



Disseminating the Authentication Process Based on Secure RGVSS Multi-Biometric Template Encryption through QR Code in Health Care Informatics

Devendra Reddy Rachapalli¹ and Hemantha Kumar Kalluri²

¹Department of Computer Science & Engineering,
Srikalahasteeswara Institute of Technology, Srikalahasti, (Andhra Pradesh), India.

²Department of Computer Science & Engineering,
Vignan's Foundation for Science Technology and Research University, Vadlamudi, (Andhra Pradesh), India.

(Corresponding author: Devendra Reddy Rachapalli)

(Received 06 July 2019, Revised 23 September 2019, Accepted 03 October 2019)

(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: In recent years, the use of biometrics for person authentication and image encryption to achieve and maintain the security of the image is extensively used. A competitive call is made for the researchers in transmission of digital data with truth of security is prioritized in image applications, in particular, Health Care Informatics (HCI). A novel method is proposed to cater to these requirements, which realizes the properties of Random Grid Visual Secret Sharing through the Quick Response Code (RGVSSQRC). RGVSSQRC provides perfectness, idealness, storage, and contrast requirements for preventing authenticating information from stolen attacks. The objective of the present research paper is to disseminate the use of Random Grid Visual Secret Sharing (RGVSS) for multi-biometric template encryption in medical applications without the use of any key for generating secret cipher shares with optimal contrast and aspect ratio for better vision through Quick Response (QR) Code.

Keywords: Biometrics, QR Codes, Security, visual secret sharing, Visual cryptography, Authentication.

I. INTRODUCTION

In HCI applications, multimodal biometric cryptosystems use different biometric modalities for accurate person authentication and key generation purposes. The fused biometric traits increase correctness and robustness. Thus, the extraction of essential features from biometric modality is called a biometric template. The fusion of biometric traits performed at various stages. They are known as image stage, feature stage, match score stage and decision stage [1]. There are two classes of biometric template protection techniques, namely Biometrics Cryptosystems (BC) and Cancellable Biometrics (CB). Of these two categories, the CB template protection technique is good in preventing database stolen attacks compared with the BC template protection technique [2].

The fused biometric template information can be encoded in the QR Code since it is quite compatible with QR Codes which are being widely used everywhere for quick reading of information. The encoded QR code is an image containing some valid information, which is subjected to encryption by using either symmetric block cipher techniques with a secret key such as AES or asymmetric block cipher schemes such as RSA, Elliptic Curve Cryptography, etc.

The existing medical management application systems have been used effectively in biometric based authentication, and also, these methods have been used to access patient records along with medical images by watermarked encryption. However, there is a chance of providing more security and confidentiality of the patient information with quick access through QR Codes than the previous study [3]. In this paper, the "proposed method is developed for achieving better

results in terms of fulfilling an increase in the speed of providing patient information access with better vision and the perfectness of patient authentication by using RGVSSQRC".

The encrypted image can be divided and distributed by VSS(k,n) cryptographic principle. The total number of secret shares generated as an output of VSS(k, n) is 'n'. By collecting $k \leq n$ number of secret shares from 'n' participants, it is possible to generate a secret QR image. According to VSS(k, n) cryptographic principle, when a person tries to combine (k-1) number of secret shares, it does not reveal the original encrypted QR image. The RG based VSS efficient technique is developed for implementing secure multi-biometric template protection for patient identification through QR Code without using any keys for image transmission in HCI.

While section I of the present research paper discusses providing better security to the information by using RG based VSS techniques, the rest of the paper discusses various other related issues in the following parts. Section II explores the preliminaries of QR Codes and VSS techniques. While section III deals with reviews about literature work. Section IV exploits the beauty of the proposed work. Section V analyzes the experimental results. Section VI contains the conclusion. The future scope statement is given in section VII.

II. PRELIMINARIES

A. Biometrics

In HCI applications, secure data transmission over the internet worked services is more essential in terms of patient authentication, data confidentiality and integrity. At present, the biometric based authentication [4] has become the most popular method for patient

identification than various conventional authentication schemes. In connection with increasing the speed of visual data reading, which is transmitted over the network, the QR Code is combined with a biometric based authentication process is used [5] as a foundation to ensure integrity and confidentiality of the security system.

The unimodal biometric recognition system has less accuracy than a multimodal biometric fusion recognition system [6-8]. In HCI applications, medical image fusion increases authentication accuracy by avoiding artificial noise. As per the comparative study made [9], there are several methods for the extraction of most prominent features from the original fused biometric for information retrieval systems. From the extracted biometric template, a unique biometric key [10] can be generated, which can be used for either image encryption or unique identification generation purposes.

B. Error correction codes

In medical applications, for patients identification(ID) purposes, traditional 2D barcodes are replaced with QR Codes. QR Codes are more effective in storing a large amount of information than 2D barcodes. The length of data that can be encoded is limited to 40 characters only [11, 12]. But by using QR Codes data loss can be reduced up to 70 percent based on Error Correcting Code (ECC) Levels. Further, the QR Code not only encodes and distributes data related to a secret in many shares but also it has an inbuilt mechanism to correct errors [13]. Data masking is used to modify the QR Code to make it as easy for QR Code readers to scan as possible. QR Codes are read by QR scanners even though they are presented in any direction due to their automatic alignment feature.

C. Random grid visual secret sharing

Ranjan *et al.*, [14] proved Visual Cryptography (VC) which is playing an important role in many applications for images or text encryption/decryption with pixel expansion and without pixel expansion methods for security purposes. It is also shown that in the pixel expansion technique, the resolution of the resulting decrypted image is diminished. VC can be used in biometric template protection applications. VSS (n,n) generates 'n' shares from the secret, and those 'n' shares can be transferred to all 'n' number of participants.

Later, all participants have to genuinely support in combining all required shares required to reveal the original secret. The principle of VSS [15] says that the combining of even one less than the required number of shares can not reveal the original secret if all the 'n' number of shares are required to combine to reconstruct the original secret. Normal VSS with pixel expansion takes more storage space, computationally complex, and increase in bandwidth, which causes increases in power consumption and decreases in contrast [16]. The size of each VSS shares increases exponentially as pixel sizes increases. A variant of VSS called RG VSS is proposed, which reduces storage space by generating 'n' random grids without codebook design

A system is developed[3] to overcome the traditional watermarked image attacks by using a visual encryption method. The visual watermarked image is encrypted by

[17, 18]. The size of every RG VSS cipher secret share is equal to that of the original secret.

III. REVIEW ON LITERATURE

A system is developed[19] to made a conclusion that, a much better security of data transmission in the networked spread services is achieved in hybrid security mechanisms than normal information security techniques, such as cryptography and steganography by duly considering the following parameters PSNR, entropy, keyspace, encrypted code, and embedding capacity. In HCI applications, image encryption is very important because of data confidentiality, legibility, and integrity. Image encryption has to be performed [20, 21] by decomposing the original image into color Red, Green and Blue components without loss of any valuable information and any change in image size. The QR Codes have been widely used in digital watermarking and steganography applications for image encryption and text hiding purposes.

It is proved that[22], in normal Secret Sharing schemes, the secrets and shares consist of numerical data and computer systems are used for their decryption. But in VSS, both secrets and shares are visible, and their decryptions are visually observable to the naked eye. It is possible to achieve a better practical resolution of share images by using the lower pixel expansion. The phrase 'pixel expansion' refers to the presence of subpixels in a secret share which is encrypted from a pixel in secret. It is important to note that the optimization of a VSS scheme and encryption can be achieved with the lowest pixel expansion. The access structures for a single secret are better in contrast and lower pixel expansion than multiple secrets. The adversary attacks for decryptions are more difficult if VSS is applied to encrypting multiple secrets. Bakshi [23] developed a scheme with a VSS(2,2) for telemedicine applications. The data sensitivity and confidentiality are prominent parameters on a public network against passive or active attackers. The VC methods are novel keyless encryption on par with watermarking or conventional image encryption algorithms [24, 37].

Xuehu & Yuliang [25] have analyzed security defects in medical management and introduced the possible use of QR Codes to improve the security in medical management applications by using a visual security technique called RGVSS (2, 2). The patient's biometric trait is used for feature extraction, and the extracted biometric template is combined with basic patient information for accurate authentication purposes. In hybrid biometric traits, one biometric trait can be used for authentication purpose and another can be used for key generation purposes [26]. With enhanced utilization, CB based key generations are more secure and dependable than conventional biometric cryptanalysis [27]. These methods can be further made efficient and sophisticated with the combination of VSS technologies with QR Codes [28] by deeply integrating the error-correcting codes for better recovery of the original information as an output of QR Code image scan reader device with keyless encryption/decryption of secret.

using biometric keys to attain more security than traditional password based authentication. In this scheme according to pixel expansion the original pixel is

expanded to four sub-bands LL, LH, HL, and HH respectively. This shows pixel expansion four times the original pixel. The aspect ratio of the pixel in original image and expanded image is 1:1 for pixel expansion 1. According to Table 3, the intensity difference of the original image and encrypted image is 0.00023. In connection with ciphering, this technique has been used wavelet filter set as a key.

To avoid the pixel expansion problems like lossless reconstructing of original secret and storage requirements [29] given an alternative promising solution for the information security conditions, fast network transmission, computation complexity, storage management and reconstructing the original secret perfectly without any distortions by using an optimal(k,n) threshold VSS based on matrices transposition operation. According to Table 3, the visual quality of the encrypted image for pixel expansion 1 is the same original image.

On par with pixel expansion VSS, the RGVSS scheme is better in the utilization of storage space [35, 36]. The contrast value is nearer to threshold value '0' and aspect ratio for any pixel expansion is also equal to 1:1. The processing time for pixel expansion VSS is a bit overhead compared to RGVSS. The shadow of the reconstructed image is decreased and visual quality increased.

In recent years in RGPVSS [30], it is proposed an alternative technique for secret sharing through the internet for avoiding pixel expansion problems in traditional VSS without any encoding matrices by algorithm 4. In VSS schemes the cipher shares are

distributed among different participants in a network. In such a scenario, it is very difficult for the cryptanalysts to deciphering. In the telemedicine applications, the patient data along with his/her photo can be embedded in the QR Code, which can be submitted to the VSS process for maintaining better confidentiality and fast accessing information.

IV. PROPOSED METHOD

The design of the proposed system is giving out in Fig. 1. Here, in this section, it is described by different modules and the flow of information from patient enrolment to validation. The proposed method consists of the following primary modules. They are image-level fusion, biometric template generation, QR Code generation and secret encryption or/and decryption by using RGVSS.

A. Image level fusion

Uludag *et al.*, [31] explained the importance of multi-biometric template generation in a transformed domain, which is more accurate and difficult to forge than traditional biometric template generation from single biometric modality. They have compared the choice of selecting a combination of biometric modalities for fusion. According to Table 1, the biometric modalities selected to perform fusion operation are Iris and Palmprint because of their universality, distinctiveness, permanence, and collectability. On par with all the existing biometric traits, Iris is the universal trait for color and shape feature extraction.

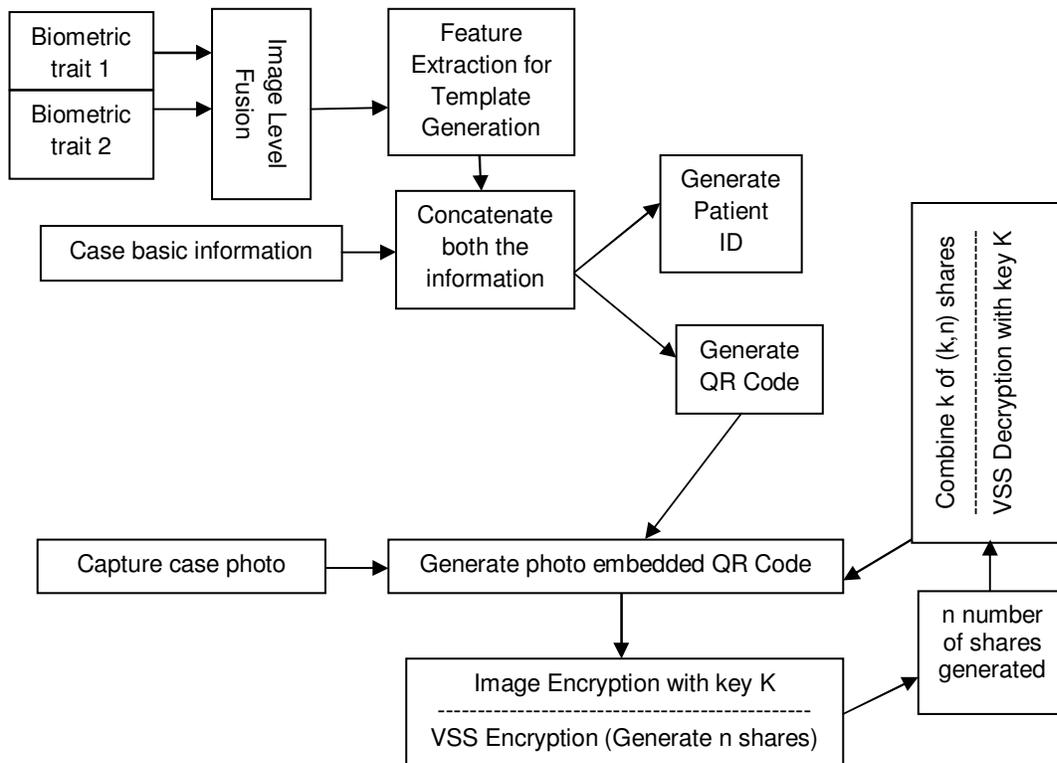


Fig. 1. The design of the proposed system.

While considering the trustability of person authentication, the physical biometric traits are more collectible and permanence than behavioral biometric modalities.

To implement image-level fusion individually collect the person biometric modalities with the machine in a better environment in global positioning. In the proposed image level fusion activity, apply Discrete Wavelet Transformation (DWT) on individual patient biometric modalities to get multi-biometric fusion output, and then use inverse Discrete Wavelet Transformation (IDWT) to complete image level fusion process for generating a fused image as shown in Fig. 2. For better accuracy purposes. The image-level fusion can be considered as input for the next module to extract features.

B. Patient ID generation through the biometric template
 A method has been developed[32] for the multi-biometric template generation by forming a fused image with the following sub-modules. They are, namely, Local Binary Pattern for texture classification, GLCM Technique for essential feature extraction and finally PCA for most prominent feature selection. In this work, after applying these steps, a template is generated. From this template, the HCI administrator will generate a unique patient ID by concatenating the sum value of template feature values and alphanumeric random value generated by applying random key generation function. The flowchart of this sub-module work for patients' ID generation is shown in Fig. 3.

Table 1: Collation of various biometric modalities for the right choice.

Biometric modality	Universality	Distinctiveness	Permanence	Collectability	Performance
Iris	High	High	High	Medium	High
Palmprint	Medium	Medium	Medium	High	Medium
Voice	Medium	Low	Low	Medium	Low
Face	High	Low	Medium	High	Low

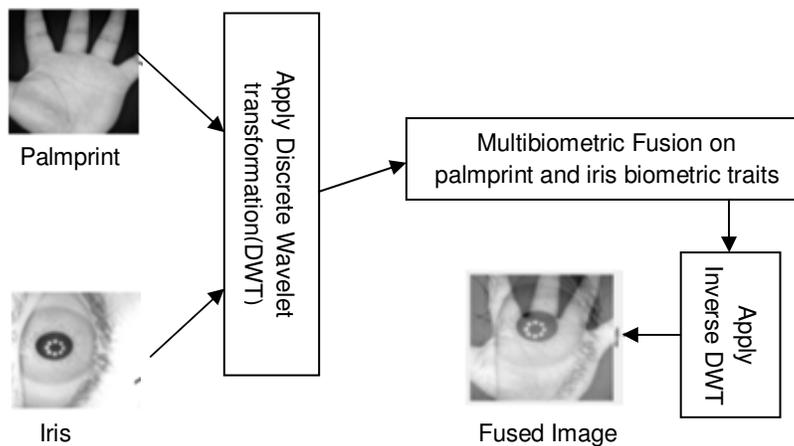


Fig. 2. Multi Biometric Image-Level Fusion.

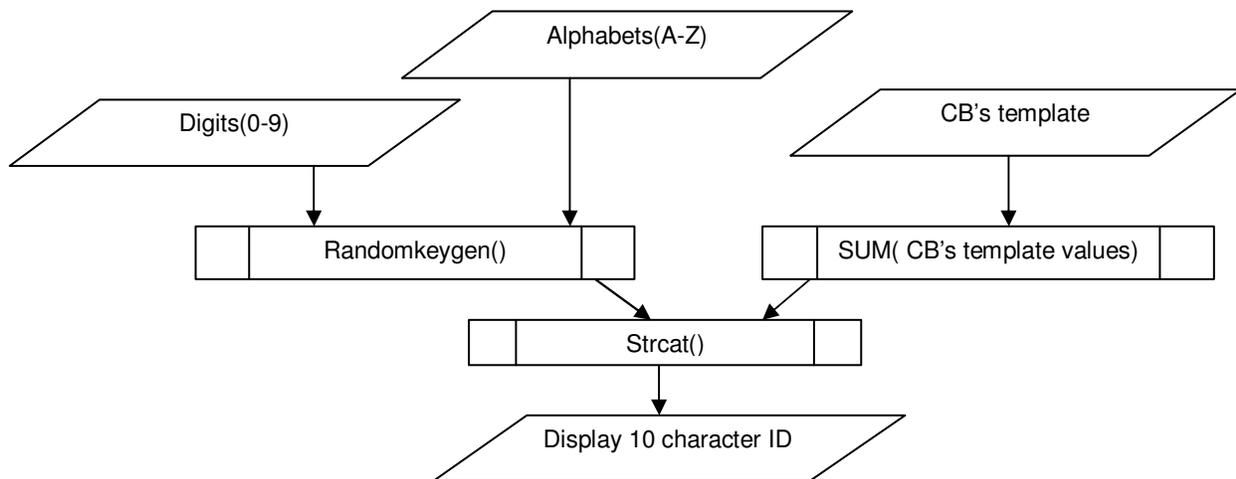


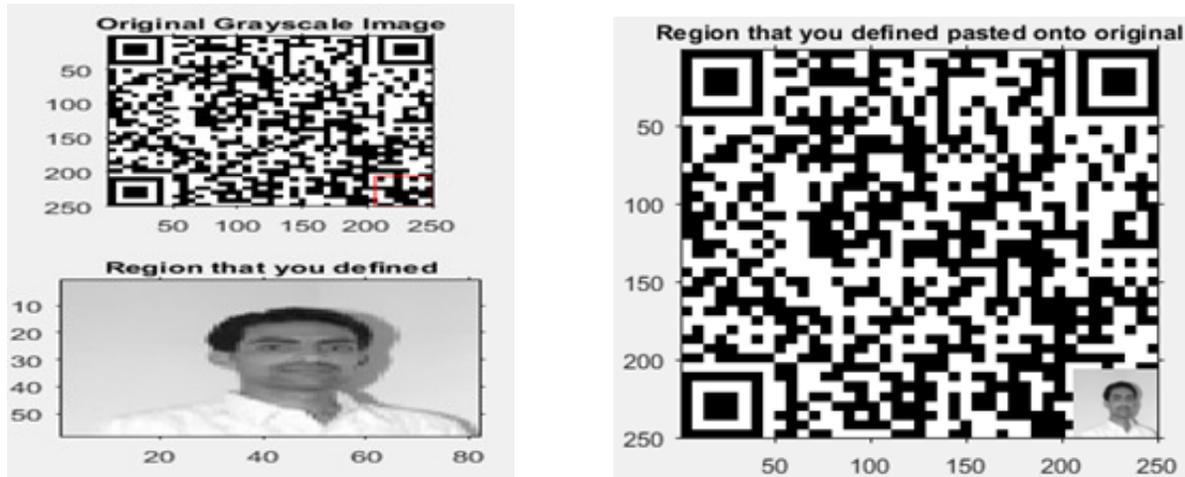
Fig. 3. Patients' ID generation.

C. Generating QR code

The primary purpose of this module has generated a scan read QR pattern, which contains patient details, as shown in Fig. 4 (a). Rachapalli & Kalluri [33] succeeded in developing a module to encode biometric template data in QR Code for quick and swift authentication.

In this work, the hybrid information of the patient is protected in the form of the QR Code by using Reed

Solomon code. The above Fig. 4 (b) shows the patient's photo embedded QR Code along with basic information for fast authentication of patient information at a later stage in the validation of the proposed system. In this activity, the Q level of ECC and version six of the QR Code is used for simulating the objective of the proposed system.



(a) QR Code showing patient details.

(b) Patient photo embedded QR Code.

Fig. 4. QR Code generation.

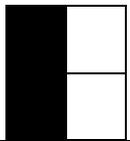
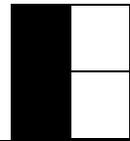
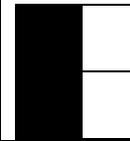
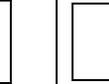
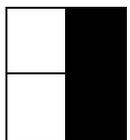
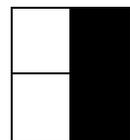
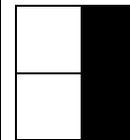
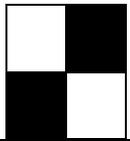
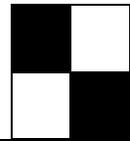
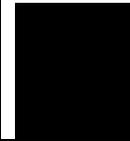
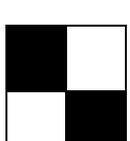
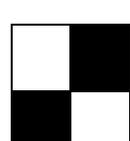
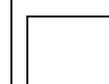
Pixel Type	Probability	VSS with pixel expansion			RGVSS		
White 	0.5						
White 	0.5						
Black 	0.5						
Black 	0.5						

Fig. 5. Pixel expansion VSS versus RGVSS for shares generation.

D. RG VSS (4, 4) encryption and decryption

There is a difference between VSS with pixel expansion and without pixel expansion methods. The later scheme requires less storage space than the former scheme, which is compared in Fig. 5. The photo embedded QR code as obtained in Fig. 4 (b) is encrypted with an HCI administrator's public key 'K', it will generate an encrypted QR pattern image shown in Fig. 6 is called a secret.

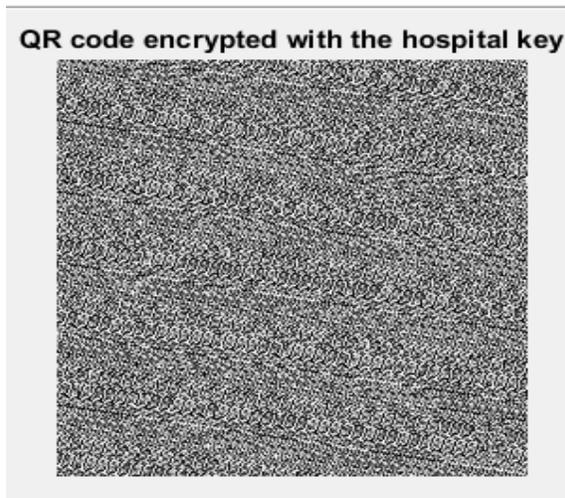


Fig. 6. Encrypted QR code as a secret.

In the recent era, it has become essential to transmit shares of the secret among more than two numbers of participants in an internetwork for many types of HCI applications. Apply RG based VSS (n, n) algorithm1 in algorithm 4 [34] on the encrypted secret to generating 'n' number of shares. They proposed a basic fundamental way on how to extend RGVSS (2, 2) to RGVSS (n,n) without codebook design and no pixel expansion to overcome the distortions in reconstructing the original secret as shown in algorithm1 and algorithm 2 for 'n' number of random grids generation. Here the pixels in the cipher grids are created in three ways with an equal probability of black and white pixels. They are Randomization, complements, and equivalence. The

pixel creation done by the above three methods is shown in equation (1), (2), and (3) respectively.

$$(1). Fr(P_Probability) = \begin{cases} 0, & P(\text{white or black}) = 0.5 \\ 1, & P(\text{white or black}) = 0.5 \end{cases}$$

$$(2). Fr(P_complement) = \begin{cases} 0, & \text{if } x = 1 \\ 1, & \text{if } x = 0 \end{cases}$$

$$(3). Fr(P_equivalence) = \begin{cases} 0, & \text{if } y = 0 \\ 1, & \text{if } y = 1 \end{cases}$$

After the first cipher grid CRG1 is created from secret S, the process is extended recursively by using cipher grid chain principle. The secret 'S' is the first split into cipher grid CRG1 and semi cipher grid RG2. The CRG1 is randomly generated first by using flip coin function method. Later the second cipher grid CRG2 is generated corresponding to secret S and RG2. Likewise, the process is continued until generating 'n' number of shares. shares generation flowchart is shown in Fig. 7.

Algorithm 1.

RGVSSQRC (n, n) secret(S, n)

Step 1. Create cipher grid CRG1 and semi cipher grid RG2

Step 2. CRG1 || RG2 = randomgrids(S)

Step 3. Create CRG2 to CRGn as cipher grids recursively

if(n>2)

For k= 2 to n-1

CRG_k || RG_{k+1} = randomgrids(RG_k)

Step 4. Create CRGn as the last cipher grid

CRGn = RGn

Algorithm 2.

Randomgrids(secret)

Step 1. Create CRG1 as first cipher grid

CRG1[i, j] = Fr(P_probability), for all i and j

Step 2. Create CRG2 as another cipher grid

Create white area of CRG2 corresponding to secret by CRG1

CRG2 [secret(0)]= Fr(P_equivalence)(CRG1[secret(0)])

Create black area of CRG2 corresponding to secret by CRG1

CRG2 [secret(1)]= Fr(P_complement)(CRG1[secret(1)])

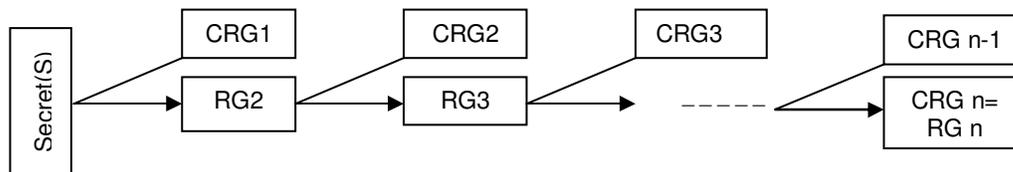


Fig. 7. RGVSS (n, n) chain for shares generation.

V. RESULTS AND COMPARATIVE ANALYSIS

In this activity from an obtained secret, four numbers of shares were generated, as shown in Fig. 8. Among those generated 4 shares, two of the shares share1 and share2 are sent to the patient through the patient's e-mail ID and other pairs of shares share3 and share4 are kept with the HCI administrator. When the patient visits the hospital the secondtime, the HCI administrator will uniquely validate the right person by his/her biometric

template, and it will be matched with the ID already sent to the patient via e-mail. Once the patient's ID is validated, then HCI administrator collects the patient's shares toperform RGVSS decryption simply by the superimposition of all the four shares 1, 2, 3 and 4 as shown in Fig. 9 without any key. The simple bitwise OR operation on four shares gives the Secret (S) = share1 || share 2 || share 3 || share 4.

The flowchart of RGVSSQRC (4, 4) decryption process with the HCI hospital administrator's public key 'K' is shown in Fig. 10, to get decrypted secret called 'S', which is equal to original secret S, as it is shown in Fig. 11 (a). Now it can be seen that the two QR Code images obtained in Fig. 4 (b) and Fig. 11(a) as a result of the proposed system are the same, which is shown in Fig. 11 (b), which reveals the validation of the right patient with fast information accessing in HCI applications. In the below shown Fig. 11 (a), to protect

it from intruders administrator will lock the results folder and unlock them whenever needed in program execution. When the program completes its execution, we will lock the folders. We will create a Graphical User Interface (GUI) to lock/unlock the results folder if needed by the admin. The result of the proposed system RGVSSQRC is attractive in terms of contrast, storage requirements and aspect ratio when compared with existing methods with the novelty of transmitting QR Code image securely, which is shown in Table 2.

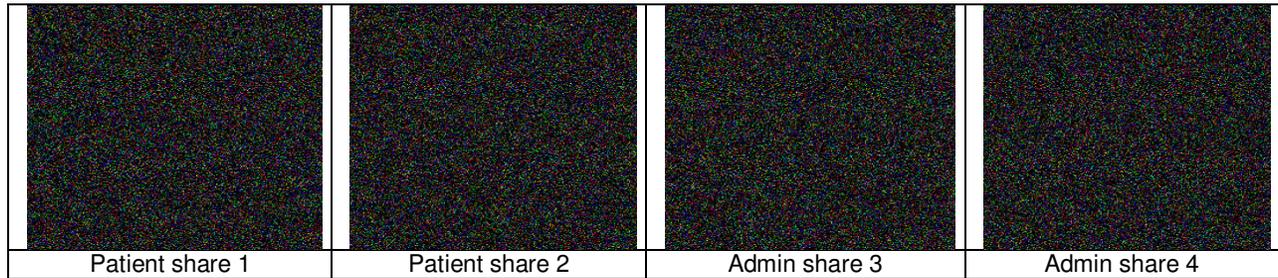


Fig. 8. RGVSSQRC (4, 4) shares generated.

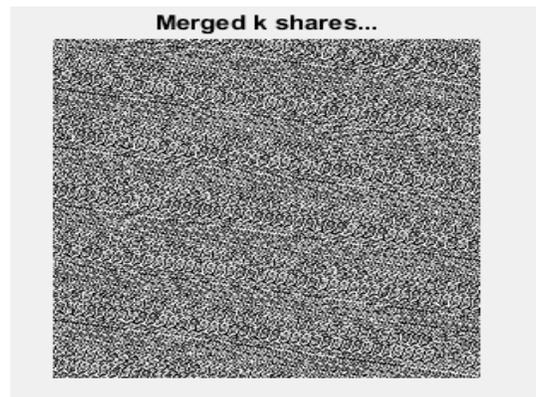


Fig. 9. Secret (S') = Share 1 || share 2 || share 3 || share 4.

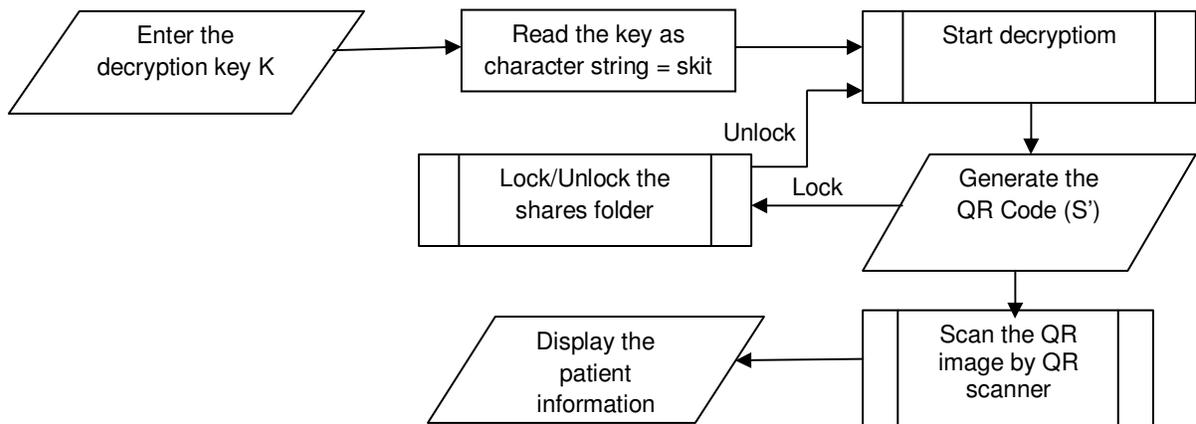
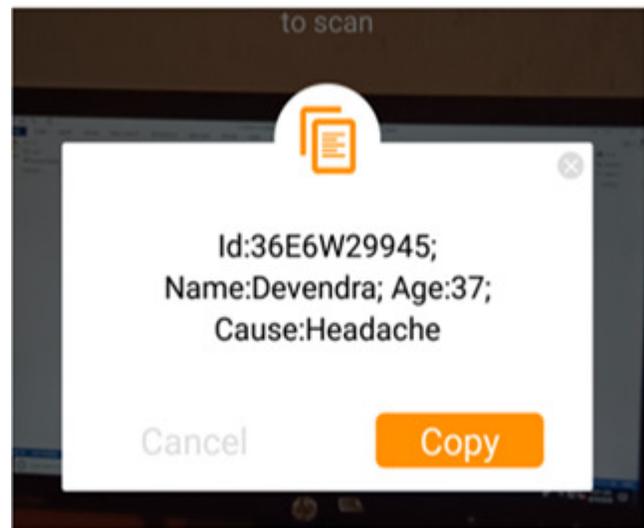


Fig. 10. RGVSSQRC decryption flowchart.



(a) RGVSSQRC decrypted output.



(b) The scanned output of patientdetails.

Fig. 11.

Table 2: Comparative analysis with existing RGVSS (n, n) techniques with this work.

Schemes	Pixel expansion	Ciphering	Contrast	Aspect ratio	Storage
Liu, <i>et al.</i> , [35]	No	No key	0.124	1:1	Unchanged
Hodeish, Mahmoud E[29]	Yes	No Key	0	1:1	Increases
Yan, Xuehu, <i>et al.</i> , [36]	No	No key	0.12451	1:1	Unchanged
Priya. S., and B. Santhi [3]	Yes	Key	0.00023	1:1	Increases
Proposed work	No	No key	0.125	1:1	Unchanged

VI. CONCLUSION

In this paper, the novelty of the proposed system RGVSSQRC has demonstrated the feasibility of protecting the multi-biometric template in HCI application by using the QR Code. The experimental results showed that aspect ratio and contrast are good for better vision of QR encrypted cipher image without any use of a key for ciphering. The main contribution of the proposed method is analyzed to demonstrate the possibility of protecting the fused biometric template by RGVSS through QR Code in digital image transmission.

VII. FUTURE SCOPE

This work can be extended to avoid noise to be generated during random grids distribution by post-processing methods.

Conflict of Interest. No.

REFERENCES

[1]. Xin, Y., Kong, L., Liu, Z., Wang, C., Zhu, H., Gao, M., ... & Xu, X. (2018). Multimodal feature-level fusion for biometrics identification System on IoT platform. *IEEE Access*, 6, 21418-21426.
 [2]. Rathgeb, C., & Uhl, A. (2011). A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security*, 2011(1), 3.

[3]. Priya, S., & Santhi, B. (2019). A Novel Visual Medical Image Encryption for Secure Transmission of Authenticated Watermarked Medical Images. *Mobile Networks and Applications*, 1-8.
 [4]. Kim, S. Y. (2018). A Study on the Factors Affecting the Intention to Payment Service Using Biometrics. *International Journal of Advanced Science and Technology*, 114(1), 69-80.
 [5]. Purnomo, A. T., Kim, C. S., Gondokaryono, Y. S., & Ra, I. (2017). The Combining Method of Fingerprint and QR Code as Mutual Authentication for Mobile Payment. *International Journal of Control and Automation*, 10(3), 345-356.
 [6]. Lei, S., & Qi, M. (2016). Multimodal recognition method based on ear and profile face feature fusion. *International Journal of Signal Processing, Image Processing and Pattern Recognition*, 9(1), 33-42.
 [7]. Xiao-xue, X., CAO, F. C., & SHANG, W. W. (2015). Multi-modal medical image fusion based on non-subsam-pied shearlet transform. *International Journal of Signal Processing, Image Processing and Pattern Recognition*, 8(2), 41-48.
 [8]. Geng, P., Su, X., Xu, T., & Liu, J. (2015). Multi-modal Medical Image Fusion Based on the Multiwavelet and Nonsubsampled Direction Filter Bank. *International Journal of Signal Processing, Image Processing and Pattern Recognition*, 8(11), 75-84.

- [9]. Bagri, N., & Johari, P. K. (2015). A comparative study on feature extraction using texture and shape for content based image retrieval. *International Journal of Advanced Science and Technology*, 80(4), 41-52.
- [10]. Yu, K., & Wei, J. (2015). The Key Extraction from Iris Features based on Wavelet Packet. *International Journal of Signal Processing, Image Processing and Pattern Recognition*, 8(7), 309-316.
- [11]. Wave, D. (2015). Information technology automatic identification and data capture techniques QR code bar code symbology specification. *International Organization for Standardization, ISO/IEC, 18004*.
- [12]. www.qrcode.com
- [13]. Chow, Y. W., Susilo, W., Yang, G., Phillips, J. G., Pranata, I., & Barmawi, A. M. (2016). Exploiting the error correction mechanism in QR codes for secret sharing. In *Australasian Conference on Information Security and Privacy* (pp. 409-425). Springer, Cham.
- [14]. Ranjan, K. H., Fathimath, S. S., Aithal, G., & Shetty, S. (2017). A survey on key (s) and keyless image encryption techniques. *Cybernetics and Information Technologies*, 17(4), 134-164.
- [15]. Dahat, A. V., & Chavan, P. V. (2016). Secret sharing based visual cryptography scheme using CMY color space. *Procedia Computer Science*, 78, 563-570.
- [16]. Mrunali, T. Gedam, Vinay, S. Kapse. (2012). Various Visual Secret Sharing Schemes- A Review. *International Journal of Engineering Research & Technology*, 1.10(2012): 1-6.
- [17]. Elavarasi, G. & Vanitha, M. (2017). A Novel Method for Securing Medical Image Using Visual Secret Sharing Scheme. *International Journal of Engineering and Technology*, 9.5: 3579-3585.
- [18]. Chao, H. C., & Fan, T. Y. (2017). XOR-based progressive visual secret sharing using generalized random grids. *Displays*, 49, 6-15.
- [19]. Bansal, R., Hediayti, A., Aggrawal, J., Sorlan, B., & Gupta, S. (2016). Comparison of Hybrid Security Schemes: A Survey. *International Journal of Signal Processing, Image Processing and Pattern Recognition*, 9(8), 169-180.
- [20]. Manikandan, G., Bala Krishnan, R., Preethivi, E., Sekar, K. R., Manikandan, R., & Prassann, J. (2019). An Approach with Steganography and Scrambling Mechanism for Hiding Image over Images. *International Journal on Emerging Technologies*, 10(1): 64-67.
- [21]. Liu, S., Yue, C., & Wang, H. (2016). An Improved Hybrid Encryption Algorithm for RGB Images. *International Journal of Advanced Science and Technology*, 95, 37-44.
- [22]. Sasaki, M., & Watanabe, Y. (2017). Visual secret sharing schemes encrypting multiple images. *IEEE Transactions on Information Forensics and Security*, 13(2), 356-365.
- [23]. Bakshi, A. (2018). Secure Authentication, Privacy and Integrity in Telemedicine using Visual Cryptography. *International Journal of Advanced Science and Technology*, 117(1), 11-28.
- [24]. Guang, Y., Yunbo, S., & Chang, C. (2015). A Kind of Encryption Method of QR Code based on ECA State Ring. *International Journal of Security and its Applications*, 9(9), 285-294.
- [25]. Xuehu Yan, & Yuliang Lu. (2018). Applying QR Code to Secure Medical Management. *9th International Conference on Information Technology in Medicine and Education* : 53-56.
- [26]. Dinca, L. M., & Hancke, G. P. (2017). The fall of one, the rise of many: a survey on multi-biometric fusion methods. *IEEE Access*, 5, 6247-6289.
- [27]. Tarek, M., Ouda, O., & Hamza, T. (2016). Robust cancellable biometrics scheme based on neural networks. *IET Biometrics*, 5(3), 220-228.
- [28]. Wan, S., Lu, Y., Yan, X., Wang, Y., & Chang, C. (2018). Visual secret sharing scheme for (k, n) threshold based on QR code with multiple decryptions. *Journal of Real-Time Image Processing*, 14(1), 25-40.
- [29]. Hodeish, M. E., Bukauskas, L., & Humbe, V. T. (2016). An Optimal (k, n) visual secret sharing scheme for information security. *Procedia computer science*, 93, 760-767.
- [30]. Chao, H. C., & Fan, T. Y. (2017). Random-grid based progressive visual secret sharing scheme with adaptive priority. *Digital Signal Processing*, 68, 69-80.
- [31]. Uludag, U., Pankanti, S., Prabhakar, S., & Jain, A. K. (2004). Biometric cryptosystems: issues and challenges. *Proceedings of the IEEE*, 92(6), 948-960.
- [32]. Rachapalli, D. R., & Kalluri, H. K. (2018). Texture Driven Hierarchical Fusion for Multi-Biometric System. *International Journal of Engineering & Technology*, 7(4.24), 33-37.
- [33]. Rachapalli, D. R. & Kalluri, H. K. (2019). Multimodal Biometric Template Protection Using Color QR Code. *International Journal of Recent Technology and Engineering*, Vol. 7(5) S4, (2019), pp. 7-11.
- [34]. Chen, T. H., & Tsao, K. H. (2009). Visual secret sharing by random grids revisited. *Pattern recognition*, 42(9), 2203-2217.
- [35]. Liu, X., Wang, S., Yan, X., & Zhang, W. (2018). Random grid-based threshold visual secret sharing with improved visual quality and lossless recovery ability. *Multimedia Tools and Applications*, 77(16), 20673-20696.
- [36]. Yan, X., Liu, X., & Yang, C. N. (2018). An enhanced threshold visual secret sharing based on random grids. *Journal of Real-Time Image Processing*, 14(1), 61-73.
- [37]. Satyam, P., & Amit, S. (2018). A Image Encryption Scheme is Based on Scan Pattern for Colour image. *International Journal of Electrical, Electronics and Computer Engineering*, 7(1): 01-05.

How to cite this article: Rachapalli, D.R. and Kalluri, H.K. (2019). Disseminating the Authentication Process Based on Secure RGVSS Multi-Biometric Template Encryption through QR Code in Health Care Informatics. *International Journal on Emerging Technologies*, 10(3): 370–378.