)$, which is the code polynomial of the minimum degree in a (n, k) cyclic code C. Therefore, the generator polynomial $g(x)$ is a factor of polynomial $xn- 1$.

Let k informative digits of message are represented by a polynomial $m(x)$, of degree, at most $k-1$. Then the codeword $c(x)$ is the polynomial of the form:

$$C(x) = m(x)\, g(x),$$

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

$$C(x) = c0 + c1^{x} + \cdots + cn-1x^{n-1.}$$

Black module replacement:-

The codeword$C_{priv}$is inserted in standard QR code by replacing the black modules with textured patterns $P_1, \ldots, P_q$respecting the codewordC_{priv}, starting from the bottom-right corner. Then, in the case of private message sharing scenario, the textured patterns are placed in the position tags with respect to the chosen permutation σ,. In the case of authentication scenario, the standard position tags keep unchanged black modules,

Patch Extraction:-

We can denote *SP* as the collection of all source patches and *SPn*=||*SP*|| as the number of elements in the set *SP*. We can employ the indexing for each source patch *spi*, i.e., *SP*= {*spi*| *i*= 0 to ||*SP*||-1}. Given a source texture with the size of *Sw*×*Sh*, we can derive the number of source patches *SPn*using

(1) If a kernel block has the size of *Kw*×*Kh*. we assume the size of the source texture is a factor of the size of the kernel block to ease the complexity.

SP_n= (Sw/Kw)*(Sh/Kh)

Our steganographic texture synthesis algorithm needs to generate candidate patches when synthesizing synthetic texture. The concept of a candidate patch is trivial: we employ a window*Pw*×*Ph*and then travel the source texture (*Sw*×*Sh*) by shifting a pixel each time following the scan line order. Let *CP*={*cpi*|*i*=0,1, …, *CPn*-1} represent the set of the candidate patches where*CPn*=||*CP*|| denotes the number of elements in *CP*. We can derive *CPn*using (2).

CPn= ‖CP‖=(S_w-P_w+1)*(S_h-P_h+1)

When generating a candidate patch, we need to ensure that each candidate patch is unique; otherwise, we may extract an incorrect secret message. In our implementation, we employ aflag mechanism. We first check whether the original source texture has any duplicate candidate patches. For a duplicate candidate patch, we set the flag on for the first one. For the rest of the duplicate candidate patches we set the flag off to ensure the uniqueness of the candidate patch in the candidate list.

Algorithms (Required in Editable Format)

Steganography Algorithm:

1) Creating a QR Code

Step 1: Data Analysis
Step 2: Data Encoding
Step 3: Error Correction Coding
Step 4: Structure Final Message
Step 5: Module Placement in Matrix
Step 6: Data Masking
Step 7: Format and Version Information

Encoding:-

Representation of each letter in secret message by its equivalent ASCII code.

- Conversion of ASCII code to equivalent 8 bit binary number.
- Division of 8 bit binary number into two 4 bit parts. Choosing of suitable letters corresponding to the 4 bit parts.
- Meaningful sentence construction by using letters obtained as the first letters of suitable words.
- Omission of articles, pronoun, preposition, adverb, was/were, is/am/are, has/have/had, will/shall, and would/should in coding process to give flexibility in sentence construction.
- Encoding is not case sensitive.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

Decoding

Steps:

- First letter in each word of cover message is taken and represented by corresponding 4 bit number.
- 4 bit binary numbers of combined to obtain 8 bit number.
- ASCII codes are obtained from 8 bit numbers.
- Finally secret message is recovered from ASCII codes.

2) Algorithm for embedding data inside image.

Input: Input_Image, Secret_Message, Secret_Key;
Output: Stego_Image;
Process:
Step1: Begin
Step2: Transfer Secret_Message into Text_File;
Step3: Zip Text_File;
Step4: Convert Zip_Text_File to Binary_Codes;
Step5: Convert Secret_Key into Binary_Codes;
Step6: Set BitsPerUnit to Zero;
Step 7: Encode Message to Binary_Codes;
Step 8: Add by 2 unit for bitsPerUnit;
Step 9: Display Stego_Image;
Step 10: End

3) Algorithm for extracting data from stego image.

Input: Stego_Image, Secret_Key;
Output Secret_Message;
Process:
Step1: Begin
Step2: Compare Secret_Key;
Step3: Calculate BitsPerUnit;
Step4: Decode All_Binary_Codes;
Step5: Shift by 2 unit for bitsPerUnit;
Step6: Convert Binary_Codes to Text_File;
Step 7: Unzip Text_File;
Step 8: Display Secret_Message;
Step 9: End

VI. EXPERIMENTAL RESULT

QR code security with reversible texture steganography by extracting patches from cover image pixels.
Message Encoding:-

In message encoding user provides public and private information to securely transfer digitally across the media. Here proposed system hide this information in standard QR code by scrambling secret information by text steganography. Text steganography uses REED Solomon Code for data encoding, where random bit of character are added as noise to data to be transfer between digital media.

Message encoding scheme graph computes time required for steganography in Reed Solomon algorithm. This is time computation in milliseconds. Time is measured for bit shifting and adding noise into original data.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

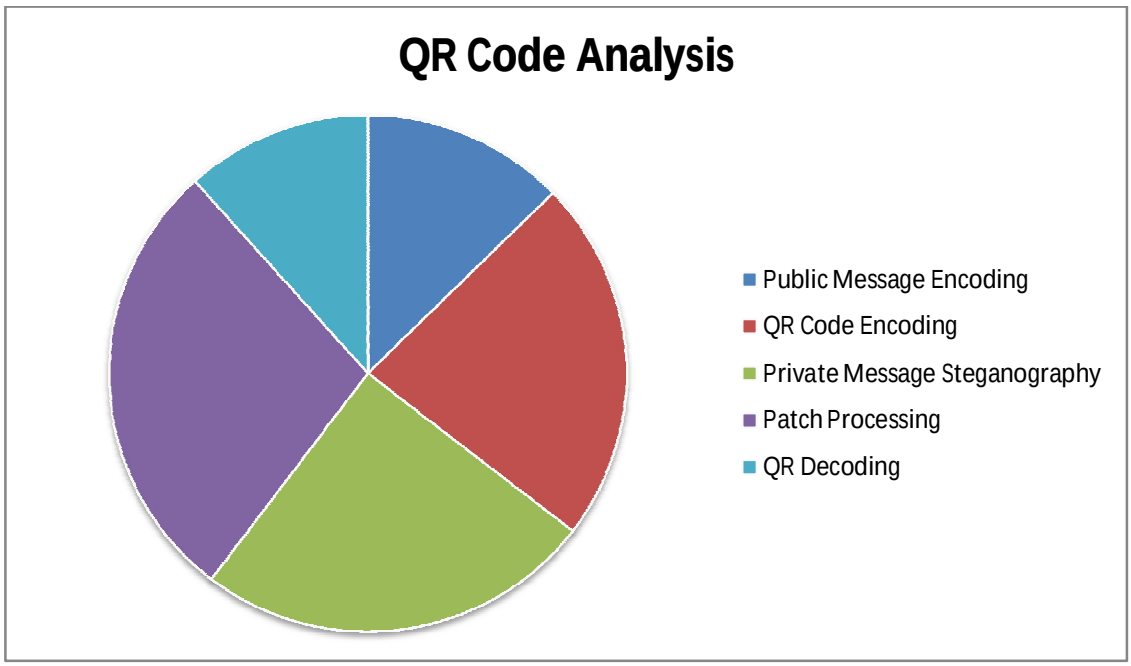

Fig.3 QR code analysis graph

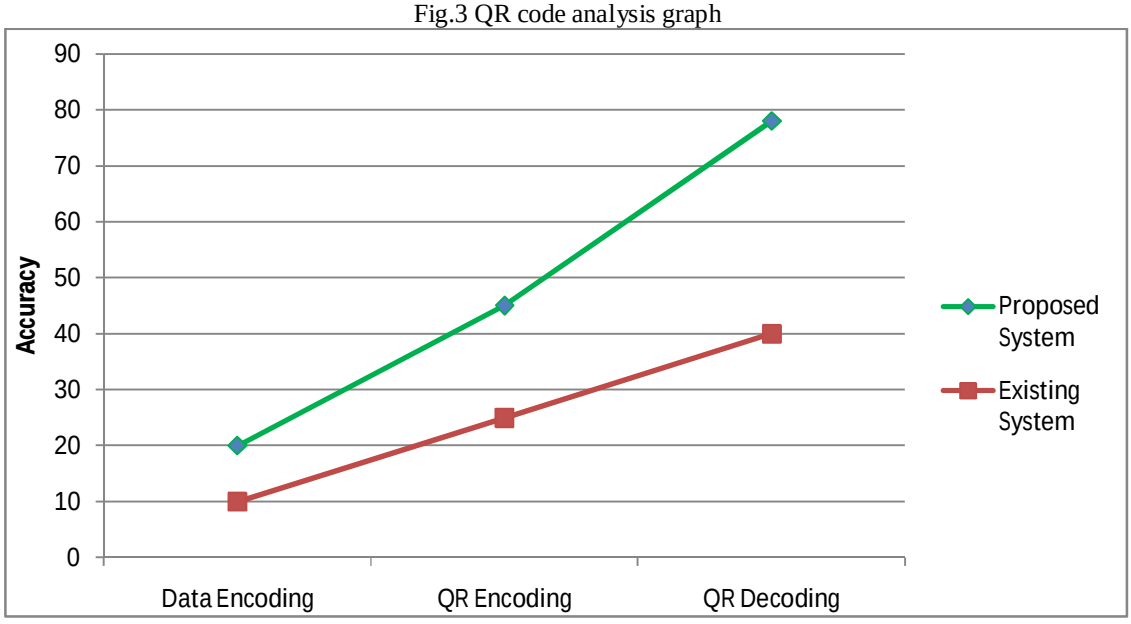

Fig. 4 Comparison graph of accuracy between existing and proposed system

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

Comparison graph shows data encoding, QR Code encoding, and QR Decoding in comparison with existing system values threshold.

This computation for accuracy range is assumed to assign weight for each level for proposed system i.e. data encoding rate and QR code encryption level and QR authentication i.e. QR decoding.

VII. CONCLUSION

This 2LQR code can be used for secure private data sharing for authentication mechanism. The private level is created by replacing black modules with specific textured patterns. Image texture patterns are considered as black modules by QR code reader. So that the private level is hidden to QR code readers, we add the private level which does not affect in anyway the reading process of the public level. The proposed 2LQR code increases the storage capacity of the classical QR code due to its supplementary reading level. The storage capacity of the 2LQR code can be improved by increasing the number of textured patterns used or by decreasing the textured pattern size. All experiments show that even with a pattern size of 6×6 pixels and with an alphabet dimension $q = 8$, it is possible to obtain good pattern recognition results, and therefore a successful private message extraction. However, we are facing a trade-off between the pattern size, the alphabet dimensions and the quantity of stored information during the 2LQR code generation.

REFERENCES

[1] C. Baras and F. Cayre, "2D bar-codes for authentication: A security approach," in Proc. 20th Eur. Signal Process. Conf. (EUSIPCO), Aug. 2012, pp. 1760–1766.
[2] 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. Intell. Inf. Hiding Multimedia Signal Process. (IIH-MSP), Aug. 2014, pp. 520–523.
[3] T. Langlotz and O. Bimber, "Unsynchronized 4D barcodes," in Proc. 3rd Int. Symp., ISVC 2007, Lake Tahoe, NV, USA, Nov. 26–28, 2007, pp. 363–374.
[4] C.-Y. Lin and S.-F. Chang, "Distortion modeling and invariant extraction for digital image print-and-scan process," in Proc. Int. Symp. Multimedia Inf. Process., 1999, pp. 1–10.
[5] 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.