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

Providing Security for Private Data Sharing and File Authentication using Two-Level QR Code

Priyanka S. Patil[1], Prof. Priya Parate [2]

Department of Computer Engineering, Rajiv Gandhi Institute of Technology, Mumbai, India[1]

Department of Computer Engineering, Rajiv Gandhi Institute of Technology, Mumbai, India[2]

ABSTRACT: The proposed work uses public and private storage level of document storage. To provide secured encoding and secured user authentication, the QR code authentication with two level storage and security is proposed, which help to verify original content in QR code. In the public level same standard QR code storage level is explored; which can be readable to any QR code readable device. The private level is constructed by replacing the black modules by specific textured patterns. It consists of information encoded using QR code with an error correction capacity. QR 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 pattern recognition method that we use to read the second-level information can be used both in a private message sharing and in an authentication scenario. For message encoding text steganography is used.

KEYWORDS: Document Authentication, QR Code, Two Storage Levels, Private Message, Pattern Recognition, Print-And-Scan Process.

I. INTRODUCTION

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.

The use of QR codes is increased because they are robust to the copying process, easy to read by any device and any user, they have a high encoding capacity enhanced by error correction facilities, they have a small size and are robust to geometrical distortions.

Specific QR code structure:

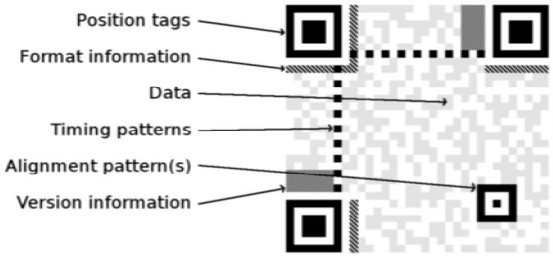

Fig 1: Specific QR code structure

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

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.

However, those undeniable advantages also have their counterparts:

- Information encoded in a QR code is accessible to every user easily, even if it is encoded.
- It is difficult to classify original content from duplicate file content due to print and scan feature.
- 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

To overcome this, proposed work is beneficial so that this drawback is overcome and man-in-middle attack is not possible also as all the communication is encrypted. Two levels QR code motivate for private message sharing and document security authorization.

The proposed two level QR (2LQR) code contains of:

- The first level accessible for any standard QR code reader, therefore it keeps the strong characteristics of the QR code;
- The second level that improves the capacities and characteristics of the initial QR code.

The information in the second level is encoded by using q−ary ($q \geq 2$) code with error correction capacities. This information is invisible to the standard QR code reader because it perceives the textured patches as black modules. Therefore, the second level can be used for private message sharing. The second level can be used to distinguish the original 2LQR code from its copies.
Steganography is a singular method for information hiding techniques. It embeds messages into a host medium in order to conceal secret messages so as not to arouse suspicion by an eavesdropper. In general, the host medium used in steganography includes meaningful digital media such as digital image, text, audio, video, 3D model, etc. There are number of image steganographic algorithms have been proposed with the increasing popularity and use of digital images. Most image steganography algorithms uses an existing image as a cover medium. The expense of embedding secret messages into this cover image is the image distortion encountered in the stego image.

II. RELATED WORK

In [1], C. Baras and F. Cayre, "2D standardized identifications for verification: A security approach," in Proc. twentieth Eur. Flag Process. Conf. (EUSIPCO), Aug. 2012, pp. 1760–1766.

From this framework they allude the confirmation issue of genuine merchandise on which 2D standardized identifications (2D-BC) were printed and taken the contenders see. The contenders are expected to have entry to uproarious duplicates of a unique 2D-BC. A straightforward estimator of the 2D-BC is relies on upon duplicates midpoints is proposed, giving the contenders a chance to print a fake 2DBC with as unique by the framework indicator. Execution of the estimator regarding mistake likelihood at the identifier side is then inferred as for Nc and contrasted and test comes about on genuine 2D-BC. It is demonstrated that the adversary can deliver a fake that effectively tricks the identifier with a sensible number of certifiable products. [1]

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

In [2], T. V. Bui, N. K. Vu, T. T. P. Nguyen, I. Echizen, and T. D. Nguyen, "Powerful message covering up for QR code," in Proc. IEEE tenth Int. Conf. Intell. Inf. Concealing Multimedia Signal Process. (IIH-MSP), Aug. 2014, pp. 520–523.
Putting away mystery information in view of bit method is so respect alteration assault. In the event that an aggressor change any piece of shrouded bits, it is difficult to recuperate the mystery data. So from this paper, alluded a plan in view of Reed-Solomon codes and List Decoding to defeat this issue. The work additionally leads our answer by investigating the intricacy, security, and examination.

In [3], T. Langlotz and O. Bimber, "Unsynchronized 4D scanner tags," in Proc. third Int. Symp., ISVC 2007, Lake Tahoe, NV, USA, Nov. 26–28, 2007, pp. 363–374.
A Proposed technique gives optical information exchange between open showcases and cell phones in light of unsynchronized 4D standardized identifications. This work considers that no immediate association between the gadgets can exist. Time-multiplexed, 2D shading standardized tags are shown on screens and recorded with camera prepared cell phones. This permits transmitting data optically between both devices.

In [4], C.- Y. Lin and S.- F. Chang, "Contortion displaying and invariant extraction for computerized picture print-and-sweep handle," in Proc. Int. Symp. Interactive media Inf. Handle., 1999, pp. 1–10.
They indicate properties of the defamed, rescanned picture in both the spatial and recurrence areas, and afterward additionally dissect the adjustments in the Discrete Fourier Transform (DFT) coefficients. In view of these properties, they demonstrate a few systems for removing invariants from the first and rescanned picture, with potential applications in picture watermarking and confirmation.

In [5], P.- Y. Lin, Y.- H. Chen, E. J.- L. Lu, and P.- J. Chen, "Mystery concealing system utilizing QR standardized tag," in Proc. IEEE Int. Conf. Flag Image Technol. Web Based Syst. (SITIS), Dec. 2013, pp. 22–25.
They composed a mystery concealing procedure for QR scanner tag. The proposed plan can hide the mystery information into the cover QR code without bending the decipherability of QR substance. That is, general programs can read the QR content from the stamped QR code for lessening consideration. Just the approved beneficiary can scramble and recover the mystery from the stamped QR code. The mystery payload of the composed plan is customizable. The plan can pass on bigger mystery into a QR code as per the choice of the QR rendition and the blunder revision level.

In [6], M. Querini, A. Grillo, A. Lentini, and G. F. Italiano, "2D shading standardized tags for cell phones," Int. J. Comput.Sci. Appl., vol. 8, no. 1, pp. 136–155, 2011.
They utilized high limit shading standardized identification, which utilize hues to build the scanner tag information thickness. The recognizable proof and acknowledgment of hued modules represents some new and non-paltry PC vision difficulties, for example, taking care of the shading bends presented by the equipment gear that understands the Print &Scan prepare.

In [7], K. Solanki, U. Madhow, B. S. Manjunath, S. Chandrasekaran, and I. El-Khalil, "'Print and output' flexible information covering up in pictures," IEEE Trans. Inf. Crime scene investigation Security, vol. 1, no. 4, pp. 464–478,Dec. 2006.
This paper proposes strategies to shroud data into pictures that accomplish power against printing and checking with visually impaired interpreting. The particular inserting in low frequencies plot conceals data in the greatness of chose low-recurrence discrete Fourier change coefficients. The differential quantization list tweak plot installs data in the stage range of pictures by quantizing the distinction in period of contiguous recurrence areas. A critical commitment of this paper is expository and trial demonstrating of the print-filter handle, which shapes the premise of the proposed inserting plans.

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

In [8], R. Villán, S. Voloshynovskiy, O. Koval, F. Deguillaume, and T. Play on words, "Sealing of electronic and printed content archives by means of hearty hashing and information covering up," in Proc. SPIE, vol. 6505, p. 65051T, Feb. 2007.

In this paper, they manage the issue of validation and sealing of content reports that can be disseminated in electronic or printed shapes. They advocate the blend of vigorous content hashing and content information concealing innovations as a proficient answer for this issue. Initially, they consider the issue of content information stowing away in the extent of the Gel'fand-Pinsker information concealing structure. For delineation, two present day content information concealing techniques, to be specific shading file tweak (CIM) and area record regulation (LIM), are clarified. Second, they concentrate two ways to deal with strong content hashing that are appropriate for the considered issue. Specifically, both methodologies are good with CIM and LIM. The principal approach makes utilization of optical character acknowledgment (OCR) and a traditional cryptographic message validation code (MAC). The second approach is new and can be utilized as a part of a few situations where OCR does not deliver reliable results.

In [9], Kuo-Chen Wu and Chung-Ming Wang, Member, IEEE, "Steganography Using Reversible Texture Synthesis", Ieee Transactions On Image Processing Vol: 24 No: 1 Year 2015

They propose a novel approach for steganography utilizing a reversible surface union. A surface union process re-tests a littler surface picture which combines another surface picture with a comparable nearby appearance and subjective size. They mesh the surface blend handle into steganography to disguise mystery messages. Rather than utilizing a current cover picture to shroud messages, our calculation hides the source surface picture and installs mystery messages through the procedure of surface union. This enables us to concentrate mystery messages and the source surface from a stego engineered surface.

III. MOTIVATION AND OBJECTIVE

The motivation of this work is to propose the storage capacity can be significantly improved by increasing the code alphabet *q* or by increasing the textured pattern size. The experimental results show a perfect restoration of private information. It also highlights the possibility.

Growing online media usage with one time password which is send to user mobile so any one can hack the information in between transaction. To overcome this proposed work use the QR code so this drawback is overcome man-in-middle attack is not possible as all the communication is encrypted. Two levels QR code motivate for private message sharing and document security authorization. QR codes is featured because they are strong to the copying data and easy for reading with any device and any user, they have a high encoding capacity enhanced by error correction facilities, they have a small size and are robust to geometrical distortions.

Although it has some advantages and some disadvantage.

1. Information encoded in a QR code is always accessible to everyone, even if it is ciphered and therefore is only easily readable to authorized users just like see and understand.
2. QR code is unable to distinguish original document content over duplicate copy of encoded document. To overcome this drawback this work motivate to standard QR code encoding capacity

IV. PROPOSED SYSTEM MECHANISM

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.

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 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 thatprivate level is hidden to QR code readers, Propose system for private level does not affect in anyway the scanningpublic 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 oftextured patterns used or by decreasing the textured pattern size.

Mathematical Model for Proposed Work:

Let us consider S as a set of document and text to encode in QR code.
S= { }
INPUT:

- Identify the inputs as text and document file.

F= {f_1, f_2, f_3 ……,f_n| 'F' as set of functions to execute to similar image retrieval}
I= {i_1, i_2, i_3…|'I' sets of inputs to the function set}//Code book entry, query image, dataset images
O= {o_1, o_2, o_3….|'O' Set of outputs from the function sets}//Similar Type images
S= {I, F, O}
I = {Document, text}
O = {QR Code}
F = {Encode, compress, decode, decompress}
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 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., $SP= \{spi| i= 0 \text{ to } ||SP||-1\}$. Given a source texture with the size of $Sw \times Sh$, we can derive the number of source patches SPnusing

I. 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 CPnusing (2).
$CPn= ||CP||=(S_w-P_w+1)*(S_h-P_h+1)$

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

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.

V. PROPOSED SYSTEM ARCHITECTURE

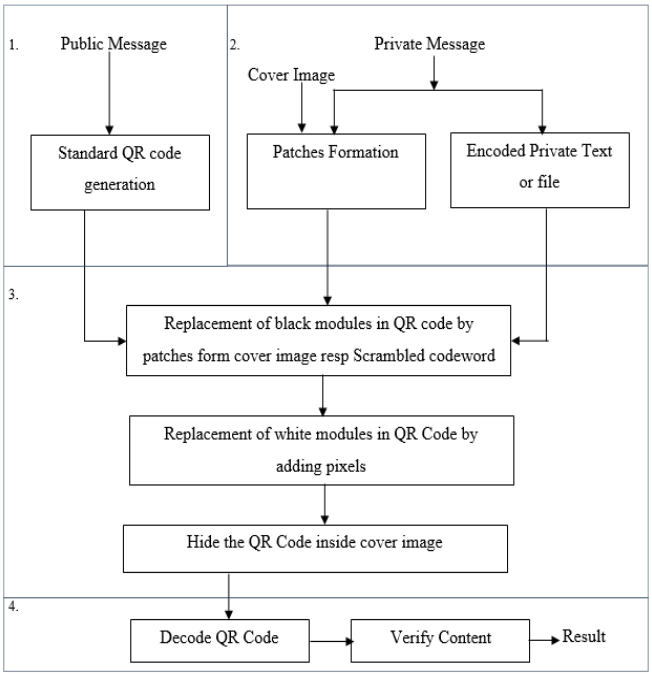

Fig 2: Proposed System Architecture

VI. ADVANTAGES

- It provides secure encoding of document or text.
- It provides two level user authentications.
- It provides text Steganography for message encoding.
- It provides Stego synthetic texture for qr code hiding.

VII. PERFORMANCE MEASURES

Performance measure of the proposed approach and the security system is done based on Precision measure. Precision is the basic measure used in evaluating security strategies. It is the ratio of number of relevant authorizations to the total number of irrelevant and relevant authorizations. It is usually expressed as percentage.
Precision measure is calculated based on the following formula.

$$\text{Precision} = \frac{tp}{tp + fp}$$

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

Where,
tp – True Positive (Correct result)
fp – False Positive (Unexpected Result)

Performance of the system:

Different Methods	tp	fp	Precision
Existing QR method	2	8	0.2
Proposed 2 level QR method	9	0	1

Table 1: Precision Measure

From the table 1, it is understood that precision of the Existing method is 0.2 and the precision of Proposed method is 1 out of 1. The results of the performance measure are plotted in Figure 2.

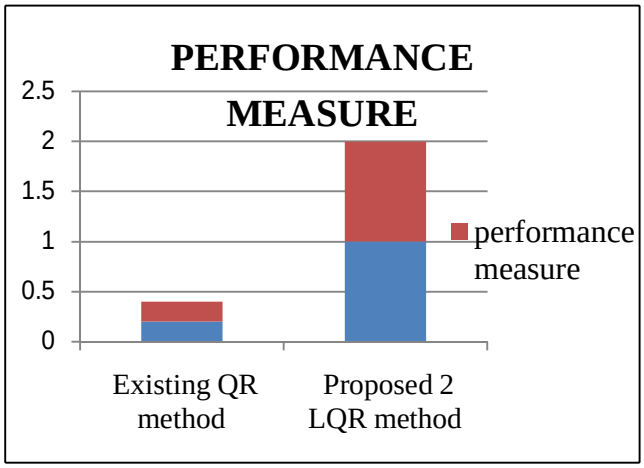

Fig 3: Performance Measure

VIII. COMPARISON BETWEEN EXISTING AND PROPOSED WORK

Existing System:

- 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.
- 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.

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

Proposed System:

- This 2LQR code can be used for private message sharing or for authentication mechanism.
- 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.
- 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.

IX. RESULT TABLE

Proposed system uses Cover image for patch processing in QR image. Where, reverse texture steganography is used. While decoding the QR image Re synthesis of cover image patches is applied.

Attribute	**Existing System**	**Proposed System**
Pattern	Textured Pattern	Patches from cover image
Code word	Reed Solomon- ECC	Patch synthesis-composition

Proposed system is designed by implementing accuracy by enhancing QR Code security by adding colour code combination in QR image.

X. 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.

XI. FUTURE SCOPE

1. Improve pattern recognition by supervised learning QR code image.
2. Image Steganography for patch processing
3. Cover the textured pattern analysis to automate its combination process for QR code.
4. Recover message from QR code by cropping and reconstructing
5. Replacing white modules with additional pixel.
6. Apply cover image over generated QR code.
7. Using QR code for payment transfer application
8. Study of the second level recovery problems in the 2LQR code images captured by a camera.

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

9. The storage capacity of 2LQR code will be increased by replacing also the white modules with textured patches.

ACKNOWLEDGMENT

I would like to express my gratitude and appreciation to all those who helped me to complete this paper. A special thanks to my guide, **Prof. Priya Parate** whose help, stimulating suggestions and encouragement helped me in writing this paper.

REFERENCES

[1] C. Baras and F. Cayre, "2D bar-codes for authentication: A securityapproach," 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 extractionfor digital image print-and-scan process," in Proc. Int. Symp. MultimediaInf. Process., 1999, pp. 1–10.
[5] P.-Y. Lin, Y.-H. Chen, E. J.-L. Lu, and P.-J. Chen, "Secret hidingmechanism using QR barcode," in Proc. IEEE Int. Conf. Signal-ImageTechnol. Internet-Based Syst. (SITIS), Dec. 2013, pp. 22–25.
[6] M. Querini, A. Grillo, A. Lentini, and G. F. Italiano, "2D color barcodesfor mobile phones," Int. J. Comput. Sci. Appl., vol. 8, no. 1, pp. 136–155,2011.
[7] K. Solanki, U. Madhow, B. S. Manjunath, S. Chandrasekaran, andI. El-Khalil, "'Print and scan' resilient data hiding in images,"IEEE Trans. Inf. Forensics Security, vol. 1, no. 4, pp. 464–478,Dec. 2006.
[8] R. Villán, S. Voloshynovskiy, O. Koval, F. Deguillaume, and T. Pun,"Tamper-proofing of electronic and printed text documents via robusthashing and data-hiding," in Proc. SPIE, vol. 6505, p. 65051T,Feb. 2007.
[9] 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.
[10] IuliiaTkachenko" Two-Level QR Code for Private Message Sharing and Document Authentication" IEEE Transactions On Information Forensics And Security, Vol. 11, No. 3, March 2016.