Biometric Security Through Visual Encryption for Fog Edge Computing

Wadood Abdul, *Member, IEEE,* Zulfi ar Ali, Sanaa Ghouzali, *Member, IEEE,*
Budour ALfawaz, Ghulam Muhammad and M. Shamim Hossain, *Senior Member, IEEE*
Wadood Abdul, Zulfi ar Ali, Ghulam Muhammad and Budour ALfawaz are with the Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia.
Sanaa Ghouzali is with the Information Technology Department, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia.
M. Shamim Hossain is with the Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia.
Corresponding author: M. Shamim Hossain (mshossain@ksu.edu.sa) and Ghulam Muhammad (ghulam@ksu.edu.sa)

***Abstract*—Fog and mobile edge computing have gained considerable attention from the research and development community. The problems related to security and privacy of biometric content are simpler to solve through edge computing resulting in improved security and privacy of biometric and other critically private information. Zero-watermarking has been proposed as a solution to help protect the ownership of multimedia content that is easy to copy and distribute. Visual cryptography is another approach to secure data that is to be shared through generating multiple shares. The presented work is concerned with developing a biometric security solution for face images, using visual cryptography and zero-watermarking, that does not adversely impact the visual quality of the image. The original face image is not modif ed through the zero-watermarking and visual encryption procedures and this in-turn does not adversely impact the recognition rate.**

***Index Terms*—edge, image, visual cryptography, zero-watermarking, security, cloud.**

I. Introduction

THE edge of the network requires certain level of computational capability and control due to the requirements of privacy and security for mobile devices. It is considered to be one of the most signif cant enablers towards $5G$ [1]. There are numerous cases of individual privacy breaches relating to personal information and multimedia content due to the limited protection provided by the cloud. An effective way to ensure edge privacy and security is to initiate the security and privacy of personal information and multimedia content at the edge.

The proposed work deals with the security of biometric content, specially face images that are produced on the edge and shared through the cloud. The protection mechanism should not degrade the visual quality of the image so that the difference of the recognition rate before and after the application of the mechanism should be minimum.

When it comes to personal or biometric data, such as face images of an individual which can be used for personal exchange or for applications such as face recognition for banking services [2] it becomes essential that the face images are protected to guarantee private sharing for personal use and secure for safe sharing for banking and other services.

The inherent characteristics of edge computing allow for the added advantages of computational capabilities that are necessary for privacy and security sensitive applications. This amongst other potential advantages of edge computing enable the operation of smart cities [3]. The computational capabilities of the edge allow for improved security and privacy by processing vital data at the edge and sharing the processed and secure or encrypted data through the cloud.

Figure 1 shows the basic concept of edge computing applied for the proposed work. The cloud is connected to the different edges, the edges are basically considered to be an extra layer between the cloud and the devices. Basic security functions are performed on the edge and sharing is achieved through the cloud. In the Internet of Things (IoT) [4] scenario, the advantages of edge computing allow for mobility, scalability and reliability [5], [6].

The security of biometric data on the cloud, specially images is of paramount importance in this digital age that allows copying and distribution of content at increasing ef f ciency. For data to be processed and shared on the cloud, a great deal of trust dependencies are raised because private information that was traditionally saved on personal computers becomes vulnerable as it is controlled by third parties [7], [8]. This raises additional privacy concerns [9]. Watermarking is considered as an effective solution, where the identity of the user is watermarked into the biometric image but this causes distortions in the image which can result in incorrect decision by the recognition system. Zero-watermarking on the other hand, allows for extracting pertinent information from the image without making any changes to the image.

Recently, visual cryptography was used with watermarking [10], to protect iris templates. This marriage between visual cryptography is achieved through a 2-share mechanism and watermarking by swapping Discrete Cosine Transform (DCT) coeff cients.

The proposed solution for the security of biometric images

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2017.2693438, IEEE Access

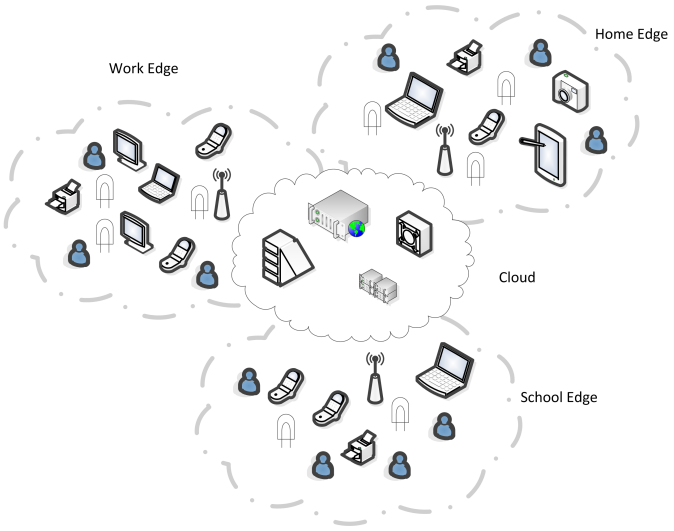

Fig. 1. Cloud and edge computing.

enabled through the Weber Local Descriptor (WLD) [11] based zero-watermarking allows for watermarking the unique user identity number into the image. On the other hand visual cryptography generates multiple (n) shares of the watermarked image. These shares individually reveal no information about the contents of the image and even if an eavesdropper or attacker gains access to all the shares, he is not able to collect meaningful information regarding the user or his identity without the correct secret key.

Watermarking is the process of inserting some information [12] into multimedia content to allow for security applications such as authentication [27], [28] and copyright protection. Watermarking of sensitive data [13], [14] has been extensively used to provide security to biometric content and medical images [15], [16]. Zero-watermarking allows for the watermarking of multimedia content but without making any changes to it. For the case of biometric data represented as an image, an operation between the image data and a random matrix is applied to generate the secret that is required to insert and extract the watermark. The random matrix is generated through a chaotic process. The watermarked image along with the parameters of the chaotic matrix are required for the extraction process. The added advantage of using zero-watermarking is that the recognition rate before and after the watermarking processes is the same as zero-watermarking does not change the image.

Figure 2 shows the block diagram of the proposed approach where we use face image to show the effectiveness of the proposed solution. The proposed zero-watermarking and visual cryptography algorithms are not only robust to common signal distortions, such as compression, but also ensure that the face images are not changed after watermarking and the shares after visual cryptography reveal no information about the original or watermarked images.

The remaining paper is organized as follows, section II gives the details of the proposed zero-watermarking approach for sharing biometrics, section III details the visual encryption and decryption procedures along with the results of the procedures. Section IV illustrates the face recognition process and that is followed by the conclusion in section V.

II. Zero-Watermarking for Sharing Biometrics

The captured image is f rst converted to gray scale followed by face detection through the Viola Jones algorithm [17]. The detected face is then watermarked through the zero-watermarking algorithm using the unique user identity. The zero-watermarked image is then subjected to visual cryptography, which generates the shares or visually encrypts the image based on the secret key. All this processing takes place at the edge. After the shares are generated they are shared on the cloud where further processing for different applications (e.g. face authentication, based on the same secret key used in the encryption process) takes place. The entities that have legal access to the face images can process and generate results accordingly.

As mentioned earlier, the face is detected through the captured user image using the Viola Jones face detection algorithm [17]. The detected face, or the original image is then decomposed using the Discrete Wavelet Transform up to level 2. THE WLD operator is then applied to the low-pass sub-band at level 2, L_2 using Equation 1 to f nd the coeff cients suitable for zero-watermarking. The differential excitation of the WLD is used to f nd the suitable coeff cients of the wavelet decomposition for each wavelet coeff cient C_w.

$$DE_w = arctan\left(\sum_{i=0}^{N-1}\frac{C_i - C_w}{C_w}\right) \tag{1}$$

where N is the window size of the WLD operator.

The suitable features, C_f, are binarized (C_{fb}) and XORed with the binarized (X_b) chaotic sequence using the Tent map of Equation 2. For parameter $\mu = 2$, the Tent map is given by a discrete-time dynamical system as

$$x_{t+1} = \begin{cases} \mu x_t, & \text{when } x_t < \frac{1}{2} \\ \mu(1 - x_t), & \text{when } \frac{1}{2} < x_t \end{cases} \tag{2}$$

and the binary zero-watermark is generated through Equation 3.

$$ZW_b = C_{fb} \oplus X_b \tag{3}$$

The receiver, receives the visually encrypted images that are shared through the cloud along with the initial parameters of the Temp map used for the zero-watermarking and visual encryption procedures. The visual decryption procedure is then applied to generate the received zero-watermarked image. Watermark detection and face recognition are applied to the visually decrypted image to validate the authenticity of the image.

If the bit error rate between the original watermark and the extracted watermark are below a certain threshold t, then the extracted watermark is considered as valid and the user is authenticated. The bit error rate is ratio of the Hamming distance D_H (between the original and extracted watermark) and the length of the watermark W_l. It is calculated using Equation 4.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2017.2693438, IEEE Access

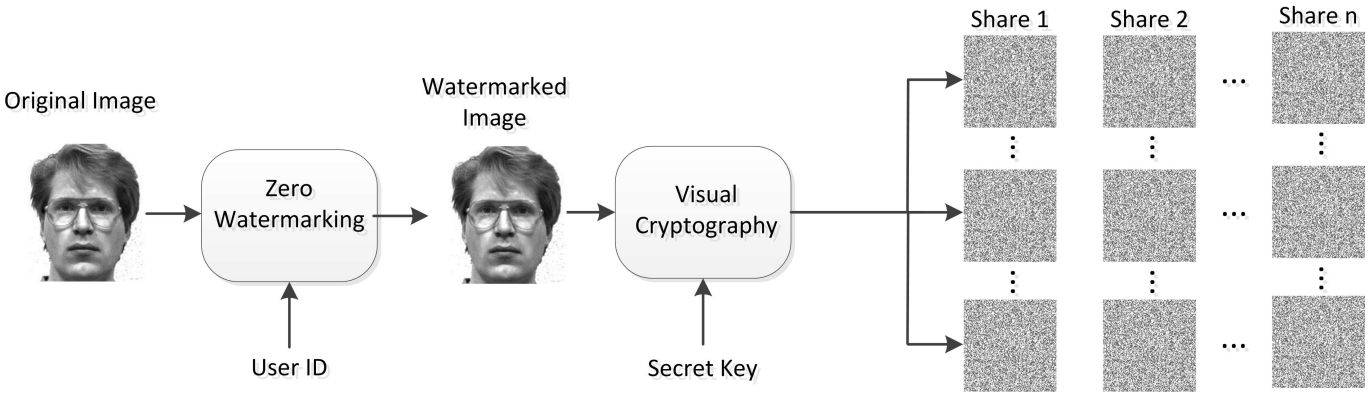

Fig. 2. The zero-watermarking and visual cryptography procedures at the edge.

$$BER = \frac{D_H}{W_l} \tag{4}$$

III. Visual Encryption for Biometric Security

Visual encryption [18] was designed to encode and decode secret images without using complex cryptographic computations. This has led to the development of visual cryptography for associated fields [19], [20], [21] such as secret sharing [22], biometrics [10] and watermarking [23]. For the proposed work, intended for the security of zero-watermarked biometric images, the encoding and decoding procedures using face images with 5 shares are illustrated in the following sections.

A. Visual Encryption Process

The proposed method encrypts a gray scale image of a person by generating n secret shares. The identity of a person will not be revealed unless all n secret shares are not available simultaneously. To generate secret shares, the method encrypts each pixel of every bit plane of an image. Pixels of an original gray scale image O of dimension $u \times v$ can be represented as

$$O_{(i,j)} = \sum_{k=0}^{p-1} 2^k \times o^k_{(i,j)} \tag{5}$$

where o^k denotes the k^{th} bit of a pixel, and p represents the number of bit planes in an image. Since every pixel in a gray scale image consists of 8 bits, therefore, $p = 8$. The number of rows of an image are denoted by i in Equation 5, and $i = 1, 2, 3, ..., u$. In addition, j stands for the number of columns and $j = 1, 2, 3, ..., v$. The first step for generation of secret shares is the retrieval of all bit planes. A p^{th} bit plane can be obtained by considering the corresponding p^{th} bits from all pixels of the image O, and a p^{th} bit plane B^p can be obtained by using Equation 6.

$$B^p_{(i,j)} = \begin{bmatrix} O^p_{(1,1)} & O^p_{(1,2)} & \cdots & O^p_{(1,v)} \\ O^p_{(2,1)} & O^p_{(2,2)} & \cdots & O^p_{(2,v)} \\ \vdots & \vdots & \ddots & \vdots \\ O^p_{(u-1,1)} & O^p_{(u-1,2)} & \cdots & O^p_{(u-1,v)} \\ O^p_{(u,1)} & O^p_{(u,2)} & \cdots & O^p_{(u,v)} \end{bmatrix} \tag{6}$$

The bit plane B^0 contains the least significant bits of all pixels, whereas, the bit plane B^7 comprises of the most significant bits. The dimensions of every bit plane, B^0, B^1, B^2, B^3, B^4, B^5, B^6, and B^7, are the same as that of the original image O which is $u \times v$. To generate the secret shares, we will create secret shares for each bit plane. In other words, for n secret share of the image O, we will have $8n$ shares in all (n shares for each bit plane). For n shares of a bit plane, every black pixel in a bit plane will be replaced by $n+(n-2)$ sub-pixels. The sub-pixels contain $n-1$ black sub-pixels and $n-1$ white sub-pixels, and $n-2$ of the black sub-pixels are common between the secret shares. To generate the sub-pixels having the mentioned criteria, first we will produce a matrix G of $n \times (n-2)$ black sub-pixels. In case of five secret shares ($n = 5$), the dimension of matrix G will be 5×3 and is given by Equations 7.

$$G = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \tag{7}$$

As mentioned earlier, $n-2$ black sub-pixels out of $n-1$ are common between shares, which means that shares have 1 individual black sub-pixel. The individual black sub-pixels are created by $n \times n$ identity matrix H. For five shares, the identity matrix H of dimensions 5×5 is given by Equation 8.

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{8}$$

The concatenation of the matrix G and H produces the required criteria of the sub-pixels. The concatenated matrix GH is presented in Equation 9.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2017.2693438, IEEE Access

$$GH = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad (9)$$

Each row of the matrix GH provides the sub-pixels for a share. The dimensions of the matrix GH are 5×8, i.e. $n \times (n + (n-2))$, for five secret shares, and it can be noticed that there are $n-2$ black sub-pixels common between secret shares and each share has one individual black sub-pixel. Similarly, every white pixel in a bit plane will also be replaced by $n + (n-2)$ sub-pixels. The sub-pixels for white pixels are obtained by taking the complement of each sub-pixel in the matrix GH. The matrix containing complement of each sub-pixel is denoted by $(GH)'$ and is given by Equation 10.

$$(GH)' = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} \quad (10)$$

All black and white pixels in the original image O can not be replaced by using the same set of sub-pixels provided in Equation 9 and 10. The secret shares should be random so that there should not be any clue of the original image. Therefore, various combinations of matrix GH and $(GH)'$ need to be produced by permuting their columns randomly. To permute the columns, we need a random sequence and it can be created through chaotic theory. The randomness through chaotic theory is deterministic and the same sequence can be regenerated by using exactly same initial conditions. The chaotic theory to generate random sequence X is implemented by applying the Tent map. For parameter $\mu = 2$, the Tent map is given by discrete-time dynamical system given by Equation 2.

For the image O of dimension $u \times v$, the length of X will be $u.v.p(n + (n-2))$, where, . represents multiplication. The values of X constitute our required random sequence but it lies in the interval $[0, 1]$. In our case, every sub-sequence of X containing $n+(n-2)$ values should provide 1 to $n+(n-2)$ random integers and it can be achieved by using Equation 11.

$$y = b + \left\lfloor (a-b) \times \frac{x^s - min(x^s)}{max(x^s) - min(x^s)} \right\rfloor \quad (11)$$

where x^s is a sub-sequence containing $n + (n-2)$ values, $a = 1$, $b = n + (n-2)$, y is the required sequence to permute the columns of GH and $(GH)'$, and $\lfloor . \rfloor$ represents the floor operator. For example, in case of five shares ($n = 5$), a and b will be 1 and 8, respectively, and the sub-sequence y will produce values like $[2, 6, 1, 3, 8, 4, 7, 5]$.

After creation of the encryption matrices, GH and $(GH)'$, and secret key y through chaotic theory, the next step is the replacement of black and white pixels with the sub-pixels in the bit planes to generate the secret shares. The secret key permutes the columns of GH if there is a black pixel in a bit plane, and secret key permutes the matrix $(GH)'$ in the case of white pixels. Each row of the permuted matrices GH and $(GH)'$ is used in one of the shares. The encryption process for 5 secret shares is depicted in Figure 3. It can be observed in Figure 3 that the columns of encryption matrix GH are permuted by using an 8-digit chunk $[2, 6, 1, 3, 8, 4, 7, 5]$ of the secret key for a black pixel in a bit plane.

Each row of the permuted matrix GH is used separately to produce a share. It can be seen that the generated 5 secret shares have one of the rows of the permuted matrix GH. Similarly all black and white pixels in B^0, B^1, B^2, B^3, B^4, B^5, B^6, and B^7 are replaced with the sub-pixels obtained through permutation of encryption matrices. The generated secret shares for each bit plane are presented in Figure 4.

The identity of a person will be disclosed only if all 40 secret shares are accessible at the same time. In Figure 4, the aspect ratio of secret shares is distorted. The reason is that a pixel is replaced by $n+(n-2)$ sub-pixels (eight sub-pixels in case of 5 shares), and the dimensions of the secret share will become $u \times 8v$. To avoid the distortion in aspect ratio, a black and white pixel can be replaced by $(n+(n-2)) \times (n+(n-2))$ sub-pixels.

For example, in Figure 3, for 5 shares, the circled black pixel is replaced by eight sub-pixels 10110100 in the secret share 1 (S^1). The aspect ratio will be disturbed, and to avoid it, a square matrix SP is shown in Equation 12 for the case of sub-pixels 10110100. In this way, the aspect ratio of each share will be $8u \times 8v$, which solves the problem but at the same time increases the dimensions by a factor of 8.

$$SP = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} \quad (12)$$

In this study, five secret shares ($n = 5$) for each bit plane of the gray scale image O are created to hide the identity of a person. The dimensions of the encryption matrices GH and $(GH)'$ are 8×14. The length of secret key is 8×14 times the dimension of the image O. The chunks of secret key are scaled to produce the integer from 1 to 14 by considering $a = 1$ and $b = 14$ in Equation 11. In addition, sub-pixels are used in form of square matrix to keep the same aspect ratio.

The visually encrypted shares are shared on the cloud and the recipient (having the correct secret key) can visually decrypt the encrypted shares to generate the watermarked, decrypted face image. The details of visual decryption process are given in the following section.

B. Visual Decryption Process

The given secret shares can be decrypted to obtain the original image O such that the image O and recovered image O' are exactly same, i.e., $\sum |O_{u,v} - O'_{u,v}| = 0$. The image O' is recovered from the secret shares by using the chaotic secret key with the same initial condition of the Tent map used in

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2017.2693438, IEEE Access

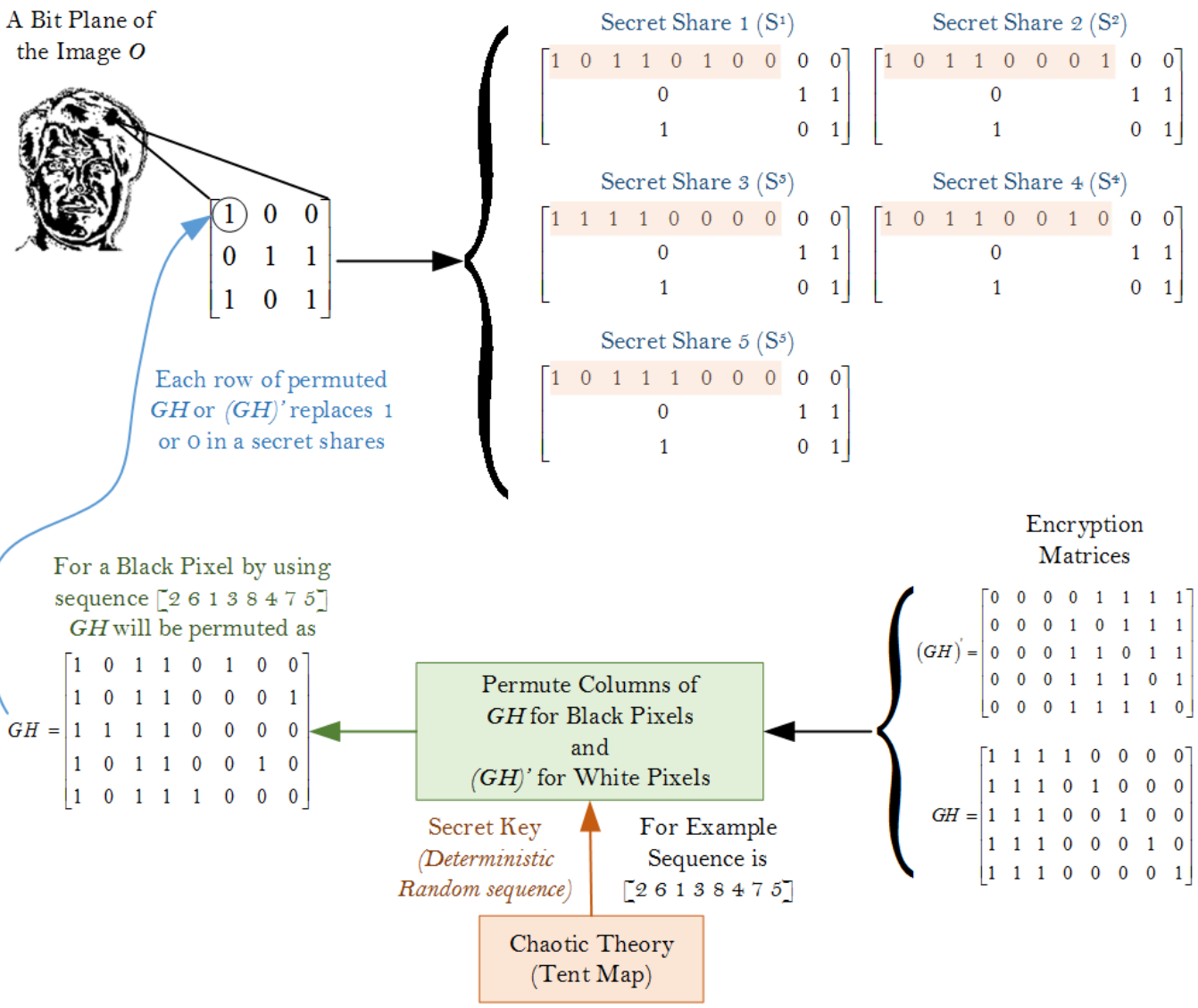

Fig. 3. The encryption process.

the encryption process. If secret shares are generated without maintaining aspect ratio then each secret share contains one row of the encryption matrices. In this scenario, to get a bit plane from its n shares, $n+(n-2)$ elements form each share are taken, and a matrix is formed. A chunk of $n+(n-2)$ elements from the secret key determine that how the columns of encryption matrices were permuted during the encryption process.

After arranging the columns of the obtained matrix, if it is equal to GH then the original pixel in the bit plane is black. However, if obtained matrix is equal to $(GH)'$ then the pixel is white. Similarly, original pixels are obtained for all bit planes. By taking the corresponding bits of the recovered bit planes, the original image is recovered. The decryption process for five shares is illustrated in Figure 5.

IV. Face Recognition

The Orthogonal Laplacianface (OLPP) [24], [25] is used to carry out face recognition on the cloud or another edge of the cloud, depending on the requirements of the application. The OLPP is an appearance based recognition approach for face images. It allows for the creation of orthogonal basis functions resulting in the advantage of proper reconstruction of data over the non-orthogonal Locality Preserving Projection (LPP) [26] method.

The Yale face database contains images of 15 users, with 11 images per user. There are 165 images in the database with different expressions and lighting conditions. The users have normal, sad, happy, sleepy, surprised and winking facial expressions. 5 images were used for training and 6 images were used for the testing process.

Figure 6 shows the Receiver Operating Curve (ROC) of the Yale database. The % error rate is plotted against the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2017.2693438, IEEE Access

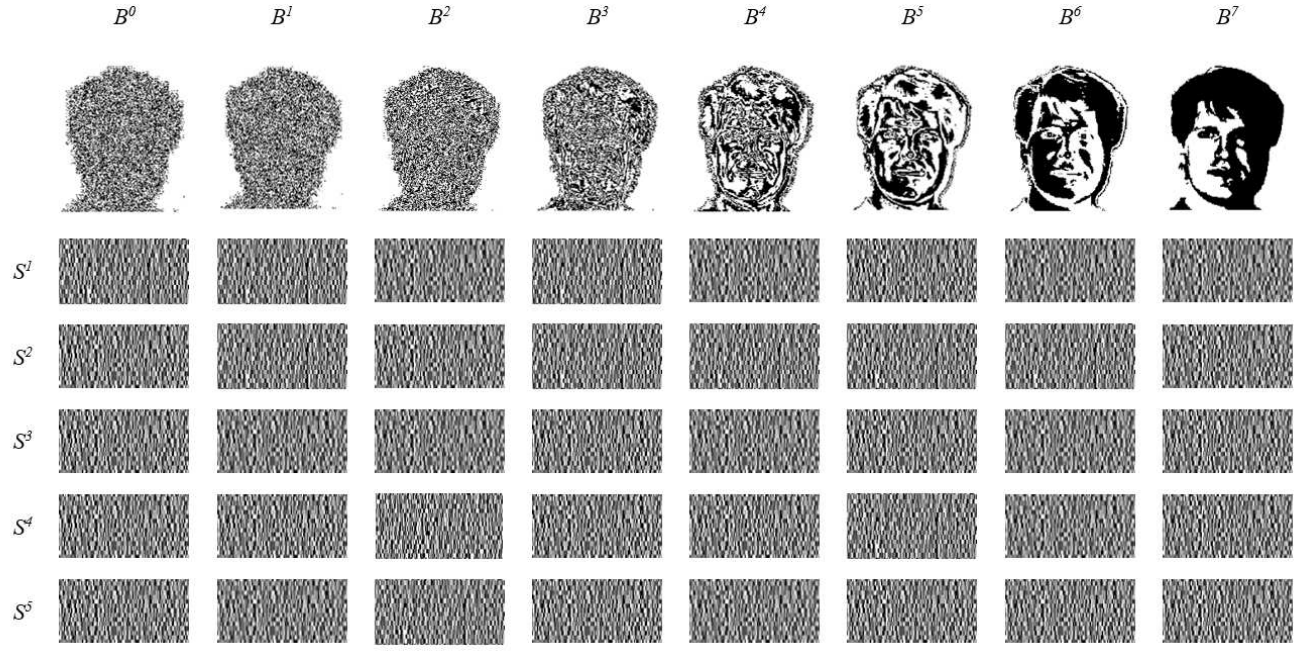

Fig. 4. Secret shares for all bit planes B^0, B^1, B^2, B^3, B^4, B^5, B^6, and B^7.

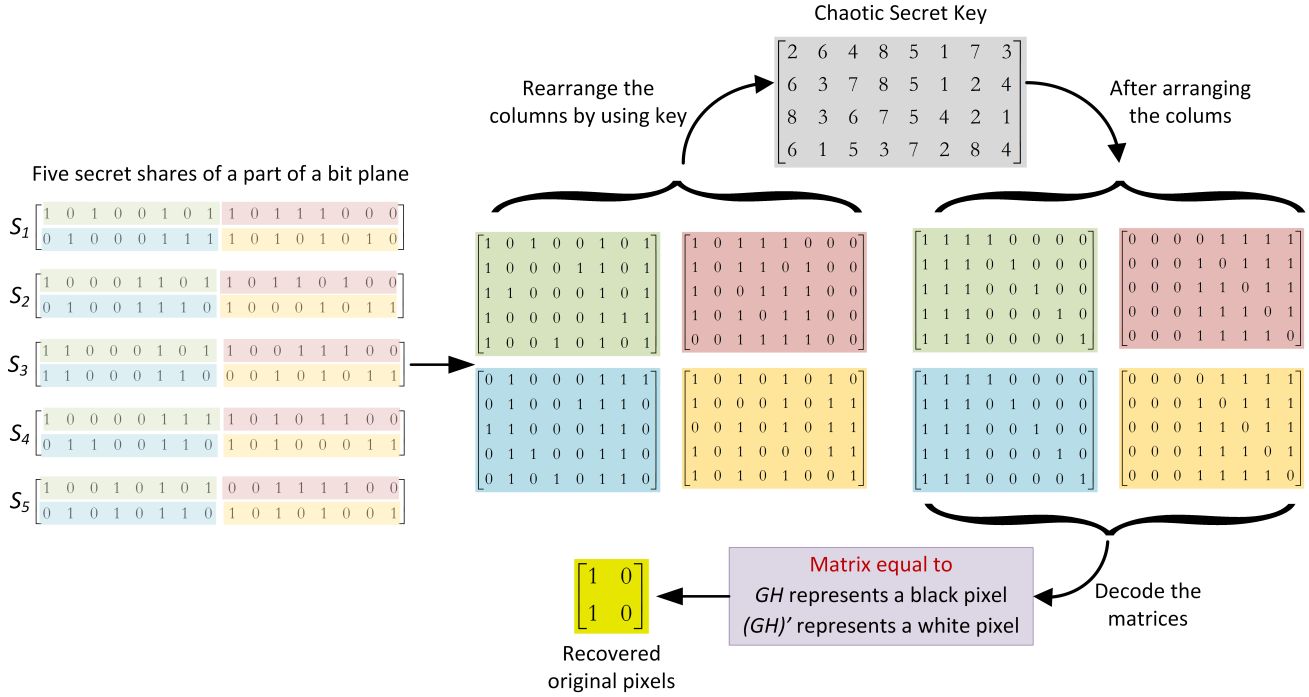

Fig. 5. The decryption process.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2017.2693438, IEEE Access

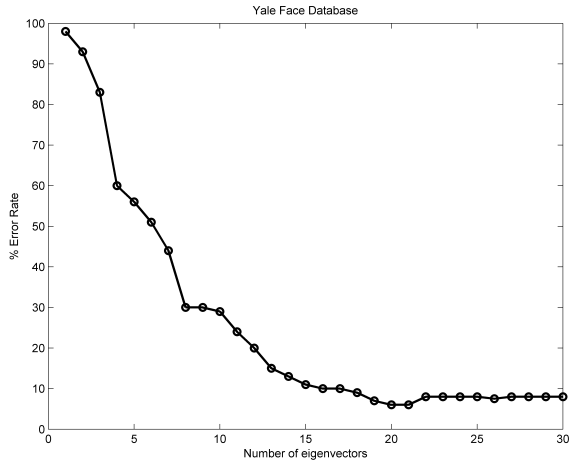

Fig. 6. Receiver Operating Curve of Yale database.

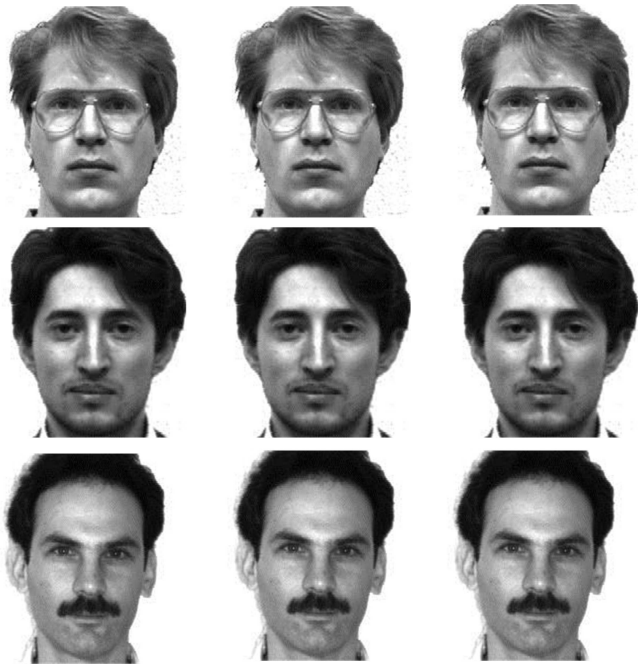

Fig. 7. Original, zero-watermarked and visually decrypted images of 3 users.

number of eigenvectors. As the images are not changed due to zero-watermarking and visual encryption and decryption procedures, the ROC for all 3 cases (original database, zero-watermarked database and visually decrypted) is the same.

Figure 7 shows 3 face images from the Yale database in the first column. The second column shows the zero-watermarked images and the third column shows the visually decrypted images. It can be noticed that the images are exactly the same, as the procedures of zero-watermarking, visual encryption and decryption do not make any changes to the image. Additionally, the Peak Signal to Noise Ratio (PSNR) is ∞ and Structural Similarity (SSIM) [29] is 1 for the entire Yale face image database.

V. Conclusion

Fog or edge computing allows for improved security where the original image or multimedia content is not shared over the network, rather a protected or watermarked image is shared. This allows for the security of the original image and also effective sharing. Visual cryptography and zero-watermarking are used for the security of biometric images. The processing at the edge is due to the requirements of a secure biometric solution where the original image is not shared on the cloud. The advantages of the proposed approach of edge computing range from copyright protection to authentication of multimedia content. In this work, we have shown that the shares generated through the visual encryption process can be perfectly decrypted only with the correct secret key. Through zero-watermarking of the face image, the authentication at the cloud, again with the only the correct key used for the watermarking process is possible. Additionally the watermarking and visual encryption procedures do not reduce the efficiency of the face recognition system in terms of recognition rate. Also, these procedures do not change the visual quality of the image.

Acknowledgment

The authors extend their appreciation to the Deanship of Scientific Research at King Saud University, Riyadh, Saudi Arabia for funding this work through the research group project no. RGP 228.

References

[1] Y. C. Hu, M. Patel, D. Sabella, N. Sprecher and V. Young. Mobile edge computingA key technology towards 5G. ETSI White Paper. 2015 Sep;11.
[2] Newsroom mastercard - self e payments, http://newsroom.mastercard.com/tag/self e-payments/, 28 03 2017.
[3] T. Taleb, S. Dutta, A. Ksentini, M Iqbal and H. Flinck. Mobile Edge Computing Potential in Making Cities Smarter. IEEE Communications Magazine. 2016 Jul.
[4] F. Bonomi, R. Milito, J. Zhu and S. Addepalli. Fog computing and its role in the internet of things. In Proceedings of the first edition of the MCC workshop on Mobile cloud computing 2012 Aug 17 (pp. 13-16). ACM.
[5] M. Yannuzzi, R. Milito, R. Serral-Graciá, D. Montero and M. Nemirovsky. Key ingredients in an IoT recipe: Fog Computing, Cloud computing, and more Fog Computing. InComputer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2014 IEEE 19th International Workshop on 2014 Dec 1 (pp. 325-329). IEEE.
[6] H. Chang, A. Hari, S. Mukherjee and T. V. Lakshman. Bringing the cloud to the edge. In Computer Communications Workshops (INFOCOM WKSHPS), 2014 IEEE Conference on 2014 Apr 27 (pp. 346-351). IEEE.
[7] A. Weiss. Computing in the clouds. Computing. 2007 Dec; 16.
[8] S. Pearson and A. Benameur. Privacy, security and trust issues arising from cloud computing. InCloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on 2010 Nov 30 (pp. 693-702). IEEE.
[9] R. B. Wells. The fog of cloud computing: Fourth Amendment issues raised by the blurring of online and offline content. U. Pa. J. Const. L.. 2009;12:223.
[10] M. A. Abdullah, S. Dlay, W. Woo andJ. Chambers. A Framework for Iris Biometrics Protection: A Marriage between Watermarking and Visual Cryptography. IEEE Access. 2016 Nov 14.
[11] J. Chen, S. Shan, C. He, G. Zhao, M. Pietikainen, X. Chen and W. Gao. WLD: A robust local image descriptor. IEEE transactions on pattern analysis and machine intelligence. 2010 Sep;32(9):1705-20.
[12] W. Abdul, P. Carré and P. Gaborit. Error correcting codes for robust color wavelet watermarking. EURASIP Journal on Information Security. 2013 Dec 1;2013(1):1.

[13] O. Nafea, S. Ghouzali, W. Abdul and E. Qazi. Hybrid Multi-Biometric Template Protection Using Watermarking. The Computer Journal. 2016 Sep 1;59(9):1392-407.
[14] M. S. Hossain, G. Muhammad, Sk. M. M. Rahman, W. Abdul, A. Alelaiwi and A. Almari, "Towards End-to-End Biometrics-Based Security for IoT Infrastructure, IEEE Wireless Communication magazine, vol. 23. no. 5, pp. 45-51, October 2016
[15] G. Badshah, S.C. Liew, J.M. Zain and M. Ali, Watermark compression in medical image watermarking using Lempel-Ziv-Welch (LZW) lossless compression technique, Journal of digital imaging 29, 216-225 (2016).
[16] M. S. Hossain and G. Muhammad, Cloud-assisted Industrial Internet of Things (IIoT) - enabled framework for Health Monitoring, Elsevier Computer Networks, Vol. 101, No. (2016), pp.192-202, June 2016
[17] P. Viola, M. J. Jones. Robust real-time face detection. International journal of computer vision. 2004 May 1;57(2):137-54.
[18] M. Naor and A. Shamir. Visual cryptography. In Workshop on the Theory and Application of Cryptographic Techniques. 1-12 (1994).
[19] S. Sridhar, R. Sathishkumar and G. F. Sudha. Adaptive halftoned visual cryptography with improved quality and security. Multimedia Tools and Applications. 2017 Jan 1;76(1):815-34.
[20] J. Lu, Z. Yang, L. Li, W. Yuan, L. Li and C. C. Chang. Multiple Schemes for Mobile Payment Authentication Using QR Code and Visual Cryptography. Mobile Information Systems. 2017 Mar 23;2017.
[21] C. N. Yang, J. K. Liao and D. S. Wang. New privilege-based visual cryptography with arbitrary privilege levels. Journal of Visual Communication and Image Representation. 2017 Jan 31;42:121-31.
[22] Y. W. Chow, W. Susilo, G. Yang, J. G. Phillips, I. Pranata and A. M. Barmawi. Exploiting the error correction mechanism in QR codes for secret sharing. In Australasian Conference on Information Security and Privacy. 409-425 (2016).
[23] A. Rani and B. Raman. An image copyright protection scheme by encrypting secret data with the host image. Multimedia Tools and Applications, 75, 1027-1042 (2016).
[24] D. Cai, X. He, J. Han and H.J. Zhang. Orthogonal laplacianfaces for face recognition. IEEE transactions on image processing. 2006 Nov;15(11):3608-14.
[25] S. Ghouzali, Watermarking based multi-biometric fusion approach. In International Conference on Codes, Cryptology, and Information Security 2015 May 26 (pp. 342-351). Springer International Publishing.
[26] X. He and P. Niyogi. Locality preserving projections. InNIPS 2003 Dec 8 (Vol. 16, No. 2003).
[27] A. Tewari, B. B. Gupta:A lightweight mutual authentication protocol based on elliptic curve cryptography for IoT devices. IJAIP vol. 9, no.2, 111-121 (2017)
[28] A. Tewari, B. B. Gupta: Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags. The Journal of Supercomputing 73(3): 1085-1102 (2017)
[29] Z. Wang, A.C. Bovik, H.R. Sheikh and E. P. Simoncelli. Image quality assessment: from error visibility to structural similarity. IEEE transactions on image processing. 2004 Apr;13(4):600-12.

Wadood Abdul (M'12) received his Ph.D. in signal and image processing from the University of Poitiers, France, in 2011. Currently he is working as an assistant professor in the Department of Computer Engineering, CCIS, King Saud University. His research interests are focused on color image watermarking, multimedia security, steganography, f ngerprinting, and biometric template protection.

Zulf qar Ali obtained his Master degrees in Computational Mathematics from the university of the Punjab, Lahore, and Computer Science from the University of Engineering and Technology (UET), Lahore, with the specialization in system engineering. Since 2010, he is working as a full-time researcher in the Digital Speech Processing Group in the Department of Computer Engineering, King Saud University, Saudi Arabia. He is also a member of Center for Intelligent Signal and Imaging Research (CISIR), Universiti Teknologi PETRONAS (UTP), Malaysia. His research interests include Speech and Language Processing, Medical Signal Processing, Privacy and Security in Healthcare, Multimedia Forensics, and Computer-aided Pronunciation Training Systems.

Sanaa Ghouzali (M'09) received both the Master's and the Ph.D. degrees in computer science and telecommunications from University Mohamed V-Agdal, Rabat, Morocco, in 2004 and 2009, respectively. In 2005 she has received a Fulbright grant to undertake dissertation research on a joint-supervision program at the Visual and Communication Laboratory of Cornell university, Ithaca, NY, USA. Between 2009 and 2011, she was an Assistant Professor at ENSA (the National school of Applied Sciences) within Abdelmalek Essaadi University. Starting 2012, she joined King Saud University as an Assistant Professor in the College of Computer and Information Sciences. Her research interests include statistical pattern detection and recognition, Biometrics, Biometric Security and Protection.

Budour ALfawaz is a graduate student at the Department of Computer Engineering, College of Computer and Information Sciences, King Saud University. Her research interests are focused on image watermarking and multimedia security.

Ghulam Muhammad (M'12) is a full Professor at the department of Computer Engineering, CCIS, King Saud University, Riyadh, Saudi Arabia. Prof. Ghulam received his Ph.D. degree in Electrical and Computer Engineering from Toyohashi University and Technology, Japan in 2006, M.S. degree from the same university in 2003. He received his B.S. degree in Computer Science and Engineering from Bangladesh University of Engineering and Technology in 1997. He was a recipient of the Japan Society for Promotion and Science (JSPS) fellowship from the Ministry of Education, Culture, Sports, Science and Technology, Japan. His research interests include image and speech processing, cloud and multimedia for healthcare, serious games, resource provisioning for big data processing on media clouds and biologically inspired approach for multimedia and software system. Prof. Ghulam has authored and co-authored more than 120 publications including IEEE / ACM / Springer / Elsevier journals, and f agship conference papers. He has a U.S. patent on audio processing. He received the best faculty award of Computer Engineering department at KSU during 2014-2015. He supervised more than 10 Ph.D. and Master Theses. Prof. Ghulam is involved in many research projects as a principal investigator and a co-principal investigator.

M. Shamim Hossain (SM'09) is an Associate Professor at the King Saud University, Riyadh, KSA. Dr. Shamim Hossain received his Ph.D. in Electrical and Computer Engineering from the University of Ottawa, Canada. His research interests include serious games, social media, Internet of Things (IoT), cloud and multimedia for healthcare, smart health, and resource provisioning for big data processing on media clouds. He has authored and coauthored around 120 publications including refereed IEEE/ACM/Springer/Elsevier journals, conference papers, books, and book chapters. He has served as a member of the organizing and technical committees of several international conferences and workshops. He has served as co-chair, general chair, workshop chair, publication chair, and TPC for over 12 IEEE and ACM conferences and workshops. Currently, he serves as a co-chair of the 7th IEEE ICME workshop on Multimedia Services and Tools for E-health MUST-EH 2017. He is the recipient of a number of awards including, the Best Conference Paper Award, the 2016 ACM Transactions on Multimedia Computing, Communications and Applications (TOMM) Nicolas D. Georganas Best Paper Award, and the Research in Excellence Award from King Saud University. He is on the editorial board of IEEE Access, Computers and Electrical Engineering (Elsevier), and International Journal of Multimedia Tools and Applications (Springer). Previously, he served as a guest editor of IEEE Transactions on Information Technology in Biomedicine (currently JBHI), International Journal of Multimedia Tools and Applications (Springer), Cluster Computing (Springer), Future Generation Computer Systems (Elsevier), Computers & Electrical Engineering (Elsevier), and International Journal of Distributed Sensor Networks. Currently, he serves as a lead guest editor of IEEE Communication Magazine, IEEE Transactions on Cloud Computing, IEEE Access and Sensors (MDPI). Dr. Shamim is a Senior Member of IEEE, a member of ACM and ACM SIGMM.