Securing Biometric Face Images via Steganography for QR Code

Sercan Aygün, Muammer Akçay

***Abstract*—Recent evaluations in technology require deep awareness in terms of security. Both the users and developers need to bear in mind that there is no perfect way to be in secure. At least by using the brute force approach, every password has its own way to be deciphered, even though it takes years with supercomputers. Passwords can be changed with the ease of use. Whereas, there are some other authentication methods that serve quite convenient advantages like portability. Biometric features of our own are the part of biological human body which have admirable structure to be distinguished perfectly. On the other hand, these unique features are to be secured carefully in the application based usage the reason why cannot be changed physically like passwords. Therefore, in this paper it is proposed to use quick response code-QR for biometric face features to be ciphered by steganography and Relational Bit Operator-RBO. Recent access control systems require aforementioned biometric structures especially for e-government and e-passport applications. This paper presents a new approach to be used in application related biometric face image features in tiles to be safely transmitted. Consequently, by using an operator, first a pattern is obtained in the light of image processing and cryptography. After, the pattern is mixed up randomly by saving the actual positions of each element. Finally, the new pattern, in other words new image, is embedded into QR code by inserting the actual parameters of each element via steganography, too. Following sections present relatively the introduction, literature review, face biometry related operator, proposed method and conclusion at the end.**

***Index Terms*—Biometry, cryptography, face biometry, QR code, relational bit operator, steganography.**

I. Introduction

Security plays an important role in the human history. From the ancient times to the World Wars there were many stories about the cryptographically constructed approaches and systems. Also with recent technological developments, cyber security has become very crucial area that appeals researchers. In this work, it is aimed to propose a model that hides biometric face image features into QR code that is hard to be obtained by attackers. In daily technologies, biometric authentication provides more suitable ways for users to be supplied by easy to carry personal identification indicators. These indicators are every time with the human, the reason why they are the part of human body. There is no need to carry extra cards or remember things like passwords. Hardware engineers add some biometric sensors like fingerprint sensors into the personal computers and mobile phones to make access controls more robust, too. Besides, banking also uses bio-signatures during ATM machine operations. Thus, public is getting used to employ these access methods in their daily authentication systems. Furthermore, some other governmental areas are requiring biometric face and finger data for verification purposes. For instance in Turkey, the new biometric data inserted national ID cards are going to be in use near future. Therefore, handling these significant biometric data must be securely implemented.

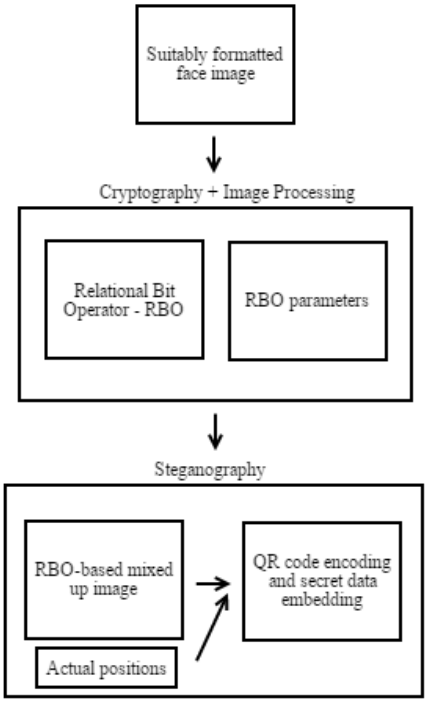


Fig. 1. Summary of the general approaches that are used in this paper.

In Fig. 1, it is illustrated the basic points of this work that are gathered together. Input image that obeys the biometric face picture format is inputted, which is cropped and its color conversion managed. After, the feature extraction process starts. In that step, getting features both must be meaningful for image analysis knowledge and must be cryptographically manageable. Therefore, a convenient approach is needed which is going to be presented in Section III. Then, the operator related new image –the image feature data– is obtained in matrix format. This is then randomly mixed up by caching the first positions of each row-column based pixel element. Up to that point, image processing is deployed in the frame of ciphering data where all mixing data will be placed in QR codes by hiding actual row-column based location keys into QRs via steganography.

II. Related Works

In the literature, there are some examples for the usage of QR code to be an element as a security level increaser. Chen and Wang propose to hide some data in QR code by considering some of its useless parts [1]. In that work, the lossy and lossless data are categorized. One can be partially lost, there is no matter, because during reconstruction, error correction feature of QR code works well. They add that the proposed scheme is resistant to JPEG attacks. 25% is the well enough rate for error correction on their work. On the other hand, Zigomitros and Patsakis make vice versa proposal that embedding QR coded data into one another image [2]. This is good for compression applications according to their final draw. Besides, during web searches, embedding some data into several images should speed up the search time by checking the text data inside of QR. Chung et al. proposes a similar approach to [1] by embedding lossless text data into QR code and using the regular areas in the QR code even like cropping it for reduction of dimension [3]. Therefore, it can be understood that there are some parts which are omittable and can be used for saving the key of the ciphered data.

There are also some other applications of QR code like to be used in medical applications. Chang et al. uses QR code in a hospital environment to embed secret data of patients etc. [4]. Maheswari and Hemanth give Fresnelet Transform and Least Significant Bit (LSB) related to steganography knowledge where LSB is the one also considered in this study [5]. Ramesh et al. uses the general trend as embedding text data into QR code, but this time by using Discrete Wavelet Transform (DWT) to make encoding and decoding operation in frequency domain. It is proposed that the highly secure output is obtained [6]. In the literature, the general trend is to embed text data into QR and to handle this data. From the inspiration of that, in this work it is going to be added image data bytes up into the QR which is different from the standard text data.

For the visual cryptography, one of the state-of-art study [7] exhibits how to secure the biometric data in visual cryptography by Ross and Othman. In Visual Cryptography Scheme (VCS), the original binary image T is encrypted into n images where n is the number of noisy images. The scheme, namely k-out-of-n uses the Boolean operation as follows:

$$T = S_{h1} \oplus S_{h2} \oplus S_{h3} \oplus \ldots \oplus S_{hk} \quad (1)$$

Reconstruction of original image T is only possible under the condition that k or more out of n images will be used. Encryption for each pixel is done by using subpixels, namely shares, and the independent random choices. Ross and Othman uses one step higher approach of VCS named as Gray-Level Extended Visual Cryptography Scheme (GEVCS) for face images. There are one private and two host face images. Host images look alike private image in terms of geometry and appearance. Transparency, the number of white pixels, is obtained by the control of subpixels in shares of host images during encryption which is done via Active Appearance Model (AAM). This model contains training set annotation, texture model and combined AAM building. After, selection of the hosts, image registration & cropping, secret encryption & reconstruction are handled. In the final phase, GEVCS does secure private image O in the two host images, H_{s1} and H_{s1}, by resultants S_1 and S_2.

III. Face Biometry and Relational Bit Operator

Authentication is the one process that the face recognition is employed. Therefore, biometry plays an important role. In this section, biometry related knowledge and a new operator will be presented.

A. Biometry

It is better to understand what the biometry is and its subdivisions to make it clear before security related issues. Every human being has its own genetic structure which is perfectly different from one other. This phenomenon makes every person unique in the way of behavior, appearance, character, even illnesses, habits, and so on. Biometric data from biological being also the one makes it peerless. Biometry can be thought of three ways: physical, behavioral and the chemical. All the features used for authentication purposes are in the one of these subdivisions like fingerprint, face, signature, DNA, ear etc. Face biometry is relatively easy to be captured via image acquisition. Therefore, this paper uses the face biometry to be secured.

B. *Relational Bit Operator*

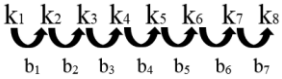
Extracting feature from biometric images is an important step in image processing related approaches. There are some methods to obtain a pattern from face images. Local Binary Pattern (LBP) is the one proposed by Ojala used for both in face detection algorithms and for texture analysis. Referencing the center pixel by considering the neighbors a pattern is captured. The size of the operator that effects neighborhood and the direction of the operator for processing each neighboring pixel are crucial parameters [8].

From the inspiration of LBP, a relatively new operator is proposed to search for relations of each neighbors. Fig. 2 shows the rectangle shape operator which is the 1 step size and 8-neighbouring based.

k_1	k_2	k_3
k_8	c	k_4
k_7	k_6	k_5

Fig. 2. RBO-Relational Bit Operator illustration with center pixel c, and all k_x neighbors.

In Fig. 2, k's are all the neighbors in that rectangle shape and it is 1–pixel long distanced operator. The relations based on the neighbors can be calculated in some ways like the one in the following pattern as $b_1b_2b_3b_4b_5b_6b_7$ format. The starting pixel and the rotation can be any of the possibility. Fig. 3 illustrates some examples of them. Next, k_x neighbors are checked according to their numerical values. Then the pattern of b_s in 0's and 1's is obtained:



Center pixel is not in the scope of interest but the all neighbors are processed. For example, in Fig. 3, the first square tells the starting point from k_1 till the k_8 same as previous pattern. Whereas, the pattern can be obtained from any other starting pixel in counter-clockwise direction as in the second operator. The crucial point is to use the fixed approach for all pixels of raw face image and save parameters like rotation, starting pixel etc. as the key elements.

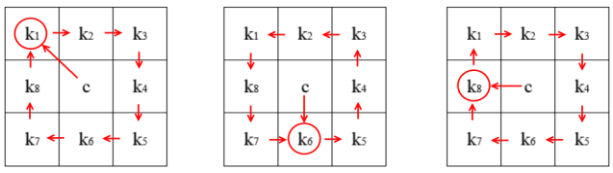


Fig. 3. Some RBO examples of possible starting pixels and rotation.

Numerically, it is considered if $k_1 > k_2$, the pattern is taken as 0 where it represents that there is a decreasing behavior, otherwise if it is $k_1 < k_2$ then the related bit is taken as 1. Fig. 4 shows a numerical example related to the Relational Bit Operator.

211	71	13
58	67	110
42	9	98

Fig. 4. A real valued piece of image that has 8-bit gray level pixel values to be processed via RBO, k_1 is the starting pixel and the rotation is clock-wise.

$k_1k_2k_3k_4k_5k_6k_7k_8$ = 211 71 13 110 98 9 42 58
$b_1b_2b_3b_4b_5b_6b_7 = (0010011)_2 = (19)_{10}$

The number 19 is now stored for operator based matrix instead of center pixel value 67. By that way, the feature of face image is preserved but it cannot give any meaningful information to attackers. Even, there will be some other security increasing approaches that are explained in the section of proposed system.

IV. Other Concepts

A. *QR Code*

Coding some information into a visual material like barcode brings some remarkable advantages as seen in shopping environment. All products in supermarkets have barcode on them to be scanned by the cashier. The barcode has 1 dimensional approach, whereas QR code is the 2D which was invented by the Japanese corporation Denso Wave. QR image has white and black colors mostly, even though recent QR codes can have some colorful visual pictures on it. The encoding operation is done vertically and horizontally, therefore more data than 1D barcoding can be processed. Data can be text, number, URL, or even Kanji characters, too. In QR image there are 3 finder pattern that the camera can understand the horizontal or vertical positions of the image. The greatest amount of data is 2953 bytes as binary (8 bits) format that can be stored in QR. There is error correction possibility in QR code with 4 levels that inspires this work to use some areas of QR code for steganography [9].

B. *Steganography vs. Cryptography*

Steganography and cryptography are quite close concepts whereas there are slight differences between them. Securing data against malignant actions is the basic aim to be considered. One survey underlines the relation between cryptography and steganography in a

well-structured way. It puts all answers between the similarities and differences of cryptography and steganography concepts [10].

Steganography uses an ordinary digital media, as if there is a way to embed a special message into it. The message can be embedded by using special techniques like LSB as in this work. On the other hand, cryptography is the skill of altering the secret message. If the attacker reaches the secret message, then the cryptographical system is broken. For steganography, the attacker first needs to understand whether there is a stegoimage or not which can be visually hard.

V. Proposed Method

Using QR code in the biometric data transmission is a bright idea to confuse intruders. The raw data of biometric face image is not shared openly, but its extracted data is sent. Also, it is mixed up randomly by using permutation cipher that the actual positions are stored as key for deciphering process on the destination side. After, this complex data is encoded into QR code where the key of one other image tile is randomly put into QR, too. The key is hidden via steganography. Therefore, the actual positions of featured biometric data are hidden.

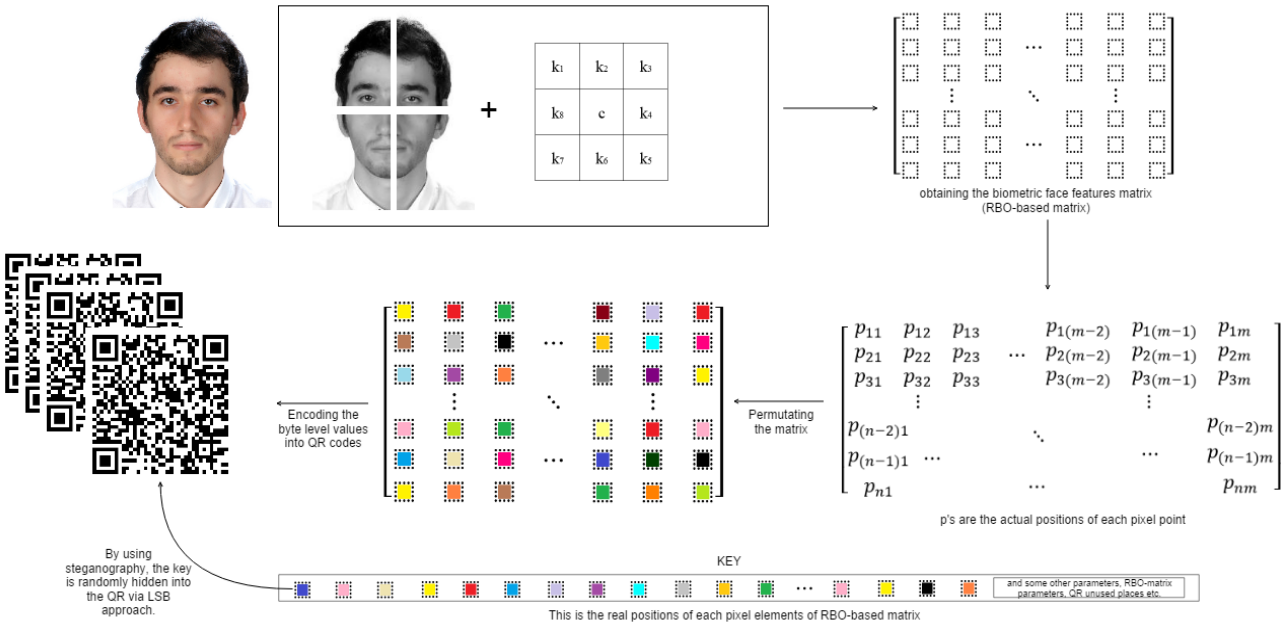


Fig. 5. The whole proposed system that secures biometric face image.

As in Fig. 5, first the face image is used for pre-processing like gray level conversion and tiling. Then, the feature extraction by using RBO is handled. The matrix format like an image is constructed and each *p* is the actual position of the related pixel value. The extracted features are then mixed up randomly by saving their actual positions for the decoding process. The colorful matrix is the new complex data to be encoded in the QR image. The important point in the proposed system is getting the features. The method as Relational Bit Operator is also proposed both by considering the image processing and the cryptography together. During mixing up extracted data, permutation is employed. By keying the actual positions of first nxm sized matrix illustrated with *p*'s is embedded into QR code regular area by LSB while rest of the QR holds the permuted feature data. The face image is actually tiled and each part is embedded into different QRs because of quick response code memory.

A. *Vulnerability and Limitation Analysis*

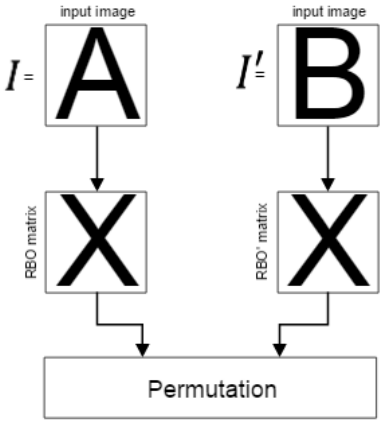
The proposed method can be analyzed in the sense of attackers, thus the complexity of the proposed method can be thought in terms of the several dependents:

i.) Noticeability of the steganography by an attacker
ii.) RBO method
iii.) Permutating the matrix
iv.) QR code unused areas (key placement)
v.) Key management of different image parts

All these concepts have their own difficulty to be issued by an attacker. Even, whomever obtains the QR code of this biometric data should probably first concentrate on the data encoded itself, however it is not the only valid data for authentication.

In practice, from different input images getting the same RBO matrix is not quite possible where it relates to the biometric features. Somehow, it is assumed to have identical outputs because of the physical effects on the images like illumination, noise, acquisition issues etc. If

two matrix have the same values, then the permutation acts. Fig. 6 shows that the case when even two different images get the same RBO output. Each input image is also a parameter for the permutation. Plus, the Gray Level Co-occurrence Matrix - GLCM is other input. Each image input has its gray level value occurrences and that differ in different images leading to obtain GLCM, then even though the results are the same, because input images and GLCM differ, the output of permutation changes, too. This preserves to have non-identical results for biometric issues, also giving an advantage to use GLCM for authentication.



$$f_{permutation}(raw\ image\ pixels, GLCM, RBO\ matrix)$$

Fig. 6. The worst case scenario that the different images have the same RBO matrix output.

If the overall complexity for the attacks is measured, the exhaustive trials through the database can be checked. For 200x240 pixels and 8-bit gray level face image given in Fig. 5, there are $(2^{\text{gray-level}})^{\text{row*column}} = (2^8)^{48000}$ brute force trials. For the proposed method, each pixel is revalued by considering the neighbors. This is then converted a decimal value such as gray level value. The occurrences between neighbors cannot be easily inferred from just a decimal number. Even more, the starting pixel and rotation of RBO are other secrets for the attacker. Moreover, the image could be in tiles because of the QR memory. QR code size has a remarkable concern. Version 40 QR code has maximum capacity of 2953 (~3000 will be assumed) bytes which has 177x177 modules. This brings a limitation and the whole data cannot be embedded into the just one QR directly, but the tiles of the image can be generated and they can be used for different QR images. The tiles can be sent in a random order which must be figured out by only the receiver. This puts one other complication for the intruders. Limitation itself brings an advantage, too. For parallel processing issues, tiles can be computed in parallel. Fig. 7 shows the overall reverse operation of reaching back to keys. In this figure, first the image parts are obtained in random order. For instance, 200x240=48000 pixels can be put into 48000/(~3000)=16 QR items approximately. All possible image parts (n=16) can be reordered accurately by $n!$ amount of brute force trials. Then, the attacker needs to understand the steganography. The risk of steganography is the same as all other scenarios: the embedded data should not be captured from its place. If the attacker can understand the steganography, then it can pose a threat but the embedded key itself is like a data package, there are several sub-blocks inside that cannot be easily understood. Exhaustive key search then begins for the malicious attack. The problem can be more complex if the keys are not sent via the QR to which belongs. Keys can be bound to different pairs to make it complex as $n!$ again for each key. The n parts of the image is taken into account and $n*n!$ is reached. Finally, expected key is tried to be extracted from the ~1800x1800 pixels of QR image (version 40). Order of these pixels can give the key as (*QR_Row*QR_Column*)! times attempts. All in all, the two scenario is compared: obtaining the biometric data by a brute force attack and reversing the proposed method to get the keys to make the system broken. On the condition that the number of image tiles n is large enough, then the proposed scheme is stronger than a brute force attack.

$$n*[n!*(QR\_Row*QR\_Column)!*n] >> (2^{\text{gray-level}})^{\text{row*column}}$$

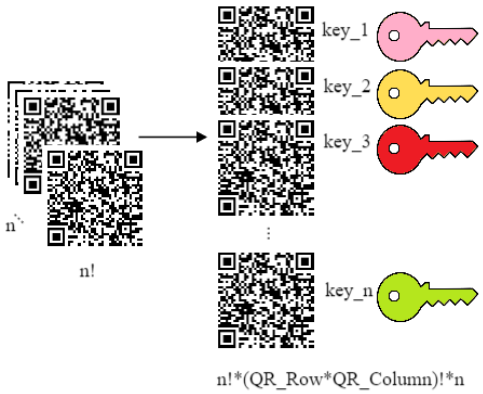


Fig. 7. Hardness of the recovering information in brute force sense.

VI. Conclusion

This study proposes a secure, biometric based data hiding technique by using two interesting work space: QR coding and steganography by considering the cryptography. Therefore, this paper aims at combining cryptography which can be useful for image processing techniques. The person who gives biometric data may

not want to share his or her data in public openly. Therefore, just the features are sent in a secure way.

There may arise a question that why to choose QR codes for steganography. First, document authentication systems have been becoming quick response code related and QR codes can be used for data compression and web search issues related to image based queries. Besides, QR code has its own correction algorithm and even there can be some losses because of embedding the secret key, but the QR should be recovered successfully.

Security level of this study as discussed in Section V concludes a trade-off where the size of original biometric face image can be in some interval. The tests have shown that as the image size increases, computation load of each image tile – or QR code numbers – increases, too. Whereas, increased *n* makes the system more resistant to attacks. Finally, it is arrived that the biometric image standards by some institutions like International Civil Aviation Organization-ICAO are successfully met in terms of sufficient image size requirement of this study.

This work is the part of a master thesis, therefore there are some other approaches as future work. For instance, image feature extraction process can be in parallel during the slicing the image into parts. Moreover, for authentication purposes there can be a multi-modal approach like adding fingerprint sensor which was previously realized in [11].

All in all, this paper achieves to use QR codes in a different manner by embedding biometric data features as byte level values into them. In the literature, general trend is just placing text data and after using QR to be hidden into one other image. Therefore, this paper differently uses steganography to hide a key into QR itself via error correction flexibility.

REFERENCES

[1] W. Y. Chen, J. W. Wang, "Nested image steganography scheme using QR-barcode technique," *Optical Engineering* vol. 48(5), May 2009.

[2] A. Zigomitros, C. Patsakis, "Cross format embedding of metadata in images using QR codes," *Intelligent Interactive Multimedia Systems and Services*, vol. 11 of the series Smart Innovation, Systems and Technologies, pp 113-121.

[3] C. H. Chung, W. Y. Chen, C. M. Tu, "Image hidden technique using QR-barcode," *2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 522 – 525, Kyoto, Sept. 2009.

[4] Y. Y. Chang, S. L. Yan, P. Z. Lin, H.B. Zhong, J. Marescaux, J. L. Su, M L. Wang, Pei-Yuan Lee, "A mobile medical QR-code authentication system and its automatic FICE image evaluation application," Journal of Applied Research and Technology, vol. 13, pp. 220–229, 2015.

[5] S. U. Maheswari, D. J. Hemanth, "Frequency domain QR code based image steganography using Fresnelet transform," *AEU - International Journal of Electronics and Communications*, vol. 69, pp. 539–544, Feb. 2015.

[6] M. Ramesh, G. Prabakaran, R. Bhavani, "QR- DWT code image steganography," *International Journal of Computational Intelligence and Informatics*, vol. 3, pp. 9–13, April 2013.

[7] A. Ross and A. Othman, "Visual cryptography for biometric privacy," IEEE Transactions on Information Forensics and Security, vol. 6, no. 1, pp. 70–81, March 2011.

[8] T. Ojala, M. Pietikäinen, and D. Harwood, "A comparative study of texture measures with classification based on featured distributions," *Pattern Recognition*, vol. 29, no. 1, pp. 51–59, 1996.

[9] W. Islam and S. alZahir, "A novel QR code guided image stenographic technique," *2013 IEEE International Conference on Consumer Electronics (ICCE)*, Las Vegas, Jan. 2013.

[10] A. J. Raphael, V. Sundaram, "Cryptography and Steganography – A Survey," *Int. J. Comp. Tech. Appl.*, vol. 2 (3), pp. 626–630.

[11] S. Aygün, M. Akçay, and E. O. Güneş, "Bulut sistemler için önerilen biyometri tabanlı güvenlik sistemine genel bakış," *The Third International Symposium on Digital Forensics and Security (ISDFS 2015)*, May 2015.