ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

A Survey on Two-Level QR Code for Private Message Sharing and Document Authentication Using Steganography

Harshada Jahagirdar[1], Himangi Jalgaonkar[2], Madulika Chaudhari[3], Anjali[4], Ila Savant[5]

Department of Computer Science, SPPU, Pune, India[1,2,3,4]

Assistant Professor, Marathwada Mitra Mandal's College of Engineering, SPPU, Pune, India[5]

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. Steganalytic algorithm is not likely to defeat our steganographic approach. Third, the reversible capability inherited from our scheme provides functionality which allows recovery of the source texture. We weave 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

I. INTRODUCTION

Today graphical codes such as EAN-13 barcode, Quick Response (QR) code, Data Matrix, PDF417, are frequently used in our daily lives. These codes have a huge 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 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): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

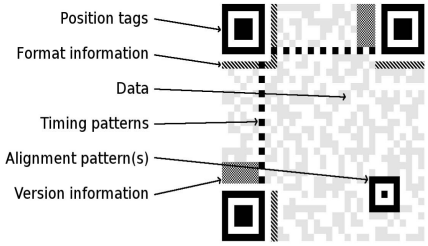

Fig. 1 Specific QR Code Structure

As illustrated in Fig. 1, the QR code has a specific 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 adjustment. The module coordinates are 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 mainly 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 undeniable advantages also have their counterparts:

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

II. LITERATURE SURVEY

AUTHENTICATION SECURITY APPROACH, from [1] system we refer the authentication problem of real-world goods on which 2D bar-codes (2D-BC) were printed and we take the competitors view. The competitors 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 competitors 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 opponent 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.

Unsynchronized 4D Barcodes Coding and Decoding Time-Multiplexed 2D Colorcodes, Proposes 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 [2] 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.

Distortion Modeling and Invariant Extraction for Digital Image Print-and-Scan Process, We show properties of the discredited, rescanned image in both the spatial and frequency domains, and then further analyze the changes in the

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

Discrete Fourier Transform (DFT) coefficients. Based on these properties, we show several techniques [3] 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.

Tamper-proofing of Electronic and Printed Text Documents via Robust Hashing and Data-Hiding, In [4] paper, we deal with the problem of authentication and tamper-proofing of text documents that can be distributed in electronic or printed forms. We advocate the combination of robust text hashing and text data- hiding technologies as an efficient solution to this problem. First, we consider the problem of text data-hiding in the scope of the Gel'fand-Pinsker data-hiding framework. For illustration, two modern text data-hiding methods, namely color index modulation (CIM) and location index modulation (LIM), are explained. Second, we study two approaches to robust text hashing that are well suited for the considered problem. In particular, both approaches are compatible with CIM and LIM. The first approach makes use of optical character recognition (OCR) and a classical cryptographic message authentication code (MAC). The second approach is new and can be used in some scenarios where OCR does not produce consistent results. Advantage: robustness against typical intentional/unintentional document Disadvantage: does not produce consistent results.

Steganography Using Reversible Texture Synthesis, The paper [5] proposes a novel approach for steganography using a reversible texture synthesis. A texture synthesis process re-samples a smaller texture image which synthesizes a new texture image with a similar local appearance and arbitrary size. We weave the texture synthesis process into steganography to conceal secret messages. In contrast to using an existing cover image to hide messages, our algorithm conceals the source texture image and embeds secret messages through the process of texture synthesis. This allows us to extract secret messages and the source texture from a stego synthetic texture.

III. PROPOSED ARCHITECTURE

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

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 information. 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, Propose system for private level does not affect in anyway the scanning public data 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.

Cover image to hide messages, our algorithm hide the source texture image and embeds secret messages through the process of texture synthesis. This allows us to extract secret messages and the source texture from a stego synthetic texture.

Advantages:

1. Secure encoding of document or text.
2. Two level user authentication
3. Text steganography for message encoding
4. stego synthetic texture for QR code hiding

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

IV. SYSTEM ARCHITECTURE

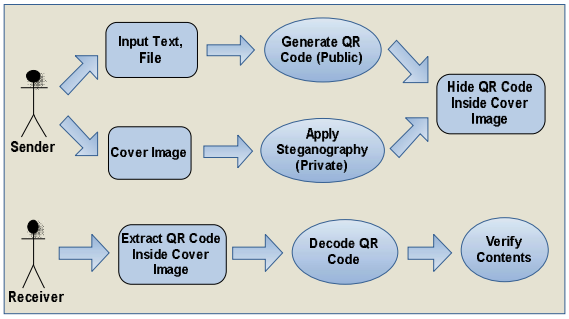

Fig.2. Proposed System Architecture

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:

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

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 codeword C_{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., $SP= \{spi| i= 0 \text{ to } \|SP\|-1\}$. Given a source texture with the size of $Sw \times Sh$, we can derive the number of source patches SPn using

(1) If a kernel block has the size of $Kw \times Kh$. 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 $Pw \times Ph$ and then travel the source texture $(Sw \times Sh)$ by shifting a pixel each time following the scan line order. Let $CP=\{cpi|i=0,1, \ldots, CPn-1\}$ 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 a flag 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.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

Algorithms-

1)Creating a QR Code: Part 1

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: Part 2

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

1. Conversion of ASCII code to equivalent 8 bit binary number.
2. Division of 8 bit binary number into two 4 bit parts. Choosing of suitable letters corresponding to the 4 bit parts.
3. Meaningful sentence construction by using letters obtained as the first letters of suitable words.
4. 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.
5. Encoding is not case sensitive.

Decoding: Part 3

Steps:

1. First letter in each word of cover message is taken and represented by corresponding 4 bit number.
2. 4 bit binary numbers of combined to obtain 8 bit number.
3. ASCII codes are obtained from 8 bit numbers.
4. 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;

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

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

V. 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. 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.
[3] 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.
[4] R. Villán, S. Voloshynovskiy, O. Koval, F. Deguillaume, and T. Pun, "*Tamper-proofing of electronic and printed text documents via robust hashing and data-hiding*," in Proc. SPIE, vol. 6505, p. 65051T, Feb. 2007.
[5] S. V. Voloshynovskiy, O. Koval, F. Deguillaume, and T. Pun, "*Visual communications with side information via distributed printing channels: Extended multimedia and security perspectives*," Proc. SPIE, vol. 5306, pp. 428–445, Jun. 2004.