Multimodal Biometric Template Protection Using Color QR Code

Devendra Reddy Rachapalli1, Hemantha Kumar Kalluri

ABSTRACT--- Several cancelable biometric cryptosystems have been proposed to give security and protection to the biometric data. Even though these- techniques provide security from pre-image attacks and template protection. Developing innovative and highly robust cancelable biometric cryptosystems are vital. This paper proposes a novel cancelable biometric cryptosystem for template protection using color QR code. The proposed biometric cryptosystem is key generation based and registration free feature based multimodal biometric template of cancelable biometric method and works with conventional matcher. The proposed system has realized the properties of cancelable biometrics – revocability, diversity, non-invertible biometric encryption and pre-image attack resistant.

Keywords:cancelable biometrics; biometric cryptosystems; color QR code; revocability, pre-image attack; non-invertible.

1. INTRODUCTION

Biometrics always denotes the unique characteristics or traits associated with each individual for identification. To provide access controls, these biometric traits are used as verification and authentication mechanisms. Biometric systems that use multiple traits like fingerprint, iris and palmprint etc., are named as multimodal biometric systems. Multimodal biometric systems ensure more reliability over unimodal biometric systems as it is reducing Failure-to-Capture Rate (FTCR) and Failure-to-Enroll Rate (FTER). Considering this objective the authors have proposed multimodal template fusion system which takes the fused biometric traits as inputs to generate fused template. The features of fused template are extracted after performing texture, color and shape classifications. Now, the extracted features of the biometric fused template have to be encrypted with a suitable biometric cryptosystem. Protection for fused biometric template can be provided by transforming the biometric template [1, 2].

Now-a-days, cancelable biometrics and biometric cryptosystems play a key role in designing many modern applications for banking, office security systems, shopping malls etc. Cancelable biometrics uses transformations to deal with protecting biometric template and cryptosystems focuses on encryption and authentication to deal with securing biometric templates [3, 4]. For securing biometric templates randomized key generation and binding modules have to be developed. In order to protect biometric templates transformations on features of biometric templates are indispensable. The transformed template protection system should possess the properties like revocability, diversity, non-invertible and also resistant from pre-image attacks [5]. To improve robustness the transformed templates need not to be stored in database. The authentication process for the transformed biometric template with input biometric template has to be performed in the transformed domain. For matching purpose, the existing conventional matcher is sufficient. It is crucial time for the researchers to develop a novel and robust approach that performs crypto based feature transformation on biometric template to provide protection and security for fused biometric templates.

An innovative step towards the cancelable biometrics with biometric cryptosystems is to introduce color QR code representation for transformed features of multimodal biometric template. Before extracting the features and fusing the template, the fused multimodal biometric traits (iris, palm and fingerprint) are classified based on texture, shape and color.

The rest of the paper is organized as follows. First, the background introduction about biometric cryptosystems, cancelable biometrics and QR code are discussed in section 2. In section 3, the literature is reviewed. In section 4, the motivation and proposed system are described in detail. Section 5 narrates about the comparative analysis of the proposed system with existing approaches using revocability, diversity and non-invertible properties. Finally, the conclusions are presented in section 6.

2. BACKGROUND

2.1. Biometric cryptosystems

The objective of Biometric Cryptosystems (BCSs) is to design secure cryptographic key for biometric features which are similar to password based key generation systems. The advantage of BCSs over password based key generation systems is, biometrics is difficult to forge, share, copy and distribute [6]. To retrieve or generate keys, biometric dependent public information, referred as helper data is stored by BCSs [7]. BCSs are classified as key release based biometrics, key generation and key binding cryptosystems based on how helper data are derived. In key binding biometric cryptographic systems, cryptographic key is combined with biometric template to generate protected biometric template. The key is independent from biometric features. But, in key generation biometric cryptographic systems, cryptographic key is directly produced from biometric features and helper data. The protected biometric templates are derived only from the biometric template. In the proposed work a novel form of key generation based

Revised Manuscript Received on February 11 , 2019.

Devendra Reddy Rachapalli1, SriKalahasteeswara Institute of Technology, India.(csdreddy@gmail.com)

Hemantha Kumar Kalluri, CSE Department, Vignan's Foundation for Science, Technology & Research, India.

biometric cryptosystems is used for securing biometric templates.

2.2. Cancelable biometrics

Cancelable Biometrics (CBs) also denoted as feature transformation, transforms original or features of biometric template using a one-way function and make available to compare biometric templates in the transformed domain. Inverting of such transformed biometric templates is not being possible for imposters. In contrast, during authentication the standard encryption algorithms for biometric template protection need not be implemented for decryption. Such cancelable biometric template protection system offers irreversibility and unlinkability for biometric templates. Irreversibility means, comparing with the transformations to generate the protected biometric template, it should be computationally difficult to reconstruct the original biometric template or featured biometric template from the protected template. Unlinkability means, using the same biometric data, protected biometric templates can be generated which are not same and also called renewability, there should not be any cross-matching in protected templates as well. Other template protection properties are revocability, non-invertible and diversity. Revocability means for different randomization, same biometric template should produce different output. In non-invertible biometric encryption, it is very difficult to extract/decrypt input biometric information from cancelable biometric templates or finding the transformation keys used. Diversity denotes output related to the same biometric data should produce different output using different key size, value or methodologies [8].

The design of cancelable biometric template protection systems are made in such a way that it is very hard to compute and recuperate the original biometric data from the transformed domain. During the transformations, the individuality of biometric characteristics should not be condensed (false acceptance rate restraint) and also, the transformations should be acceptable to intra-class variation (false recognition rate restraint).

Methods for cancelable biometric template protection are roughly divided into 2 categories. Category – 1 CBs work with a special matcher whereas category – 2 CBs work with conventional matcher. These categories are further divided based on the registration of biometrics. The first category in which registration of biometrics needed and in other category no need of registration is required. Again these schemes are further classified into two types – signal based schemes i.e. CBs that work with original biometrics templates and feature based schemes i.e. CBs that work with features extracted from biometric templates.

Summarizing the existing cancelable biometric template protection methods: methods such as Biometric salting, PalmPhasor, PalmHasor and BioConvolving are feature based CBs that require registration and special matcher. A signal based CB method named Biotokens, also requires special matcher and registration. On the other hand, another signal based CB method, correlation-based MACE filter that involves special matcher is a registration free method.

Signal based CB methods that work with conventional matcher and requires registration are dynamic random projections, image warping, block remapping, noninvertible transforms and COMBO. Feature based CB methods that works with existing matchers and require registration are Palm Hashing, Bio Hashing, permutations and random projections (RP). Similarly signal based CB methods that work with existing matchers but are free from registration are curtailed circular convolution and minimum distance graphs [9].

Finally, feature based registration free CB method that works with convolution matcher is registration-free approach. The proposed cancelable biometric cryptosystem using color QR code is registration free method which uses feature based multimodal biometric fused template.

2.3. QR code

QR Code format contains diverse patterns that are reserved for special purposes as per the standardization ISO/IEC 18004:2015(E) [10]. There are forty versions of QR code symbols each one referred as version1, version2 … version40. The most common and simple version (version 1) of QR code contains the following patterns and is shown in Fig. 1.

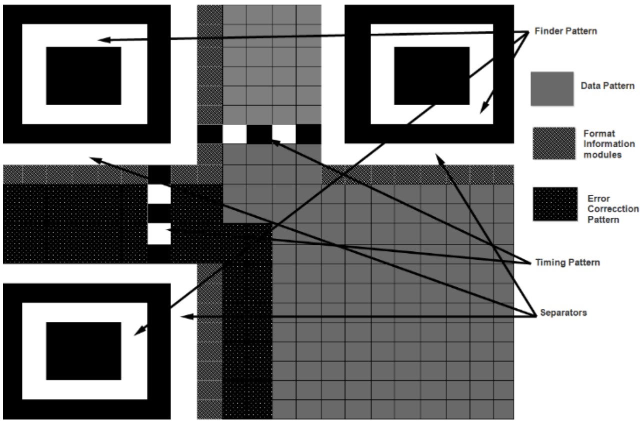

Fig. 1: Structure of QR code version 1

Finder pattern: Three identical structures of a pattern is located in three corners left-top, left-bottom and right-top of the QR code. Each pattern consists of 7x7 matrix of black and white modules such that a 3x3 matrix of black modules are bounded by white modules to form 5x5 matrix. This matrix is again bounded by black modules to form 7x7 matrix. These patterns enable the QR scanner software to recognize and determine the correct orientation.

Separators: One pixel width of white modules separates the three finder patterns from other data modules.

Timing pattern: This is a pattern with discontinuous black and white modules, which helps in determining the width of a single module.

Format information modules: The format information and error correction consists of 31modules next to the separators. Error correction level of the QR code is stored in this pattern.

Data pattern: Data module contains actual data to be stored in QR code. Actual data is converted into 8 bit data stream called codewords and then stored in the data section.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Error correction pattern: This is also a part of data modules, which stores error correction codes of 8 bit long codewords.

3. RELATED WORKS

In this section various developments related to biometric cryptosystems using cancelable biometrics are described. The objective of biometric cryptosystem is to protect the template from security attacks. To protect the biometric template one can use the most popular method, Fuzzy vault. It binds biometric features with a secret key and produces helper data. This helper data helps in recovering the secret key during authentication.

Rathgeb et al., [11] proposed an alignment-free cancelable biometrics based on adaptive bloom filters based representation for binary iris biometric template. The basic operation for the proposed cancelable biometric system for iris biometric trait based on adaptive bloom filter is alignment-free non-invertible transformation. The proposed system adapts bloom filter on texture feature transformation of iris biometric to achieve irreversibility and unlinkability. For evaluation in transformed domain, simple XOR operations are used for comparing a pair of binary biometric feature vectors. The binary biometric feature vector representation based on bloom filters doesn’t require any template alignment. The proposed system works for biometric trait iris only and also efficient serial combination of iris texture feature extractors of biometric template are applied to accelerate biometric identification.

Dang et al., [12] proposed a periodic transformation involved in cancelable fuzzy vault for biometric template protection. Though the proposed cancelable fuzzy vaults with periodic transformation achieves cancelability property but are failed in generating low FAR and FRR rates.

Edlira Martiri et al., [13] proposed a biometric template protection scheme using bloom filters and honey templates to award privacy protection to the biometric templates and detect whether the templates are stolen. Bloom filter based protected templates are used by the proposed system. The performance of the system is tested with logistic regression (LR), support vector machine (SVM) and quadratic discriminant analysis (QDA). The performance metrics chosen for testing this system are false match rate (FMR), equal error rate (EER) and false non-match rate (FNMR). This scheme is performing better for facial verification but cannot be feasible for multimodal biometric template protection. Even in facial templates, needs improvement in templates indistinguishability by employing feature selection scheme, honey template construction and other classification algorithms.

Mayada et al., [14] proposed a convolution based bidirectional associative memory (BAM) neural network for novel correlation attack-resistant cancelable biometric scheme. In the BAM neural network random transformed key is used in adjusting the weights of the output layer in achieving revocability. Regarding non-invertible encryption process the proposed system uses two level transformations one in the way of generating weights and another for convolution process. The system is attack-resistant and the BAM modelis used with weights that is kept safely in a central database and is robust against pre-image attacks.

Karthi et al., [15] proposed an improved hybrid template protection algorithm to protect multi biometric template. The system uses multiple biometric traits like face, fingerprint and iris. The biometric traits are fused at feature level fusion to form fused template. In order to protect the biometric attack like modification of stored template, Template protection algorithm is applied to the biometric features to overcome this. The multi biometric template protection process generates a key using key generation algorithm. The generated key is used for bio-hashing algorithm to produce bio-code to store in database. The performance of the proposed system is compared by calculating FAR and FRR for single biometric template and multi biometric fused template but not with other template protection systems.

4. CANCELABLE CRYPTOSYSTEM USING COLOR QR CODE GENERATOR

The objective of the proposed system is to design cancelable biometric cryptosystem for multimodal biometric fused template. Devendra et al., [16] proposed a multi biometric template fusion system which takes fused biometric traits of same class. The fused biometric traits are classified based on texture, share and color and are applied for feature extraction. The extracted features are fused at feature level to generate fused template for each classification. These fused templates are inputs for proposed system.

The novel cancellable cryptosystem shown in Fig. 2 consists of the four sub modules shown in colour filled boxes. The proposed system takes the multimodal biometric fused template for texture, shape and color classification as input to the cipher data conversion module and generates color QR code image for them.

4.1. Cipher Data Conversion

This module is a part of biometric concealment to solve security issues related to the fused template which is stored in the database. The process involves simple permutations and module operations to encrypt the fused template. A symmetric encryption key is used to formulate both permutations and XOR operations to generate cipher data. As the cipher data needs to be cancelable, it is necessary to encode the cipher data such that the protected template acquires irreversibility property of cancelable biometrics (CBs).

4.2. Encoding and Grouping

In this sub module, the generated cipher bit stream data received from cipher data conversion is considered as input to produce an encoded bit stream data which is irreversible. The necessary values of bit stream data are identified and formulated a mechanism to generate encoded bit stream. If the necessary values of the bit stream is n, then there are [A_1, A_2, A_3, … A_n] necessary values. i.e., for each necessary value A_i of the bit stream [A_1, A_2, A_3, … A_n] of n values formulate an encoded value E_i to get an encoded bit stream [E_1, E_2, E_3, … E_n]. The grouping mechanism is derived as

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

$EG_1 = E_1 * C + E_2$, $EG_2 = E_2 * C + E_3$, $EG_3 = E_3 * C + E_4$, $\ldots EG_n = E_n * C + E_1$, Where C is a suitable hidden constant for grouping mechanism.

4.3. 8-bit Decimal Conversion

The purpose of this module is to generate encoded and grouped bit stream values within the range of 0 to 255 so that they can be plotted in the QR code. The previous modules of cancelable cryptosystem achieves irreversibility feature of CB. To achieve unlinkability and diversity in template protection, the encoded bit stream data is converted to color QR code image. The QR code chosen for given bit stream data is byte data i.e. 2953 characters. In order to fit the data to QR code it is assumed to generate the encoded bit stream data in the range of 0 to 255.

4.4. Color QR Code Masking Pattern

The proposed system generates color QR code version1 of 21 x 21 modules (441 modules – A2). The function pattern modules contains 202 modules – B. i.e. the three 7x7 modules of finder pattern on left-top, left-bottom and right-top of QR code, 15 modules of separators and Timing patterns of 10 modules.

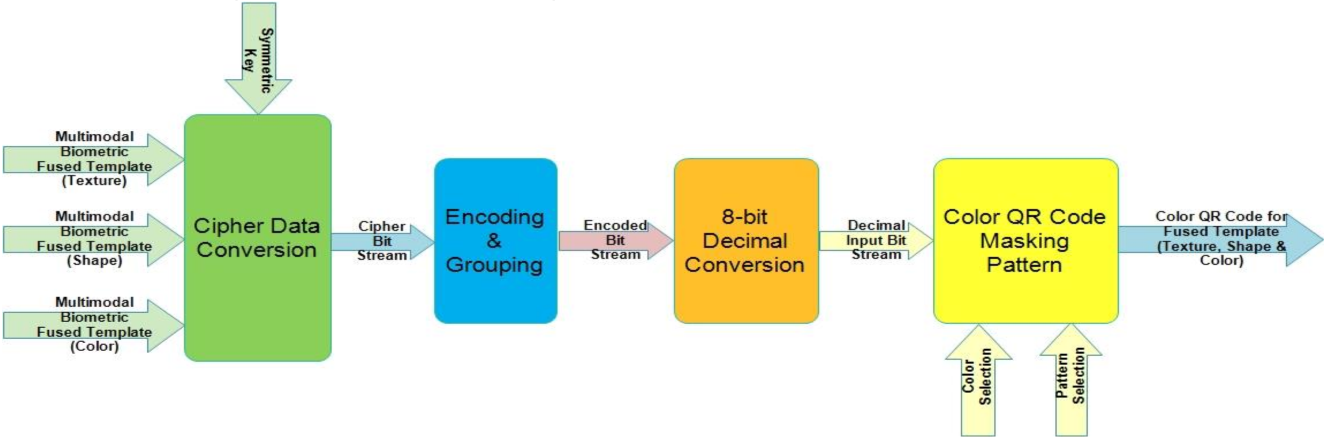
Symmetric Key
Multimodal Biometric Fused Template (Texture)
Multimodal Biometric Fused Template (Shape)
Multimodal Biometric Fused Template (Color)
Cipher Data Conversion
Cipher Bit Stream
Encoding & Grouping
Encoded Bit Stream
8-bit Decimal Conversion
Decimal Input Bit Stream
Color QR Code Masking Pattern
Color QR Code for Fused Template (Texture, Shape & Color)
Color Selection
Pattern Selection

Fig. 2: Cancelable crypto encoder using color QR code generator

Format information and its error correction code contains error correction information which takes 31 modules – C. Data modules except (C) is D = A2 – B – C i.e. 208 modules. Data capacity of version 1 QR code is 26 codewords of 1 byte each. The data and error correction code words hold 26 bytes of cancelable encoded crypto bit stream data. Based on the bit stream data generated after decimal conversion the QR code obtained for a sample biometric template is shown in Fig.3. Any input required for masking pattern of QR code data and error correction words are send through pattern selection. The input related to color selection is either RGB or CMY. Before the color selection, the QR code contains black and white pixels. The option for choosing color for QR code or selecting the color randomly or based on the encoded bit stream is also implemented in this module. QR codes with RGB and CMY are shown in Fig.4.

Fig. 3: QR code output generated

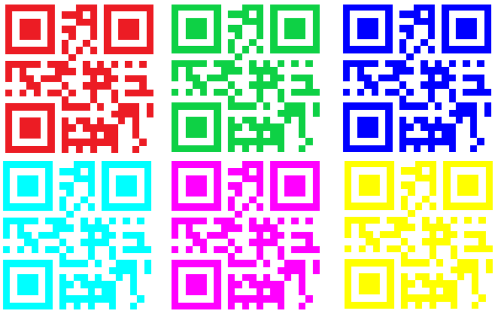

Fig. 4: RGB & CMY color QR codes

5. RESULTS & DISCUSSIONS

To compare the proposed cancelable biometric cryptosystem using color QR code with the existing approaches the template protection properties like diversity, revocability and non-invertible are compared for study. To achieve revocability highly randomized symmetric key generation is used for each transformation in cipher data conversion. To realize the biometric cryptosystem as non-invertible biometric encryption system, for template transformation three hierarchical stages – key driven module operation, key based color selection and key based pattern selection are developed. Finally to accomplish diversity, both randomized symmetric key and user defined unified module are used for template protection. The randomized symmetric key is used in three stages of template transformation. The encoding and grouping of cipher bit stream is the user defined unified module. The comparative analysis with some existing schemes is shown in the Table 1.

Table 1: Comparative analysis with existing schemes

Scheme	Rathgeb et al., (2013)	MayadaTarek et al., (2016)	Proposed system
Revocability	Secret key	Random transformed key	Randomized symmetric key
Non-invertible biometric encryption	Single level	Two level	Hierarchical stages three levels
Pre-image attack	No protection	Protected but not robust	Protected and highly robust

6. CONCLUSIONS

In this paper multimodal biometric template protections are performed using color QR code approach. The proposed approach is feature based biometric template and is registration free method.The proposed method is based on randomized symmetric key generated from seed. Towards non-invertible biometric encryption this approach used hierarchical stage wise transformation in three levels. Concerning about pre-image attack, the proposal is more protected as the design is made with user defined encoding and grouping modules and also highly robust as the protected template is need not be stored in database. The future work of the proposed approach is to develop authentication process that works with conventional matcher.

REFERENCES

1. Ramalho MB, Correia PL &Soares LD, “Hand-based multimodal identification system with secure biometric template storage”, IET Computer Vision, Vol.6, No.3, (2012), pp.165-173.
2. PeterWild,HeinzHofbauer,James Ferryman&Andreas Uhl,“ Quality-based iris segmentation-level fusion”, EURASIP Journal on Information Security, Vol.2016, No.25, (2016).
3. Vishal M. Patel, Nalini K. Ratha, & Rama Chellappa, “Cancelable Biometrics: A review”, IEEE Signal Processing Magazine, Vol.32, No.5, (2015), pp.54-65.
4. Sandhya Mulagala & Prasad V.N.K. Munaga, “Securing fingerprint template using fused structures”, IET Biometrics, Vol.6, No.3, (2017), pp.173-182.
5. Harkeerat Kaur &Pritee Khanna, “Random Distance Method for Generating Unimodal and Multimodal Cancelable Biometric Features”, IEEE Transactions on Information Forensics and Security, Vol.14, No.3, (2018), pp.709-719.
6. Rathgeb C, &Uhl A, “A survey on biometric cryptosystems and cancelable biometrics”, EURASIP Journal on Information Security, Vol.3, No.1, (2011). pp.1-25.
7. Gomez-Barrero M, Galbally J, Morales A, &Fierrez J, “Privacy-preserving comparison of variable-length data with application to biometric template protection”, IEEE Access, Vol.5, (2017), pp.8606-8619.
8. Devendra Reddy Rachapalli, Hemantha Kumar Kalluri, "A survey on biometrie template protection using cancelable biometric scheme", 2nd International Conference on Electrical, Computer and Communication Technologies (ICECCT), (2017), pp.1-4.
9. Cheniti M, Boukezzoula NE, & Akhtar Z, “Symmetric sum-based biometric score fusion”, IET Biometrics, Vol.7, No.5, (2018), pp.391-395.
10. ISO/IEC 18004:2015(E) International Standard, “Information Technology – Automatic Identification and data capture techniques – QR Code bar code symbology specification”, ISO/IEC Switzerland, (2015).
11. Rathgeb C, Breitinger F & Busch C, “Alignment-free cancelable iris biometric templates based on adaptive bloom filters”, 2013 International Conference on Biometrics, (2013).
12. Dang TK, Truong QC, Le TTB, & Truong H, “Cancellable fuzzy vault with periodic transformation for biometric template protection”, IET Biometrics, Vol.5, No.3, (2016), pp.229-235.
13. EdliraMartiri, Marta Gomez-Barrero, Bian Yang &Christoph Busch, “Biometric template protection based on Bloom filters and honey templates”, IET Biometrics, Vol.6, No.1, (2016), pp.19-26.
14. Mayada Tarek, Osama Ouda&Taher Hamza, “Robust Cancelable biometric scheme based on neural networks”, IET Biometrics, Vol.5, No.3, (2016), pp.220-228.
15. Karthi G, &Ezhilarasan M, “Multi biometric Template Protection using Hybrid Technique”, International Journal of Engineering & Technology, Vol.7, No.4, (2018), pp.2609-2613.
16. Devendra Reddy Rachapalli, Hemantha Kumar Kalluri, “Texture driven hierarchical fusion for multi-biometric system”, International Journal of Engineering & Technology, Vol.7, No.4.24, (2018), pp.33-37.