SECURED MESSAGE TRANSFER THROUGH QRCODE ENCRYPTION

Dr S Sadesh[1],Aananthavalli S[2],Karthika R[3],Kavin kumar S[4],Leena Devi R[5]

[1]Assistant Professor(Sr.Gr),Velalar College of Engineering and Technology, Thindal, TamilNadu.

[2]B.E student, Dept. of Computer Science, Velalar College of Engineering and Technology, Thindal, Tamil Nadu.
[3]B.E student, Dept.of Computer Science, Velalar College of Engineering and Technology, Thindal, Tamil Nadu.
[4]B.E student, Dept.of Computer Science, Velalar College of Engineering and Technology, Thindal, Tamil Nadu.
[5]B.E student, Dept. of Computer Science, Velalar College of Engineering and Technology, Thindal, Tamil Nadu.

ABSTRACT

The Quick Response QRcode is designed for storage information and high-speed reading applications. This two level QRcode (2LQR), has public and private storage levels. The first level is the same as the standard QRcode storage level. Therefore it is readable by any classical QRcode application. The private level is modified with black modules consists of specific textured patterns. It consists of information encoded using q-ary code with an error correction capacity. This allows us to increase the storage capacity of the QRcode as well as to distinguish the original document from a copy. The pattern recognition method can be used in a private message sharing. It also highlights the possibility of using this QRcode for document authentication.

Keywords— QRcode, 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 websites, track and trace (for transportation tickets or brands), etc. The popularity of these codes is mainly due to the following features: they are robust to the copying process, easy to read on 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. However, those advantages also have their counterparts:

1) QR code containing information is ciphered and hence it is legible only to authorized users.

2) 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. RELATED WORK

Two level QR (2LQR) code consists of first level accessible for any standard QR code reader. Therefore it keeps the characteristics of the QR code and a second level that improves the capacities and characteristics of the initial QRcode. This information is invisible to the standard QR code reader because it perceives the textured patterns as black modules. Therefore, the second level will be used for private message sharing.

1.QRcode features

The QRcode was invented for the Japanese automotive industry by Denso Wave1corporation in 1994. The most important features are small printout size and high-speed reading process. A QRcode encodes the information into a binary form. A black or a white module represents the each information bit. For data encryption, Reed-Solomon error correction code is used. Therefore, one of 4 error correction levels has to be chosen during QRcode generation. The lowest level can restore nearly 7% of the damaged information; the highest level can restore nearly 30%. Today, 40 QRcode versions are available with different storage capacities. The smallest QRcode version (version V1) has a 21 × 21 module size. It can store 152 bits of raw data at the lowest correction level. The biggest QRcode 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.

2. Rich graphical codes

Several rich graphics have been introduced to improve the graphical code properties. These are rich graphical codes that aim to produce visual significance, to personalize the stored information or to maximize the storage capacities. It consists of changing the colors and shape of the modules, or of adding an image into the QRcode. Free or paid applications are proposed by different design QRcode generators. However, most of these generators prefer to sacrifice the possibility of error correction for attractive design. The QRcode adds the significance without losing error correction capacity. We proposed a method which modifies the QRcode source pixels so that the white (rsp. black) module pixels are transformed from white (rsp. black) to any RGB values and whose luminance value is considered as white (rsp. black) pixel by blending a color image into the QR code.

III.OUR CONTRIBUTION

1.PROFILE GENERATION USING QRCODE BASED REGISTRATION

In social network, we have to begin by creating an ID to interact with other users. We have to maintain our profile by providing our personal background, hobbies, contacts, places they have been to, etc. Profile matching is a useful way to find new friends with mutual interests and to find lost connections or to search for experts. Some applications help a user automatically find users with similar profile within a certain distance. These applications use profiles to facilitate friending between proximate strangers and enable privacy-preserving people searching to some extent. In this module, the user's profile will be gathered, and it will be stored in the database. The user's profile will be noted gathering the personal. The public and the personal details will be kept secret. Friending and communication are two essential functions of social networks.

Friending is mainly based on private profile matching. There are two mainstreams of approaches to solve this problem. The first category treats a user's profile as a set of attributes and provides private attributes matching based on private set intersection (PSI) and private cardinality of set intersection. The second category considers a user's profile as a vector and measures the social proximity by private vector dot product.

2. QRcode Based Key Generation

The initiator will start the process by sending a profile request to the matching user of him/her. The request profile is a set of sorted attributes. Then we hash the attributes of the profile one by one to produce a profile vector. A profile key is generated based on the profile using some publicly known hashing function. The initiator will

encrypt the secret message using the profile key. A remainder vector of the profile vector is yield for fast exclusion of a huge portion of unmatched persons. To support a flexible fuzzy search requiring no perfect match, the initiator can define the necessary attributes, optional attributes and the similarity threshold of the matching profile. And a hint matrix is constructed from the request profile vector according to the similarity definition, which enables the matching person to recover the profile key. In the end, the initiator packs the encrypted message, the remainder vector and the hint matrix into a request package and sends it out.

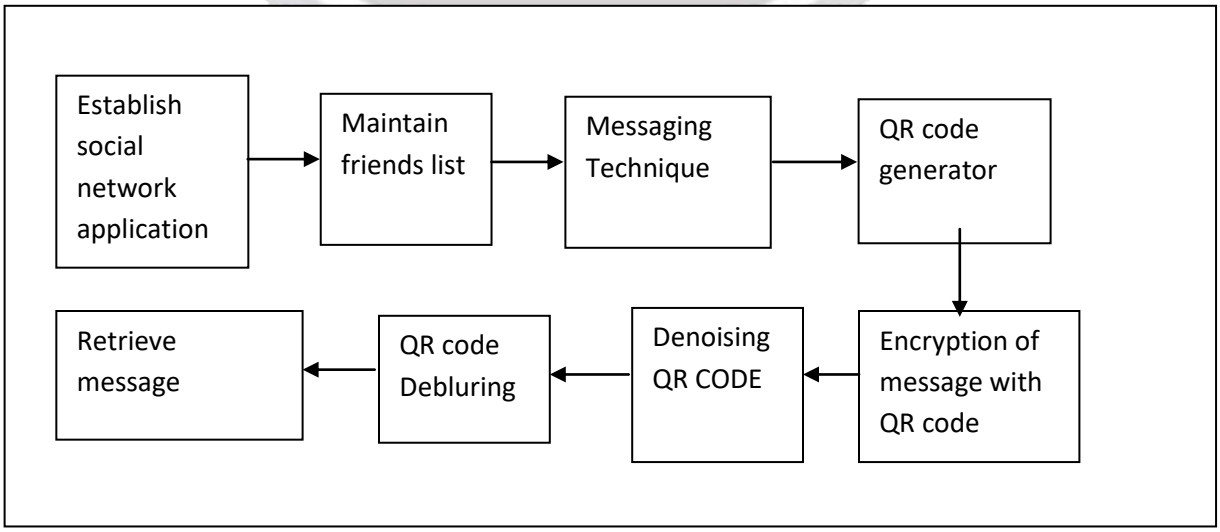
3. Deblurring And Denoising Technique Implementation

We proposed a protocol to address the privacy preserving profile matching and secure communication channel establishment in decentralized system without any presetting or trusted third party. We take advantage of the common attributes between matching users, and use it to encrypt a message with a secret channel key in it. In principle our method extends to blind deblurring and denoising of any class of images for which a part of the image is a priori known. We focus on QR bar codes because they present a canonical class of ubiquitous images possessing this property, their simple binary structure of blocks lends itself well to a simple anisotropic regularization, and software is readily available to both generate and read QR bar codes, providing a simple and unambiguous way in which to assess our methods. In our mechanisms, only a matching user can decrypt the message that contains this QRcode. A privacy-preserving profile matching and secure channel construction are completed simultaneously with only one round of communication. The secure channel construction resists the man-in-the-middle (MITM) attack by any unmatched users. Both precise and fuzzy matching/search in a flexible form are supported. A sequence of well-designed schemes make our protocols practical, flexible and lightweight, e.g., a remainder vector is designed to significantly reduce the computation and communication overhead of unmatched users. Our profile matching mechanisms are also verifiable which thwart cheating about matching result. We also design a mechanism for location privacy preserved vicinity search based on our basic scheme.

4.Extraction Of Message After Denoising And Deblurring

Now a person have sent a message in an encrypted format using QRCODE. It will contains noise and blur signal. So it will reach the receiver. After the denoising and deblurring of image has been performed, the sender's message will be decrypted and it will be retrieved by the receiver. Also after he reads the message, he will send reply to his friend using same technique using QRCode which can be decrypted on the other side to read.

Architecture



IV.Implementation Techniques

Ridgelet Image Denoising

The ridgeletdenoising is used to recover the original signal from the noisy one by removing the noise.In contrast with denoising methods that simply smooth the signal by preserving the low frequency content and removing the high frequency components, the frequency contents and characteristics of the signal would be preserved during ridgelet denoising.It maps the line singularities into point singularities by employing the embedded transform. Therefore, the wavelet transform can efficiently be applied to discover the point singularities in this new domain.Having the ability to approximate singularities along a line, several terms with common ridge lines can effectively be superposed by the ridgelet transform.

Algorithm Example:

To explain the ridgelet denoising procedure, assume I[i,j] to be the original M by M image, where i and j = 1, 2,…, M, and S[i,j] = I[i,j] + n[i,j] is the image corrupted by additive noise n[i,j] which is identically distributed and independent of I[i,j]. In the first step of ridgelet denoising, the observed image S is transformed into the ridgelet domain.Then the ridgelet coefficients are thresholded and finally the denoised coefficients are transformed back to reconstruct the image. Let RD and RR be the forward ridgelet decomposition and inverse ridgelet reconstruction transforms. Assume T and τ to be the thresholding operator and threshold respectively. Threshold value will be defined using point spread function.

Cross-validation methods

Cross-validation methods attempt to directly estimate the extra-sample prediction error in a nonparametric, data-driven way. Cross-validatory techniques for model selection are very general, in the sense that they can be used with any loss function L or nonlinear model generator, unlike other approaches to model selection whose applicability is typically restricted to quadratic loss and linear model settings.Therefore cross-validation is particularly appropriate for scale selection in our context of denoising by nonlinear diffusion under arbitrary loss function. Note, however, that for cross validation techniques to work well in our problem, it is important that the noise elements Ni at different pixels are uncorrelated. For example, if noise at neighboring pixels is positively correlated, then models selected by unadapted cross-validation tend to overfit the data.

Key Distribution Scheme (KDS)

The deblurring and denoising of QRCODE is useful only in data transmission. So in order to implement this technique we have taken a message sharing application in which a user may need to communicate with other users securely. In this application, when a user send a message to another user, it will be sent in an encrypted format using QRCODE. This qrcode will be sent to bothsender and receiver by the server. So whenever a user need to communicate with other user, he need to use this QRCODE. If it's right, the data will be decrypted and the message will be displayed.

V.CONCLUSION

In this paper a new rich code called two level QR (2LQR) code is proposed. This 2LQR code has two levels: a public level and a private level. The public level can be read by any QR code reading application, while the private level needs a specific application with specific input information. This 2LQR code can be used for private message sharing or for authentication scenarios. The private level is created by replacing black modules with

specific textured patterns. These textured patterns are con- sidered as black modules by standard QR code reader. Thus the private level is invisible to standard QR code readers. In addition, the private level does not affect in anyway the reading process of the public level.

REFERENCES

[1] ISO/IEC 15420:2009. Information technology - Automatic identifi- cation and data capture techniques - EAN/UPC bar code symbology specification 2009.
[2] ISO/IEC 16022:2006. Information technology - Automatic identification and data capture techniques - Data Matrix bar code symbology specification. 2006.
[3] ISO/IEC 18004:2000. Information technology - Automatic identifica tion and data capture techniques - Bar code symbology - QR Code. 2000.
[4] Z. Baharav and R. Kakarala. Visually significant QR codes: Image blending and statistical analysis. In Multimedia and Expo (ICME), 2013 IEEE International Conference on, pages 1–6. IEEE, 2013.
[5] C. Baras and F. Cayre. 2D bar-codes for authentication: A security approach. In Signal Processing Conference (EUSIPCO), Proceedings of the 20th European, pages 1760–1766, 2012.
[6] T. V. Bui, N. K. Vu, T. T.P. Nguyen, I. Echizen, and T. D. Nguyen. Robust message hiding for QR code. In Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2014 Tenth International Conference on, pages 520–523. IEEE, 2014.
[7] A. T. P. Ho, B. A. M. Hoang, W. Sawaya, and P. Bas. Document authentication using graphical codes: Reliable performance analysis and channel optimization. EURASIP Journal on Information Security, 2014(1):9, 2014.
[8] T. Langlotz and O. Bimber. Unsynchronized 4D barcodes. In Advances in Visual Computing, pages 363–374. Springer, 2007.