IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 25, No. 2, April, 2020, pp. 245-251
Journal homepage: http://iieta.org/journals/isi

Color QR Pattern-Driven Cancelable Biometric Fingerprint System

Devendra Reddy Rachapalli[1*], Hemantha Kumar Kalluri[2]

[1] SriKalahasteeswara Institute of Technology, Srikalahasti 517640, India
[2] Vignan's Foundation for Science Technology & Research, Guntur 522213, India

Corresponding Author Email: drkhk_cse@vignan.ac.in

https://doi.org/10.18280/isi.250212

Received: 24 December 2019
Accepted: 27 February 2020

Keywords:
cancelable biometrics, fingerprint biometric, quick response code, texture, GLCM

ABSTRACT

This paper introduces the texture alone fingerprint recognition system and uses a QR pattern to generate the cancelable biometric template with an improved probability of error. This proposed cancelable bio-cryptosystem inherits all the advantages of texture features from fingerprint biometric traits for a template generation, cipher transformation, and non-invertible properties, etc. Here, GLCM feature attributes are extracted from texture classified biometric images followed by feature selection and fusion techniques. And user key-driven random transformation is carried out for the transformed domain biometric template. And for cancelable biometric, some systematic QR patterns are generated, which directly depend on the transformed template. This will not degrade the system's performance irrespective of randomizations used for non-invertible transforms.

1. INTRODUCTION

In recent days, due to the high-speed inventions made by telecom industry with ever-increasing voice and data traffic will present new challenges to security and privacy protection [1]. The fraudulent activities in the wireless industry are emerging steadily and stealing identities in many ways. Due to its advanced analytics, unique information, and security level, biometric technologies are largely trusted to deter this fraud. However, with the rapid adaptation of biometric systems in a wide range of applications [2], there is also a growing concern that this may compromise the biometric trails, which is nothing but the anonymity of individuals.

In general biometric characteristics are immutable [3], and the leakage of biometric details in any one place resulting in permanent biometric compromise and remain unreliable forever.

Though cipher transformation [4] of these biometric details before creating the database can solve this problem, the key management problems associate with any block ciphers may reveal entire information [5]. And in the Fuzzy fault scheme [6] where all biometric information is encoded into some polynomials result in the high false rejection rate. On the other, some generic alternatives like cryptographic hash techniques [7] are not applicable for a wide range of biometric inputs and not support bio-cryptosystems. In order to overcome this generic problem that arises in any biometric systems cancelable biometrics was introduced where the original biometric information is canceled and replaced through some transformations and makes the same biometric data different for different application and reduce the impact the information leakages in biometric technologies. Since in biometric systems, well-approximated templates were used for biometric authentication to narrow down the penalty gap that exists between trials and real-time inputs, it is always motivated to transform the generated biometric template using some one-way function which producesthe cancelable biometric templates.

The work is structured systematically as follows. Section II gives an overview of various cancelable biometric systems and discusses the cancelable template transformation for a proven security system and also outlines the motivation for the proposed work. Section III discusses detailed texture analyzes, feature extraction, and the proposed template generation approach. Section IV discusses QR pattern generation and template transformation used for the cancelable biometric system. Performance and security analysis are given in Section V. Finally. Section VI concludes the work.

2. RELATED WORKS

In the cancelable biometric system, a generated template from input biometric traits is applied to some non-invertible transformation. Most generic non-invertible template transformations such as distort template by appending noise patterns and inverse mapping functions have failed to preserve discriminability properties. The limitations imposed by the multi-biometric system due to unique characteristics of different biometric modalities affect both matching performance and security strength during non-invertible template transformation.

In most cases, revocability is established using various fusion approaches [8] in the context of multi-biometric cancelable recognition. Paul et al. [9] proposed a random cross-folding model to formulate the cancelable biometric template from multiple modal biometric systems. The proposed scheme considers a wide range of fingerprint biometrics, and the unique templates are derived from the two levels of random projection after performing feature level fusion. Finally, feature selection was provided using distance-based linear discrimination of feature when both the key and the difference vectors are compromised. This adversary can exploit the compromised information to achieve better

recognition accuracy. Patel et al. [10] proved that even with the non-invertible transformations, still, one can iterate to recover the original biometric templates. Sandhya et al. [11] developed a user key-driven irreversible transformation model for generating a cancelable template. Initially, fingerprint minutiae are extracted and converted into a bit string of equal length, and discrete Fourier transform (DFT) is applied to generate a final template. Finally,a user-defined random matrix is generated based on a given key to accomplish cancelable biometrics. As discussed by Punithavathi and Geetha [12], the performance constraints of non-invertible transformation used for Denial of service Repudiation – a genuine user may access the system. In addition to this to secure the transformed templates within the database to conceal the template is also essential to exploit intruders.

Chee et al. [13] proposed Random Binary Orthogonal Matrices Projection (RBOMP) hashing combined with prime factorization (PF) functions to incorporate the cancelable technique in the biometric speech system. The template consists of fixed-length low dimensional speech utterances which exploit Cepstral Coefficients of an input speech signal. Yang, et al. [14] proposed a layered approach for the cancelable biometric system. In order to accomplish revocability, random projection-based non-invertible template transformation is used for fingerprint biometric traits. The expandable layer is used to conceal the random key used for the transformation.

Hammad et al. [15] developed two cancelable biometric techniques, namely Bio-Hashing and the matrix operation for the ECG authentication system. Feed-Forward Neural Network (FFNN) machine learning is used to validate the authentication of the process. Kau at al. [16] proposed the Random Slope method for revocable and non-invertible template generations. This method also includes dimensionality reduction schemes, which reduce the feature space up to 75% over various biometric modalities.

The primary things that are required to incorporate cancelable biometric for secured bio-cryptosystems as follows:

- Re-usability/revocability
- Irreversibility
- Diversity

In general, cancelable template generation for the unimodal biometric system is a relatively difficult task to accomplish and leads accuracy trade-off measure. Thus, designing a cancelable biometric with appropriate non-invertible template transformation that can meet all the demands like multi diversity, non-invertibility, and revocability without compromising recognition accuracy is a challenging task. In this work, a new attempt is made to carry out hierarchical transformations using QR patterns, which are hard to be understood for attackers.

3. BIOCRYPTOSYSTEM

In general, the bio-cryptosystem is widely accepted to generate a more secure composite biometric template from original input biometric traits without compromising some prominent details. Here, the proposed cipher transformation takes place with simple modulo operations, which is steered by a highly randomized key generation to obtain precise template value, which results in a comparatively better identification rate in biometric identification.

3.1 Texture analyzes, feature extraction and feature selection

In most cases,for texture analysis,a standard texture classification technique the local binary pattern operator has been used. Here, texture patterns are compared with some marginal value, which generates ternary patterns to accommodate all sorts of dynamic textures, as shown in Eq.(1), (2) and (3) where localized properties have been acquiring with the capability to setout the most discriminative patterns for template prototype modeling.

$$RMPc = \sum_{N=0}^{N-1} T(x) * 2^{N} \tag{1}$$

where,

RMPc= Resultant Matrix Pixelcode value in decimal

N= Number of pixels in the neighbourhood of central pixel

T(x) = Threshold function for LBP

$$T(x) = \begin{cases} 1 & if\ x \geq 0 \\ 0 & if\ x < 0 \end{cases} \tag{2}$$

T(x) = Threshold function for LTP upper and lower

$$T(x) = \begin{cases} 1 & if\ np > s \\ 0\ if\ np > d\ \&\&\ np < s \\ -1\ if\ np < d \end{cases} \tag{3}$$

Variable x= np-cp

np = neighborhood pixel value to the central pixel

cp = central pixel of the each decomposed spatial square block

variable s = cp+tk and d = cp-tk, where tk = threshold value

Here two different characteristics are focused during feature extraction, namely spatial and morphological characteristics.The GLCM features are extracted [17] to formulate biometric templates which includes various strategies to exploit the texture property details as follows: Energy, Entropy, homogeneity, correlation values for Orientation measure; Autocorrelation, Prominence, Shade, Dissimilarity, Homogeneity, probability values for Displacement measure; Sum average, Sum variance, Sum entropy, Difference variance, Difference entropy, Information measure of correlation for structural variant measure; Difference normalized, Moment normalized values for statistical measures.And shape features are considered for exploiting the structural appearance of the object of interest.Finally, feature selection approaches are used, which aid in decreasing the size of the template without giving rise to drastic degradation in performance metrics. Here potentially useful texture feature subset are selected from the GLCM feature set extracted by using Eq. (4) to (23) based on its variance measure, which gives prominent discriminations among various classes.

$$Autocorrelation = \sum_{i,j=0}^{M-1} ij(G_{ij}) \tag{4}$$

$$Contrast = \sum_{i,j=0}^{M-1} G_{ij}(i-j)^2 \quad (5)$$

$$Correlation = \sum_{i,j=0}^{M-1} G_{ij} \frac{(i-\mu)(j-\mu)}{\sigma^2} \quad (6)$$

$$\mu = \sum_{i,j=0}^{M-1} ij(G_{ij}) \quad (6.1)$$

$$Peakcorrelation = \sum_{i,j=0}^{M-1} G_{ij} \frac{(ij)-(\mu i.\mu j)}{\sigma^2} \quad (7)$$

$$\sigma^2 = \sum_{i,j=0}^{M-1} G_{ij}(i-\mu)^2 \quad (7.1)$$

$$\mu i = \sum_{i,j=0}^{M-1} i(G_{ij}) \quad (7.2)$$

$$\mu j = \sum_{i,j=0}^{M-1} j(G_{ij}) \quad (7.3)$$

$$Prominence = sgn\,(Z)\,|Z|^{1/4} \quad (8)$$

$$Z = \sum_{i,j=0}^{M-1} \frac{(i+j-2\mu)^4(G_{ij})}{4\sigma^4(1+c)^2} \quad (8.1)$$

$$Shade = sgn\,(X)\,|X|^{1/3} \quad (9)$$

$$X = \sum_{i,j=0}^{M-1} \frac{(i+j-2\mu)^3(G_{ij})}{\sigma^3(\sqrt{2(1+c)})^3} \quad (9.1)$$

$$Dissimilarity = \sum_{i,j=0}^{M-1} |i-j|(G_{ij}) \quad (10)$$

$$Energy = \sum_{i,j=0}^{M-1} (G_{ij})^2 \quad (11)$$

$$Entropy = \sum_{i,j=0}^{M-1} -\ln(G_{ij})G_{ij} \quad (12)$$

$$Homogeneity = \sum_{i,j=0}^{M-1} \frac{G_{ij}}{1+(i-j)^2} \quad (13)$$

$$Probability = MAX_{i,j}(G_{ij}) \text{ for all } i,j \quad (14)$$

$$Variance = \sum_{i,j=0}^{M-1} G_{ij}(i-\mu)^2 \quad (15)$$

$$Sumaverage = \sum_{i=2}^{2M} i.G_{x+y}(i) \quad (16)$$

$$Sum\,variance = \sum_{i=2}^{2M} G_{x+y}(i).(i-\mathrm{Se})^2 \quad (17)$$

$$Sumentropy(Se) = -\sum_{i=2}^{2M} G_{x+y}(i).\log\{G_{x+y}(i)\} \quad (18)$$

$$Difference\ variance = \sum_{x,y=0}^{M-1} \mathrm{var}(G_{x-y}) \quad (19)$$

$$Differenceentropy = -\sum_{i=0}^{M-1} (G_{x-y}(i).\log\{G_{x-y}(i)\}) \quad (20)$$

$$Infmcorr = \frac{PH_{XY} - PH_{XY}1}{\max(PH_X, PH_Y)} \quad (21)$$

$$PH_{XY} = -\sum_{i,j=0}^{M-1} G_{ij}\log(G_{ij}) \quad (21.1)$$

$$PH_{XY}1 = -\sum_{i,j=0}^{M-1} G_{ij}\log(Gx_iGy_j) \quad (21.2)$$

$$Differencenormalized = \sum_{i,j=0}^{M-1} \frac{C_{ij}}{1+(i-j)} \quad (22)$$

$$C_{ij} = \sum_{i,j=0}^{M-1} \frac{G_{ij}}{\sum G_{ij}} \quad (22.1)$$

$$Momentnormalized = \sum_{i,j=0}^{M-1} \frac{C_{ij}}{1+(i-j)^2} \quad (23)$$

where,

Elements i and j are intensities between 0 and grey level-1(Spatial coordinates)

G_{ij}= Grey Level Co-occurrence Matrix(Normalized symmetrical GLCM)

M = Number of grey levels or dimension of the co-occurrence matricx

μ= GLCM mean with respect to i and j

μ_i= GLCM mean with respect to i

μ_j= GLCM mean with respect to j

Sgn(x)= sign of real number

Infmcorr = Information measure correlation

PH_X and PH_Y denote the entropy values of G_x and G_y respectively.

G_{x+y} and $G_{x-y}$are sum and different distribution functions respectively

σ 2= variance

C= The Correlation feature

3.2 Template generation

The biometric cryptosystem can improve accuracy with improved security and privacy. Here, the biometric level fusion is combined with template level fusion to provide higher security than all other unimodal fusion. This Unimodal system fuse information at the feature level, and different sets of biometric texture features generate different feature spaces. To make this non-uniform feature sets into convenience for application deployments and to regulate the inter and intra-class variations feature dimensions also optimized [18] based

on the principal component (PCA) analyses, as shown in Figure 1. As compared to mutual content reduction using Independent Component Analysis (ICA) and discriminative subset selection using Linear Discriminant Analysis (LDA) proposed hierarchical PCA transform helps to reduce confusion metrics as well as dimensions.

Here texture features are extracted from three different texture regions along with shape features during feature extraction, not only increase the template size also carry redundant information. Moreover, it is always difficult to obtain discrimination with redundant data. PCA transform is used to select attributes by considering both consistency and correlative measures in a hierarchical manner to accomplish this task.

4. CANCELABLE BIOMETRIC SYSTEM

Cancelable biometric is used to convert the generated template into the irreversible transform domain for template security. These transformations take place in such a manner that they should not be recoverable, and the entire input feature sets are transformed using a one-way function. In general, there is no unified cancelable template generation methodology for biometric templates since it affects the discrimination level of various biometric classes and decreases the interclass distance between biometric traits. This transformation depends on input biometric characteristics and differs based on its applications. Here various aspects for cancelable template biometrics are achieved as shown in Table 1.

4.1 QR pattern generation

During template transformation,initially, randomized key values are used for cipher conversion. In order to increase the level of security and cancelable metrics color variants are applied for each QR code which is selected based on color selection keys, and this will give major breaking points for as intruder or hacker, and the ranges of colors consider for the QR patterns gives nothing to them to restore the converter data. This color selection not only offers maximum storage space to accommodate also provides many useful potential benefits as follows: (i) The randomization in channel color selection offers significant non-inevitability measures (ii) build in error correction metrics of QR patterns gives reduce false detection rate during validation (iii) due to compound template generation, the variation in input biometric trails won't tolerate at the validation process since each template constitutes fine details from a different type of biometric in the fingerprint system. The QR code pattern generation follows hierarchical data conversion, which includes alphanumeric encoding, data grouping, and parity generation for forwarding error correction.

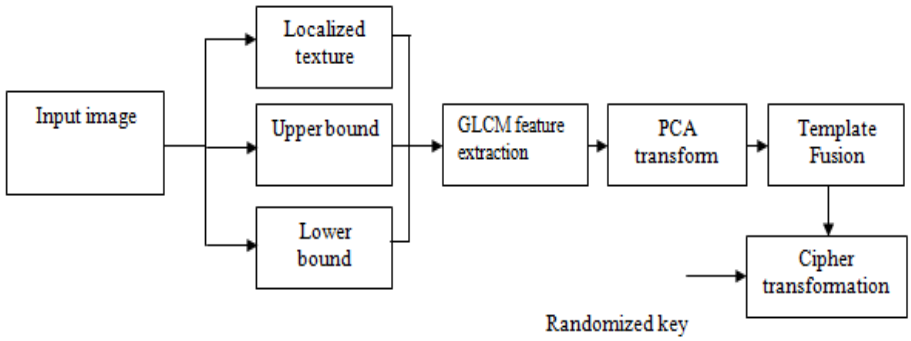

Figure 1. The secured template generation using texture computation and cipher conversion

Table 1. An inherent property of the cancelable biometric system

Property measure	Description	Steps involved
Revocability	Same biometric data input should produce different output for different randomization	Here highly randomized key generation model is used for each of transformations
Non-invertibility	Difficulty in extracting/decrypting input biometric information from cancelable biometric templates or finding the transformation key used	Stage 1- key-driven modulo operation Stage 2- key-based color selection Stage 3- key-based pattern selection
Diversity	output related to the same biometric data should produce different outputs using different key sizes, values, or methodologies. Both randomized key and user-defined unified models are used for template protection.	Set 1- randomized key used for three stages Set 2 –user-defined model Encoding model Grouping model

4.2 Color selection

Here QR pattern generation is incorporated in the cancelable biometric not only to confuse intruders and also due to its ease of integrations followed by its prominence in concealing the information. Here QR patterns are generated for given input cipher data with configurable pattern size, which is selected according to the template size. Highly randomized keys are used for color selection, which has a dynamic range equal to the number of color combinations considered for any color images. During color conversion, each binary coded QR patterns converted into equivalent R,G,B color components according to the key values. The channel values associate with the given key values is statistically computed and stored.This constrained randomization and key selection provide improved revocability since compromised keys or colors can be re-enrolled for another transformation. This key-based color

selection not only preserves privacy also improves the non-invertibility since it is computationally difficult to restore the generated cipher template from a color QR pattern. As compared to other template schemes like binary encoding and randomized data conversion, QR pattern generation from biometric templates retains all basic characteristics during the conversion process, which gives rise to the overall recognition accuracy.

5. EXPERIMENTAL RESULTS

In this brief, the ultimate goal is to validate the performance metrics of the ternary threshold bounded texture model over a wide range of the fingerprint biometric system, as shown in Figure 2, which includes FVC2002 DB2, FVC2004 DB1, and FVC2006 DB2 to carry experimental results for performance validation. The data sets include 100 biometrics from each fingerprint data set, where each class comes with different levels of non-linear distortion, textural exploration, and image quality to prove the improved recognition accuracy. It was noted due to its distortion, morphological characteristics are inconsistent with FVC2004 DB1, and FVC2006 DB2 offers the least relevant spatial details. But the different levels of attributes with PCA based feature attribute selection and transformation metrics of color variant QR transformation based irreversible transformations for cancelable template generation the associated degradation in overall system accuracy is minimized irrespective of the nonlinearity of the input object classes. In order to validate this, the proposed cancelable biometric is tested on a variety of fingerprint databases with moderate quality and texture details, as shown in Table 2.

From the obtained experimental results, the proposed texture model outperforms the state-of-the-art BioHashing LBP model [19], as shown in Table 3 in terms of template size. The recognition accuracy of QR color variant cancelable templates is compared in terms of Equal Error Rate(EER) measures, as shown in Table 3. As a result, it is well proved that using color driven QR pattern-based cancelable biometric template with appropriate texture computation as shown in Figure 3 and the GLCM feature set as shown in Figure 4 achieved better data retention with no significant changes as compared to Discrete Fourier Transform driven random projection model [20] and BioHashing function [19] in terms of the EER (%) matching rate performed over the FVC2004 DB1 database.

From the experimental results, it was found that PCA based feature selection optimally reduced the dimension set as shown in Figure 5 and also proved that through QR pattern and color conversion process as shown in Figure 6 not degrade the system accuracy significantly, and it is proved that the proposed QR pattern-based cancelable method attains better performance as shown Table 4.

In the cancelable biometric system, the transformed templates must adhere to act in accordance with security,revocation,and diversity requirements. The performance metrics of any template transformations are validated based on two key factors as follows: (i) The one-way transformation should not change the statistical characteristics of the input biometric template with any number of transformations; (ii) The performance metrics during authentication should be high with improved in variance level over input biometric trait changes.

Table 2. Parameters cogitation for the validation

Parameters	Features
Number of biometric images tested	400
Image Category Set 1	FVC2002 DB2
Image Category Set 2	FVC2004 DB1
Image Category Set 3	FVC2006 DB2
Image Types for Set 1, Set 2 and Set 3	.TIF, .TIF and .BMP formats
Image quality for Set 1, Set 2 and Set 3	296x560, 640x480 and 300x480

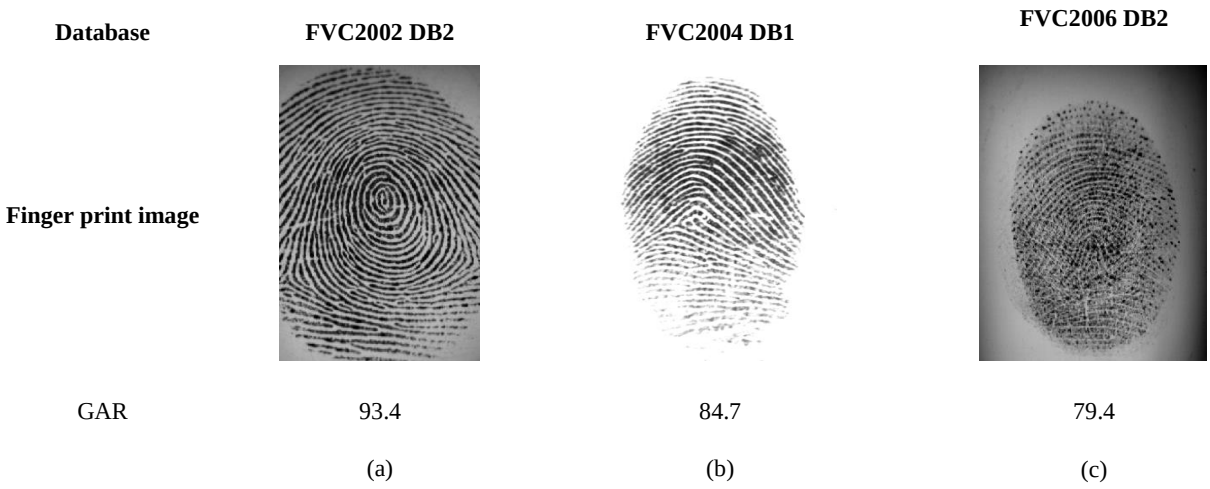

Figure 2. The fingerprint biometric samples from the databases: (a) FVC2002 DB2, (b) FVC2004 DB1, (c) FVC2006 DB2

Table 3. Performance metrics of dimensionality reduction and feature level fusion on texture features

Method	Texture classification model	Initial dimension	Dimension after PCA transform	Computational redundancy
BioHashing[19]	LBP	256	38	85%
Proposed work with feature level fusion	Ternary threshold bounded model	60	4	93%

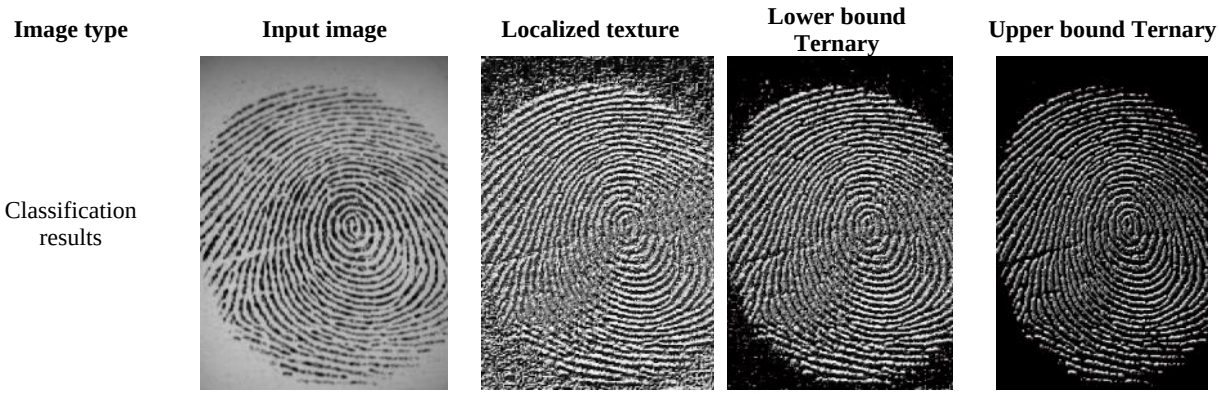

Figure 3. The classification results used for the texture computation

Table 4. Performance comparison of different cancelable biometric approaches from state of the art on the FVC2004 DB1 database (EER in %)

Method	Cancelable biometrics approach	EER (%)
BioHashing [19]	Randomized texture feature projection over the secret place	30.1
Discrete Fourier transform and random projection[20]	Template conversion into a complex form	15.57
The proposed work	Color variant QR pattern	13.43

```
Autocorrelation: 2.027445186707777e+001
       Contrast: 2.291217026378897e+001
    Correlation: 6.425106110939381e-002
PeakCorrelation: 6.425106110939377e-002
     Prominence: 1.277146972827687e+003
          Shade: 4.993817070895034e+000
  Dissimilarity: 3.273167180541281e+000
         Energy: 2.513484330726580e-001
        Entropy: 1.383632140590627e+000
    Homogeneity: 5.908541024323398e-001
    probability: 2.784160426760632e-001
       Variance: 3.159916500393435e+001
     sumaverage: 8.829008221993833e+000
     sumvariance: 8.642354169554808e+001
     sumentropy: 1.059519812356892e+000
   Diffvariance: 2.291217026378897e+001
    Diffentropy: 6.910455802327749e-001
infmeasurecorrelation: -2.981037172993483e-003
    Diffnormalized: 7.817888546305813e-001
momentnormalized: 7.972374312939030e-001
```

Figure 4. GLCM feature set

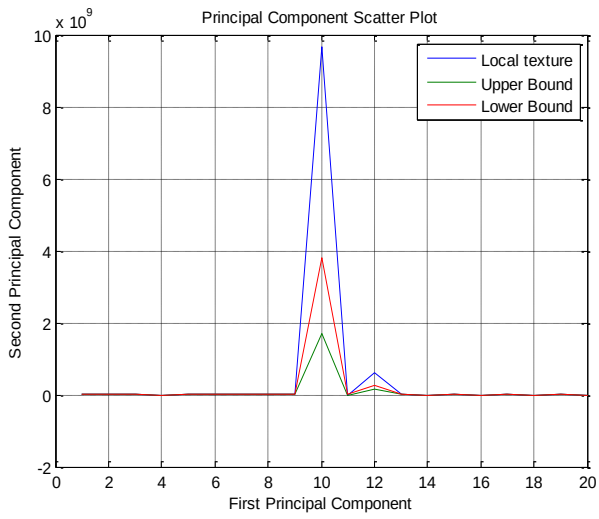

Figure 5. The Principal component analyzes of GLCM feature variants from each texture feature image set

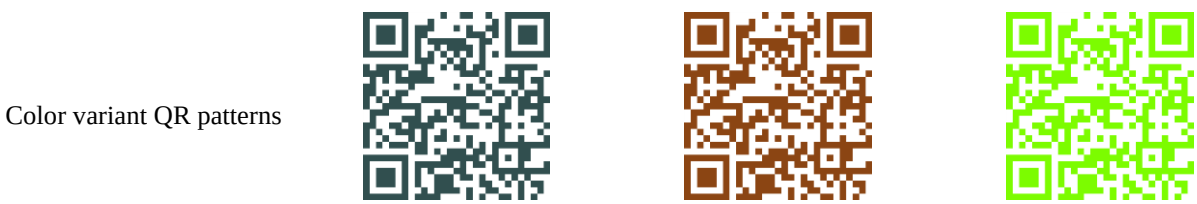

Figure 6. The cancelable biometrics through the conversion of templates into a color QR pattern

6. CONCLUSION

In this paper, texture analysis based template generation for fingerprint system is proposed and color QR pattern analysis for the cancelable biometric system. This process involves several transformations such as template generation, cipher transformation, and QR pattern conversion. This hierarchical template transformation has the advantages of randomization with improved security against an exhaustive attack. Here due to the integration of GLCM texture features extracted from different texture classified images followed by PCA transformation based feature normalization, final templates comprise of low-dimensional feature space representation and robust against intra and interclass problems that arise due to large non-linear distortion and low image quality. The experiment results obtained from the proposed system; it is demonstrated that the discrimination level of the transformed template does not differ during the one-way-mapping process. This color and pattern variants based template transformation inherits randomness required for an unpredictable template. Here, this QR pattern-based non-invertible function satisfies both quality metrics and non-invertibility requirements for the improved cancelable biometric system. Finally, this unique optimal color QR model is proved to be meet the following systemrequirements, such as non-invertibility, security, accuracy, randomness, and flexibility.

REFERENCES

[1] Eckhoff, D., Christoph S.(2014). Driving for big data? Privacy concerns in vehicular networking. IEEE Security & Privacy, 12(1): 77-79. https://doi.org/10.1109/msp.2014.2

[2] Hosseinzadeh, D., Sridhar, K. (2008). Gaussian mixture modeling of keystroke patterns for biometric applications. IEEE Transactions on Systems, Man, and Cybernetics, 38(6): 816-826. https://doi.org/10.1109/tsmcc.2008.2001696

[3] Garcia, P. (2018). Biometricsonthe blockchain. Biometric Technology Today, 5: 5-7. https://doi.org/10.1016/s0969-4765(18)30067-5

[4] Stoianov, A. (2010). Cryptographically secure biometrics. In Biometric Technology for Human Identification VII. 7667, 76670C. International Society for Optics and Photonics. https://doi.org/10.1117/12.849028

[5] Saini, N., Aloka S. (2013). Biometrics based key management of double random phase encoding scheme using error control codes. Optics and Lasers in Engineering, 51(8): 1014-1022. https://doi.org/10.1016/j.optlaseng.2013.03.006

[6] Adamovic, S., Milan, M., Mladen, V., Marko, S., Aleksandar, J. (2016). Fuzzy commitment scheme for generation of cryptographic keys based on iris biometrics. IET Biometrics, 6(2): 89-96. https://doi.org/10.1049/iet-bmt.2016.0061

[7] Teoh, A.B.J., Yip, W.K., Sangyoun, L. (2008). Cancellable biometrics and annotations on biohash. Pattern recognition, 41(6): 2034-2044. https://doi.org/10.1016/j.patcog.2007.12.002

[8] Canuto, A.M.P., Fernando, P., João, C.X. (2013). Investigating fusion approaches in multi-biometric cancellable recognition. Expert Systems with applications, 40(6): 1971-1980. https://doi.org/10.1016/j.eswa.2012.10.002

[9] Paul, P., Marina G., Stanislav, K. (2014). Situation awareness of cancelable biometric system. The Visual Computer, 30(9): 1059-1067. https://doi.org/10.1007/s00371-013-0907-0

[10] Patel, V.M., Nalini, K.R., Rama, C. (2015). Cancelable biometrics: A review. IEEE Signal Processing Magazine, 32(5): 54-65. https://doi.org/10.1109/msp.2015.2434151

[11] Sandhya, M., Munaga, V.N.K., Raghavendra, R. (2016). Generating cancellable fingerprint templates based on Delaunay triangle feature set construction. IET Biometrics, 5(2): 131-139. https://doi.org/10.1049/iet-bmt.2015.0034

[12] Punithavathi, P., Geetha, S. (2017). Can cancellable biometrics preserve privacy? Biometric Technology Today, 7: 8-11. https://doi.org/10.1016/s0969-4765(17)30138-8

[13] Chee, K.Y., Zhe, J., Danwei, C., Ming, L., Yap, W.S., Lai, Y.L., Goi, B.M. (2018). Cancellable speech template via random binary orthogonal matrices projection hashing. Pattern Recognition, 76: 273-287. https://doi.org/10.1016/j.patcog.2017.10.041

[14] Yang, W.C., Wang, S., Zheng, G.L., Chaudhry, J., Valli, C. (2018). ECB4CI: An enhanced cancelable biometric system for securing critical infrastructures. The Journal of Supercomputing, 74(10): 4893-4909. https://doi.org/10.1007/s11227-018-2266-0

[15] Hammad, M., Luo, G.N., Wang, K.Q. (2019). Cancelable biometric authentication system based on ECG. Multimedia Tools and Applications, 78(2): 1857-1887. https://doi.org/10.1007/s11042-018-6300-2

[16] Kaur, H., Khanna, P. (2019). Random Slope method for generation of cancelable biometric features. Pattern Recognition Letters, 126: 31-40. https://doi.org/10.1016/j.patrec.2018.02.016

[17] Haralick, R.M., Shanmugam, K., Dinstein, I.H. (1973). Textural features for image classification. IEEE Transactions on Systems, Man, and Cybernetics, 3(6): 610-621. https://doi.org/10.1109/TSMC.1973.4309314

[18] Kalluri, H.K., Prasad, M.V.N.K., Agarwal, A. (2012). Palmprint identification based on wide principal lines. In Proceedings of the International Conference on Advances in Computing, Communications and Informatics, pp. 918-924. https://doi.org/10.1145/2345396.2345544

[19] Belguechi, R., Hafiane, A., Cherrier, E., Rosenberger, C. (2016). Comparative study on texture features for fingerprint recognition: Application to the BioHashing template protection scheme. Journal of Electronic Imaging, 25(1): 013033. https://doi.org/10.1117/1.jei.25.1.013033

[20] Alam, B., Jin, Z., Yap, W.S., Goia, B.M. (2018). An alignment-free cancelable fingerprint template for bio-cryptosystems. Journal of Network and Computer Applications, 115: 20-32. https://doi.org/10.1016/j.jnca.2018.04.013