Journal of Theoretical and Applied Information Technology
15th July 2017. Vol.95. No 13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

GENE BASED MULTIVARIATE BIOMETRIC USER ACCESS CONTROL AND AUTHENTICATION FOR SOCIAL NETWORKS COMMUNICATION

[1]JAYANTHI SIVASUBRAMANIAM, [2]Dr. C. CHANDRASEKAR

[1]Research Scholar, Bharathiar University, Coimbatore, Tamil Nadu, India,

2Professor, Department of Computer Science, Periyar University, Salem, Tamil Nadu, India

ABSTRACT

Using multimodal biometrics for effective management of user authentication in online social networks (OSNs) is currently of practical interest. Considerable efforts is said to have taken in this field. However, multi-modal biometrics user authentication provides additional information to enhance the secured and reliable user communication compared to that of traditional cryptographic key authentication in social network. In this work, biometric user authentication scheme with multi-modalities (i.e., types of biometric data) for secured and reliable social network communication, called Multivariate Biometric User Access Control and Authentication (MBUAC-A) scheme is presented. User biometric feature template is extracted from corresponding human individuals and stored in spatial vectors. Gene encoding is applied on user biometric feature template to form an access control strategy. User biometric keys are generated for corresponding gene encoded user biometric feature templates. Authentication of user access is done based on the user biometric keys. Finally, the authenticity of user access is checked and ensured by gene decoding of corresponding user biometric keys. The experimental evaluation of proposal work is conducted with parameters such capacity of biometric feature template, user access control time, number of users, gene encode/decode latency, and access control accuracy.

Keywords: *Multimodal Biometrics, Online Social Networks, Multivariate, Access Control, Authentication, Gene Encoding/Decoding*

1. INTRODUCTION

Recently, several access control schemes have been proposed to support fine-grained authorization specifications for Open Social Networks (OSNs). SybilGuard, limits the influences of the Sybil attacks in social network where identities are represented as nodes and edges were considered as human-established trust relations. Two common drawbacks observed using Sybil Guard were that it cannot be applied to real social network data and that it proceeds with the assumption that the nodes are honest. Few other recent works adopted biometric security for user authentication in the social networks (based on single modal face recognition).

Face Recognition (FR) framework algorithm [1] introduced was a Social context for effective selection of suitable FR engines. Conditional random field (CRF) model was incorporated in social network context for FR system, resulting in the improvement in the accuracy of face annotation. However FR engines were proved to be less reliable when different types of FR engines were in use. A multimodal biometric user authentication scheme, Biosecure DS2 score-and-quality database algorithm [2] was presented with cost-sensitive evaluation, used quality-based fusion algorithms, under changing conditions. However biometric system failed to match a user query sample with a template, compromising scores and quality measures for corresponding user unavailable. However, in general multimodal biometric user authentication should in social network causes various security threats, resulting in the requirement of an access control mechanism. As a new attempt for providing access control, this paper proposes a biometric user authentication with user access control scheme to address security.

Most existing biometric systems only supports data capturing under controlled environments that can highly susceptible to replay attacks. To eliminate the environmental factors during face recognition reflection

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

matches [3] was considered as the major factor with a high degree of confidence. Performance evaluation of multimodal multifeature system using kNN classification was investigated in [4]. As reported in [5], the authentication performance using face and gestures has improved considerably over the last decade. On the other hand, encryption mechanism using logistic map and Murillo-Escobar's algorithm [6] came as a mechanism on real secure access control systems.

Fingerprint and face features are considered as representative of physical biometric systems and therefore many studies have been conducted on designing and development of eradicating the local variation [7]. However, the performance of user biometric system is easily influenced by several internal and external threats. Despite a significant number of studies performed to overcome this limitation, storage space and matching time was found to be tedious. Optical encryption with multimodal biometric authentication [8] improved the rate of security and matching time was found to be reduced considerably. Another watermarking technique based on Compressive Sensing (CS) and Fast Discrete Curvelet Transform [9] was designed to improve the authentication performance of multimodal biometric system. Gabor Wigner Transform [10] used fusion of faces and palmprint images to reduce the error rate.

1.1 Research Hypotheses

With the growing internet population, increasing use of social network system becomes the arising demand. The presence of malicious user behavior in the social network causes various security threats. Certain users in the social network system behave in an honest manner and few others in a semi-honest way, this would lead the whole community of users get compromised easily and face various user authentication issues. In order to reduce the misbehavior of users in the social networks, various user authentication and cryptographic security models were used in most of the recent researches.

1.2 Motivation

Recently, several access control schemes have been proposed to support fine-grained authorization specifications for Open Social Networks (OSNs). Inspired by the previous studies, we propose to introduce Multivariate Biometric User Access Control and Authentication scheme for user communication in a social network scenario. The proposed scheme can be easily implemented in social media through biometric feature templates ensuring authenticity of the user being accessed.

One objective of the proposed scheme is to reduce the misbehaviour of users in the social networks for user authentication system. Another one is to ensure authentication in social network for cooperative data sharing between the valid users. Although the authentication and authenticity of the user access can be ensured, they have virtually independent distributional properties, which is desirable for multivariate combination. Therefore, we expect to improve the performance of authentication systems using the proposed scheme with an insignificant increase in access control time. In addition to the benefit of low access control time, we take advantage of the common properties of the two different biometric feature templates (i.e. face and fingerprint). Noting that both face and fingerprint are stored in spatial vectors, we can use common image processing techniques to extract efficient feature matrices from the two biometric feature templates. Furthermore, we apply an appropriate encoding and decoding measure using Gene model instead of typical heuristic and computational algorithms. A comprehensive description of the proposed scheme is addressed in the subsequent sections.

This paper is organized as follows. In Section 2 related works are reviewed. The novel contribution of our work is outlined as well. Section 3 presents an overview of the proposed Biometric User Authentication scheme. Section 4 subsequently discusses the experimental methodology used in this paper. In Section 5, experimental results that demonstrate the effectiveness and the efficiency of our Biometric User Authentication scheme are presented. Finally, conclusion is presented in Section 6.

2. RELATED WORKS

Several studies have recently been presented that discuss the use of biometric user authentication with social network context for improving the effectiveness of user communication. Independent Component Analysis was applied in [11] for protecting and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

providing authenticity for watermarked digital images. This made an improvement in the authentication accuracy and robustness of the scheme. In [12], a detailed investigation on the quality assessment of image based biometric modality using image quality and pattern based quality was presented resulting in the higher rate of authentication.

Several research efforts have demonstrated that face authentication with access control system can used for improving the accuracy of face authentication. In [13], a two factor face authentication scheme using matrix transformation and user password were designed ensuring, genuine acceptance ratio. Another two factor user authentication [14] via fingerprint and password were used and applied for user verification resulting in the improvement of accessibility and security. A dynamic authentication system with sensor information instead of using human templates were used in [15] with the aid of access control systems resulting in the improvement of authentication accuracy.

Few research efforts have thus far been dedicated to address the problem of dynamic score level in fingerprint images on OSNs. In [16], a static software approach combining Speeded Up Robust Features (SURF) and Pyramid extension of Histograms of Oriented Gradients (PHOG) were designed ensuring average Equal Error Rate (EER). User authentication systems based on fingerprint images using Distal Interphalangeal Crease was presented in [17] to improve the fingerprint recognition system. A Durable True Neighbor Template (DTNT) [18] with the aid of standard encryption mechanism was designed resulting in negligible loss in fingerprint distinguishability. In [19] max-of-scores fusion technique was applied based on the face and signature traits resulting in better authentication performance. A thorough study and comprehensive evaluation relating to time consumption for user authentication was presented in [20].

3. MULTIVARIATE BIOMETRIC USER ACCESS CONTROL AND AUTHENTICATION SCHEME

In this section we formalize a Multivariate Biometric User Access Control and Authentication (MBUAC-A) scheme for Online Social Network. The MBUAC-A scheme uses Gene Encoding-based Access Control Strategy (section 3.1), an Authentic Key Generation strategy (section 3.2) and Gene Decoding-based Access Control Strategy (section 3.3) for the specification and enforcement of MBUAC-A in OSN. Figure 1 shows the block diagram of Multivariate Biometric User Access Control and Authentication scheme.

As shown in the figure, the MBUAC-C scheme provides an effective and efficient means of control for user communication in a network environment using gene-based encoding and decoding. By consolidating information from multiple sources (multi-modal biometric-based system), better potentiality is said to be achieved compared to the individual single modality systems.

3.1 Gene Encoding-based Access Control Strategy

In this section a Gene Encoding-based Access Control Strategy is designed (as in figure 2). The user biometric feature (face and fingerprint) template is extracted from corresponding human individuals and stored in spatial vectors. The spatial vector representation of face 'G_f^t' and fingerprint 'G_{fp}^t' is expressed as given below.

$$G_f^t = \begin{bmatrix} g_{f1}^{t+1} \\ g_{f2}^{t+2} \\ \dots \\ g_{fq}^{t+1} \\ \dots \\ g_{fq}^{t+1} \end{bmatrix}; \quad G_{fp}^t = \begin{bmatrix} g_{fp1}^{t+1} \\ g_{fp2}^{t+2} \\ \dots \\ g_{fp2}^{t+2} \\ \dots \\ g_{fpn}^{t+1} \end{bmatrix} \quad (1)$$

With the resultant value stored in spatial vectors, gene encoding is applied on the user biometric feature template to form an access control strategy. The proposed scheme uses a Gene Encoding-based Access Control Strategy. The main aim of selecting Gene Encoding-based Access Control Strategy in the proposed scheme is to minimize the mean absolute error of user biometric feature template between implementation stage and demonstration stage. The objective function 'fun_i' of the 'ith'

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

chromosome (user biometric feature template) is as given below.

$$fun_i = \sum_{i=1}^{n} \frac{(uf_i + ufp_i)}{j} \quad (2)$$

From (2), 'uf_i' corresponds to the face feature template, 'ufp_i' corresponds to the fingerprint feature template of the user 'u' with population (user biometric feature template size) of 'j' respectively. Then, the fitness function 'fun_i' of the 'ith' chromosome is as given below.

$$fit_i = \frac{1}{fun_i} \quad (3)$$

Followed by the fitness function, a uniform crossover operation is carried out that allows the offspring chromosomes to search all face and fingerprint templates from the user biometric feature template. Let '$G_f^t = \{g_{f1}^t, g_{f2}^t, \dots, g_{fn}^t\}$' and '$G_{fp}^t = \{g_{fp1}^t, g_{fp2}^t, \dots, g_{fpn}^t\}$' represents two parents (feature templates) for crossover and 't' refers to the generation number. Then, the two offspring (face and fingerprint) used in the proposed scheme is represented as given below.

$$G_f^{t+1} = \{g_{f1}^{t+1}, g_{f2}^{t+2}, \dots, g_{fq}^{t+1}, \dots, g_{fn}^{t+1}\} \quad (4)$$

$$G_{fp}^{t+1} = \{g_{fp1}^{t+1}, g_{fp2}^{t+2}, \dots, g_{fpq}^{t+1}, \dots, g_{fpn}^{t+1}\} \quad (5)$$

Followed by the crossover function, an adaptive mutation operation is performed in the proposed scheme for the user biometric feature template. An adaptive mutation is performed for generating new chromosomes (new templates) that explore new regions of the search space. Let us consider two chromosomes 'G_f^t' and 'G_{fp}^t' with gene 'g_{fn}^t' and 'g_{fpn}^t' selected for mutation, then 'g_{fn}^{t+1}' and 'g_{fpn}^{t+1}' is evaluated as given below.

$$g_{fn}^{t+1} = \begin{cases} [g_{fn}^t + \Delta(t, g_{fn}^u - g_{fn}^t)], if\ c = 0 \\ [g_{fn}^t - \Delta(t, g_{fn}^t - g_{fn}^p)], if\ c = 1 \end{cases} \quad (6)$$

$$g_{fpn}^{t+1} = \begin{cases} [g_{fpn}^t + \Delta(t, g_{fpn}^u - g_{fpn}^t)], if\ c = 0 \\ [g_{fpn}^t - \Delta(t, g_{fpn}^t - g_{fpn}^p)], if\ c = 1 \end{cases} \quad (7)$$

Followed by Gene encoding, the user biometric keys are generated for the corresponding gene encoded user biometric feature templates which is discussed in detail in the coming sections.

3.2 Hash Spatial Vector-based Template Authentic Key Generation

The proposed scheme uses a Hash Spatial Vector-based Template transformation. The user biometric keys are generated for the corresponding gene encoded user biometric feature templates. The authentication of the user access is done based on the user biometric keys. The Hash Spatial vector-based Template transformation improves access control accuracy as the dissimilarity between two vectors is measured on the basis of the Euclidean distance. The Hash Spatial Vector-based Template transformation obtains a secret hash key randomly for each biometric template (face and fingerprint) that is different for different users and is expressed as given below,

$$SHK = \begin{bmatrix} h_{11} \\ h_{12} \\ \dots \\ h_{1n} \end{bmatrix} \quad (8)$$

By applying the secret hash key 'SHK' to the encoded face and fingerprint biometric template, a resultant set of pseudorandom vectors are generated and is as expressed below.

$$U_{BKey} = RS[f_i fp_i] = \begin{bmatrix} h_{11} \\ h_{12} \\ \dots \\ h_{1n} \end{bmatrix} \begin{bmatrix} g_{f1} \\ g_{f2} \\ \dots \\ g_{fn} \end{bmatrix} \begin{bmatrix} g_{fp1} \\ g_{fp2} \\ \dots \\ g_{fpn} \end{bmatrix} = \begin{bmatrix} h_{11} g_{f1} g_{fp1} \\ h_{12} g_{f2} g_{fp2} \\ \dots \dots \\ h_{1n} g_{fn} g_{fpn} \end{bmatrix} \quad (9)$$

Figure 3 shows the Hash Spatial Vector-based Template Authentic Key Generation algorithm. As shown in the figure for each user, the Hash Spatial Vector-based Template Authentic Key Generation initially obtains multimodal biometric templates (face and fingerprint) from same user. Followed by this, the spatial vector representation of the user biometric templates is constructed to which the gene encoding is performed. To the gene encoded data, user biometric keys are generated using Hash-based Template transformation. With the user biometric keys 'U_{BKey}' generated for the corresponding gene encoded user biometric

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

feature templates, the authenticity of user access is checked and ensured by gene decoding of corresponding user biometric keys in the coming sections.

3.3 Gene Decoding-based Access Control Strategy

To improve the possibilities of biometric user authentication, the proposed scheme uses uniform crossover with comparison as given below (with the following rules given below). The following rules are generated according to the comprising results of the alleles (user biometric feature templates) for two parents (users).

$$if\ \left(g_{fp}^{t} - g_{f}^{t}\right) < 2, then\ g_{fp}^{t+1} = g_{f}^{t};\ g_{f}^{t+1} = g_{fp}^{t} \quad (10)$$

$$if\ \left(g_{fp}^{t} - g_{f}^{t}\right) \geq 2, and\ c = 1, then\ g_{fp}^{t+1} = g_{f}^{t};\ g_{f}^{t+1} = g_{fp}^{t} \quad (11)$$

$$if\ \left(g_{fp}^{t} - g_{f}^{t}\right) \geq 2, and\ c = 0, then\ g_{fp}^{t+1} = g_{fp}^{t};\ g_{f}^{t+1} = g_{f}^{t} \quad (12)$$

With the rules generated, the authenticity of user access is checked and ensured by gene decoding of corresponding user biometric keys. The access control is governed through the biometric featured template gene encode / decode process. Figure 4 shows the authentication phase provided through Gene Decoding-based Access Control Strategy.

4. EXPERIMENTAL SETUP

In this paper, we aim to improve the user access control accuracy and reduce the gene encode/decode latency during biometric user authentication for Social Networks Communication. A dataset containing 100 face and fingerprint images extracted from the BioSecure datasets is used to evaluate the performance of our proposed scheme.

The facial and fingerprint images are selected from BioSecure Images dataset, which provide 100 images for each person capturing every combination of features. By using BioSecure Images dataset and the defined testing method results are compared with existing method. Multivariate Biometric User Access Control and Authentication (MBUAC-A) scheme is compared with the existing Collaborative Face Recognition (Collaborative FR) [1] using Bayesian Decision Rule and Multimodal Biometric test bed using Score-level Fusion Algorithms (MB-SFA) [2].

The proposal work plan to conduct experimental and analytical evaluation of multimodality biometric user authentication in social network scenario with data sets extracted from research repositories. The experimental evaluation of proposal work is conducted on various factors such as access control time, access control accuracy, gene encode/decode latency, number of users, capacity of feature template to different user biometric feature template. Access control time is the time taken to regulate who can perform user communication in a network environment. It is measured as given below.

$$ACT = \sum_{i=1}^{n} U_i * \left[Time\left(g_{fn}^{t+1}\right) + Time\left(g_{fpn}^{t+1}\right)\right] \quad (13)$$

From (13), the access control time 'ACT' for 'i' users is obtained by the summation of the time taken for encoding based on gene formulates. It considers the gene encoding for face template 'g_{fn}^{t+1}' and gene encoding for fingerprint templates 'g_{fpn}^{t+1}'. To measure the efficiency of the template extraction rate, access control accuracy is evaluated. Access control accuracy is measured in terms of percentage (%) and is expressed as given below.

$$A = \left(\frac{TE_{size}}{FT_{size}}\right) * 100 \quad (14)$$

From (14), the access control accuracy 'A' is the ratio of size of template extracted 'TE_{size}' to the size of the entire feature template 'FT_{size}'. Higher access control accuracy ensures the efficiency of the scheme. Gene Encode/Decode Latency refers to a short period of delay, usually measured in milliseconds (ms) between when a user biometric feature template enters and when it emerges from a system for the authenticity of user access.

$$L = GED_{st} - GED_{et} \quad (15)$$

From (15), the gene encode/decode latency is the difference between the gene encode/decode start time 'GED_{st}' and the gene

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

encode decode end time 'GED_{et}'. Lower the rate of latency, more efficient the scheme is said to be.

5. DISCUSSION

In this section, we introduce the performance evaluation based on the implementation by MATLAB simulator. The validation results are presented in three tables. Table 1 represents the access control time for biometric user authentication with different number of users using Matlab simulator and comparison is made with two other methods, namely Collaborative FR [1] and MB-SFA [2]. In order to conduct experimentation, a total of thirty five user templates (face and fingerprint) extracted from similar person was selected. With these images, the access control time is identified and tabulated in table 1.

Figure 5 illustrates the access control time comparisons for biometric user authentication averaged over thirty five random raining of the hundred images. It is observed from the figure that the proposed measurement outperforms the others, indicating that it best describes the statistical distortion. To better perceive the efficacy of the proposed MBUAC-A scheme, substantial experimental results are illustrated in Figure 5 and compared against the existing Collaborative FR [1] and MB-SFA [2] respectively. The results reported above confirm that with the increase in the number of users (i.e. user biometric feature template) provided as input, the access control time also increases and comparatively observed to be higher using MBUAC-A scheme. From the table 1, the access control time for one user using MBUAC-A scheme was observed to be 2.35ms, 3.14ms using Collaborative FR whereas 3.75ms using MB-SFA. Therefore the access control time using MBUAC-A scheme when 5 templates were considered as input was observed to be 11.75ms, 15.7ms when applied with Collaborative FR and 18.75ms when applied with MB-SFA. The access control time for biometric user authentication is reduced with the application of Gene Encoding-based Access Control strategy. The Gene Encoding-based Access Control strategy extracts the user biometric feature (face and fingerprint) template and stored in spatial vectors. With the stored templates in spatial vectors, an adaptive mutation is performed for generating new chromosomes (new templates) that explore new regions of the search space for the corresponding gene encoded data. As a result, the access control time for biometric user authentication is reduced by 14% compared to Collaborative FR and 22% compared to MB-SFA.

The results of seven simulation runs conducted to measure the access control accuracy during biometric user authentication are listed in table 2. In the experimental setup, the capacity of biometric feature template ranges from 350KB to 2100KB. As listed in table 2, the MBUAC-A scheme measures the access control accuracy during biometric user authentication in Online Social Networks which is measured in terms of milliseconds (ms). The access control accuracy obtained using our scheme MBUAC-A offer comparable values than the state-of-the-art methods. The access control accuracy for single user biometric template using MBUAC-A scheme was 2.35ms, 3.14ms using Collaborative FR and 3.75ms using MB-SFA. With these values the access control accuracy is tabulated in table 2.

The targeting results of access control accuracy using MBUAC-A scheme is compared with two state-of-the-art methods Collaborative FR and MB-SFA in figure 6 is presented for visual comparison based on the relevant information. As illustrated in figure 6, when the capacity of biometric feature was 350KB, the size of template extracted using MBUAC-A scheme was observed to be 285KB, 253KB when using Collaborative FR whereas 234KB using MB-SFA were used as input, the access control accuracy using MBUAC-A scheme was 81.42%, 72.28% using Collaborative FR and 67.14% using MB-SFA scheme respectively. Our MBUAC-A scheme differs from the Collaborative FR and MB-SFA in that we have incorporated Hash Spatial Vector-based Template Authentic Key Generation algorithm. The advantage of applying Hash Spatial Vector-based Template Authentic Key Generation algorithm in MBUAC-A scheme is that the corresponding user biometric keys are generated for the gene encoded user biometric feature templates. As a result, user biometric key is not generated for the non encoded data. This in turn improves the access control accuracy by 12% compared to Collaborative FR and 17% compared to MB-SFA.

In table 3 we further compare the rate of gene encode/decode latency obtained for

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

different number of users for robust biometric user authentication. The experiments were conducted using thirty five faces and fingerprint images of similar person and size and the gene encode/decode latency is measured in terms of milliseconds (ms).

Figure 7 given above shows the rate of gene encode/decode latency for MBUAC-A scheme, Collaborative FR and MB-SFA versus thirty five different users. The gene encode/decode latency returned over MBUAC-A scheme though increases gradually for different users but proved to be efficient when compared to the two other methods. From figure 7, it is illustrative that the gene encode/decode latency rate of throughput for biometric user authentication is improved using the proposed MBUAC-A scheme. This is because with the application of Gene Decoding-based Access Control Strategy, the accuracy rate is increased where gene encoding/decoding is done on the basis of uniform crossover with gene decoding of corresponding user biometric keys. This result's in the improvement of gene encode/decode latency using MBUAC-A scheme by 19% compared to Collaborative FR and 28% compared to MB-SFA.

6. CONCLUSION

In this paper, we studied an effective user biometric authentication scheme for effective and efficient control of user communication in a network environment. The goal of our user biometric authentication scheme is to improve the access control accuracy by applying Gene-based encoding/decoding which significantly contributes to the relevance. To do this, we first devised a Gene encoding model applied on the user biometric feature template stored in the form of spatial vectors to determine the access control time. Then, based on this measure, a biometric key using Hash Spatial vector-based Template transformation was applied which reflects the access control accuracy during user biometric authentication. Finally, to improve the gene encode/decode latency, a Gene-based decoding using uniform crossover was performed through Hash Spatial Vector-based Template Authentic Key Generation algorithm based on the multimodal biometric templates (face and fingerprint). Through the experiments, we observed that our user biometric authentication scheme provided improved access control accuracy rate compared to existing state-of-the-art works. In addition, our Hash Spatial Vector-based Template Authentic Key Generation algorithm effectively improved the access control accuracy compared to the state-of-the-art methods. In the future, we plan to investigate the current work by extending the functionalities of biometric user authentication along the direction of access control through relational coefficient measure. Also, one limitation of the current prototype is the lack of control of the accessibility. To avoid such information flow issues, we are investigating stronger techniques that could allow a more stringent access control mechanism over authentication social communication in a safer environment.

REFERENCES

[1] Jae Young Choi, Wesley De Neve, Konstantinos N. Plataniotis, and Yong Man Ro, "Collaborative Face Recognition for Improved Face Annotation in Personal Photo Collections Shared on Online Social Networks", IEEE Transactions on Multimedia, Volume 13, Issue 1, February 2011, Pages 14-28.

[2] Norman Poh, Thirimachos Bourlai and Josef Kittler, "A Multimodal Biometric Test Bed for Quality-dependent Cost-sensitive and Client-specific Score-level Fusion Algorithms", Pattern Recognition, Volume 43, Issue 3, March 2010, Pages 1094–1105.

[3] Daniel F. Smith, Arnold Wiliem and Brian C. Lovell, "Face Recognition on Consumer Devices: Reflections on Replay Attacks", IEEE Transactions on Information Forensics And Security, Volume 1, Issue 1, April 2015, Pages 736 – 745.

[4] Gayathri Rajagopal and Ramamoorthy Palaniswamy, "Performance Evaluation of Multimodal Multifeature Authentication System Using KNN Classification", Hindawi Publishing Corporation, The Scientific World Journal, Volume 2015, October 2015, Pages 1-10.

[5] Hyunsoek Choi and Hyeyoung Park, "A Multimodal User Authentication System Using Faces and Gestures", Hindawi Publishing Corporation, BioMed Research International, Volume 2015, November 2014, Pages 1-9.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[6] M.A. Murillo-Escobar C. Cruz-Hernández , F. Abundiz-Pérez , R.M. López-Gutiérrez, "A robust embedded biometric authentication system based on fingerprint and chaotic encryption", Elsevier, Expert Systems with Applications, Volume 42, Issue 21, 30 November 2015, Pages 8198–8211.

[7] Tran Binh Long, Le Hoang Thai, and Tran Hanh, "Multimodal Biometric Person Authentication Using Fingerprint, Face Features", Springer, PRICAI 2012: Trends in Artificial Intelligence, Volume 7458 of the series Lecture Notes in Computer Science , Pages 613-624.

[8] Sheng Yuan, TongZhang , XinZhou , XuemeiLiu , MingtangLiu, "An optical authentication system based on encryption technique and multimodal biometrics", Elsevier, Optics &LaserTechnology54(2013), Pages 120–127.

[9] Rohit Thanki and Komal Borisagar, "Biometric Watermarking Technique Based on CS Theory and Fast Discrete Curvelet Transform for Face and Fingerprint Protection", Springer, Advances in Signal Processing and Intelligent Recognition Systems, Volume 425, October 2015, Pages 133-144.

[10] Nirmala Saini and Aloka Sinha, "Face and palmprint multimodal biometric systems using Gabor–Wigner transform as feature extraction", Springer, Pattern Analysis and Applications November 2015, Volume 18, Issue 4, Pages 921-932.

[11] Wioletta W ojtowicza, Marek R. Ogielaa, "Digital images authentication scheme based on bimodal biometric watermarking in an independent domain", Elsevier, Journal of Visual Communication and Image Representation, Volume 38, July 2016, Pages 1–10.

[12] Mohamad El-Abed, Christophe Charrier and Christophe Rosenberger,"Quality assessment of image-based biometric information", Springer, EURASIP Journal on Image and Video Processing (2015) 2015:3, Pages 1-15.

[13] Jeonil Kang DaeHun Nyang , KyungHee Lee, "Two-factor face authentication using matrix permutation transformation and a user password", Information Sciences, Volume 269, 10 June 2014, Pages 1–20.

[14] Woong Go, Kwangwoo Lee and Jin Kwak, "Construction of a secure two-factor user authentication system using fingerprint information and password", Springer, Journal of Intelligent Manufacturing, April 2014, Volume 25, Issue 2, Pages 217-230.

[15] Yuanchao Shu, Yu (Jason) Gu, and Jiming Chen, "Dynamic Authentication with Sensory Information for the Access Control Systems", IEEE Transactions on Parallel and Distributed Systems, Volume 25, Issue 2, February 2014, Pages 427-436.

[16] Rohit Kumar Dubey, Jonathan Goh, and Vrizlynn L. L. Thing, "Fingerprint Liveness Detection From Single Image Using Low Level Features and Shape Analysis", IEEE Transactions on Information Forensics and Security, Volume 11, Issue 7, July 2016, Pages 1461-1475.

[17] Feng Liu, David Zhang, and Zhenhua Guo, "Distal-Interphalangeal-Crease-Based User Authentication System", IEEE Transactions on Information Forensics and Security, Volume 8, Issue 9, September 2013, Pages 1446-1455.

[18] Fawaz E. Alsaadi and Terrance E. Boult, "Perpetuating Biometrics for Authentication Introducing the Durable True-Neighbor Template", Springer, Information Technology: New Generations, Volume 448 of the series Advances in Intelligent Systems and Computing, May 2016, Pages 161-176.

[19] Youssef Elmir, Somaya Al-Maadeed, Abbes Amira, and Abdelăali Hassaïne, "A Multi-modal Face and Signature Biometric Authentication System Using a Max-of-Scores Based Fusion", Springer, Neural Information Processing, Volume 7667 of the series Lecture Notes in Computer Science, June 2012, Pages 576-583.

[20] Naser Zaeri, "Discriminant Phase Component for Face Recognition", Hindawi Publishing Corporation Journal of Electrical and Computer Engineering, Volume 2012, Dec 2011, Pages 1-13.

[21] Mark Abernethy and Shri M. Rai, "An Innovative Fingerprint Feature Representation Method to Facilitate Authentication Using Neural Networks", Springer, Neural Information Processing, Volume 8227, May 2013, Pages 689-696.

[22] Tiago de Freitas Pereira, Jukka Komulainen, André Anjos, José Mario De Martino, Abdenour Hadid, Matti Pietikäinen and Sébastien Marcel, "Face liveness detection

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

using dynamic texture", EURASIP Journal on Image and Video Processing 2014, Feb 2014, Pages 1-15.

[23] Wen-Hui Lin , Ping Wanga, Chen-Fang Tsai, "Face recognition using support vector model classifier for user authentication", Elsevier, Electronic Commerce Research and Applications, Available online 9 February 2016, Pages 1-12.

Journal of Theoretical and Applied Information Technology
15th July 2017. Vol.95. No 13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

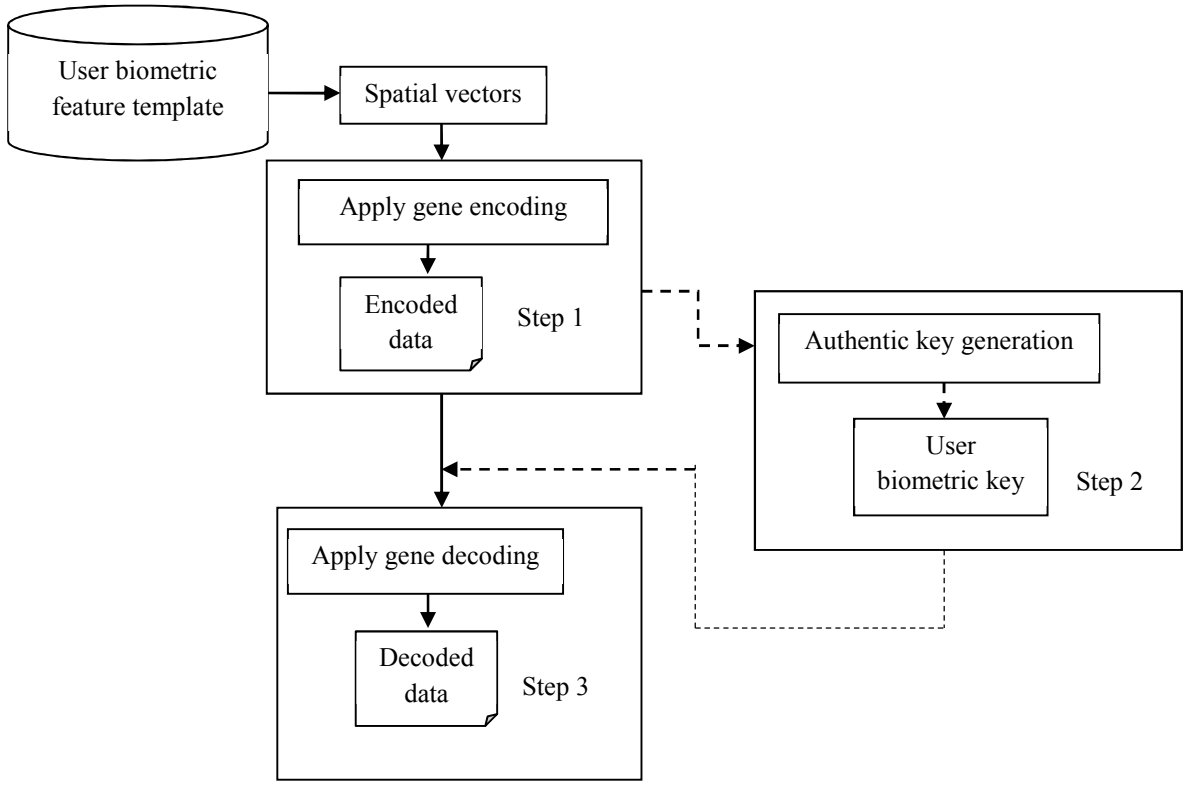
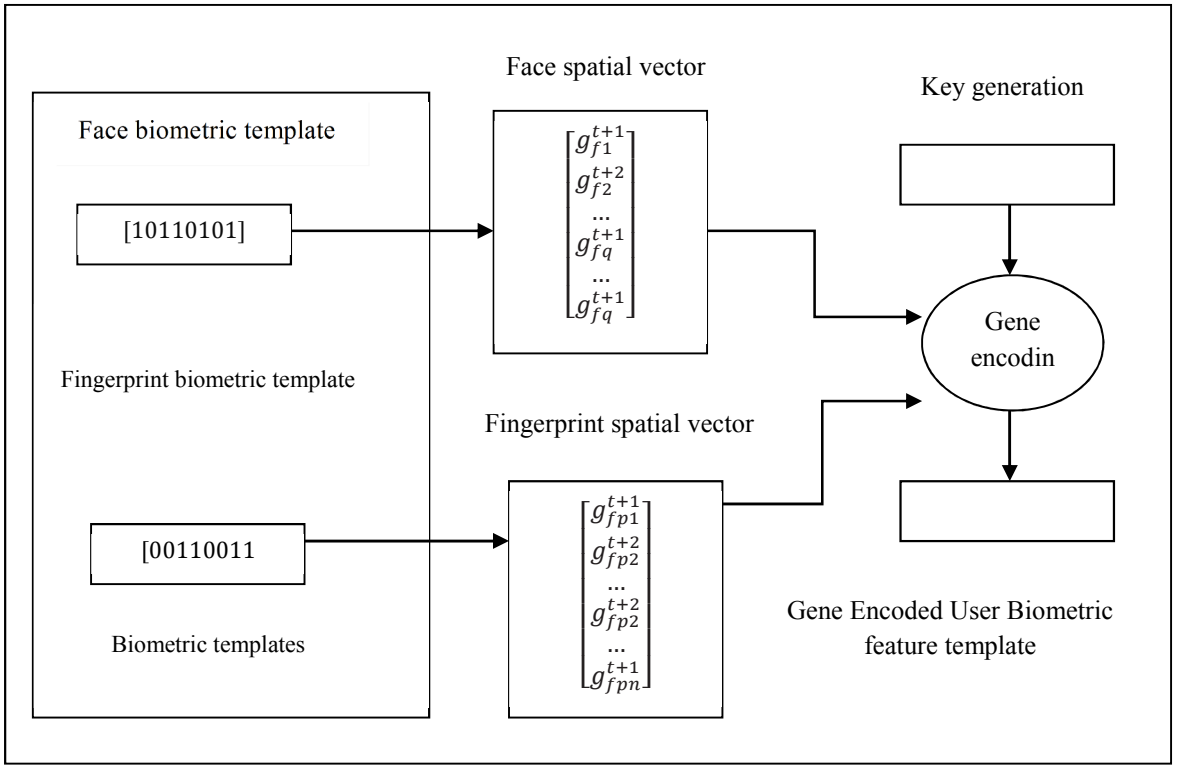


Figure 1 Block diagram of Multivariate Biometric User Access Control and Authentication scheme



ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Input: User 'u', Face Template '$f_i = f_1, f_2, .., f_n$', Fingerprint Template '$fp_i = fp_1, fp_2, \dots, fp_n$',
Output: Improved access control accuracy

1: Begin
2: For each User 'u'
3: Obtain multiple face templates 'f_i'
4: Obtain multiple fingerprint impressions 'fp_i'
5: Obtain spatial vector representation of face and fingerprint templates using (1)
6: Measure fitness function using (3)
7: Generate offspring for face and fingerprint using (4) and (5) //crossover
8: Generate adaptive mutation for face and fingerprint using (6) and (7)
9: Generate random hash key using (8)
10: Generate user biometric keys for gene encoded user biometric feature templates using (9)
11: End for
12: End

Figure 3 Hash Spatial Vector-based Template Authentic Key Generation

Input: User 'u', Face Template '$f_i = f_1, f_2, .., f_n$', Fingerprint Template '$fp_i = fp_1, fp_2, \dots, fp_n$'
Output: Reduced latency rate

1: Begin
2: For each User 'u'
3: Obtain multiple face templates 'f_i'
4: Obtain multiple fingerprint impressions 'fp_i'

Perform gene encoding

→

5: Perform gene encoding for face template 'g_{fn}^{t+1}'
6: Perform gene encoding for fingerprint template 'g_{fpn}^{t+1}'

No – Perform operation with other user

←

Yes – Proceed with generation of authentic key

→

7: Obtain biometric key 'SHK'
8: Append hash key to gene encoded face and fingerprint template 'U_{BKey}'

Perform gene decoding

→

9: Obtain user biometric key 'SHK_i''
10: If (SHK_i'') == (SHK)
11: Compare rules using (10), (11) and (12)
12: If verification OK
13: Authentication succeeded
14: End if
15: If verification not OK
16: Authentication failed
17: End if
18: End if
19: End for
20: End

Figure 4 Gene Decoding-based Authentication

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

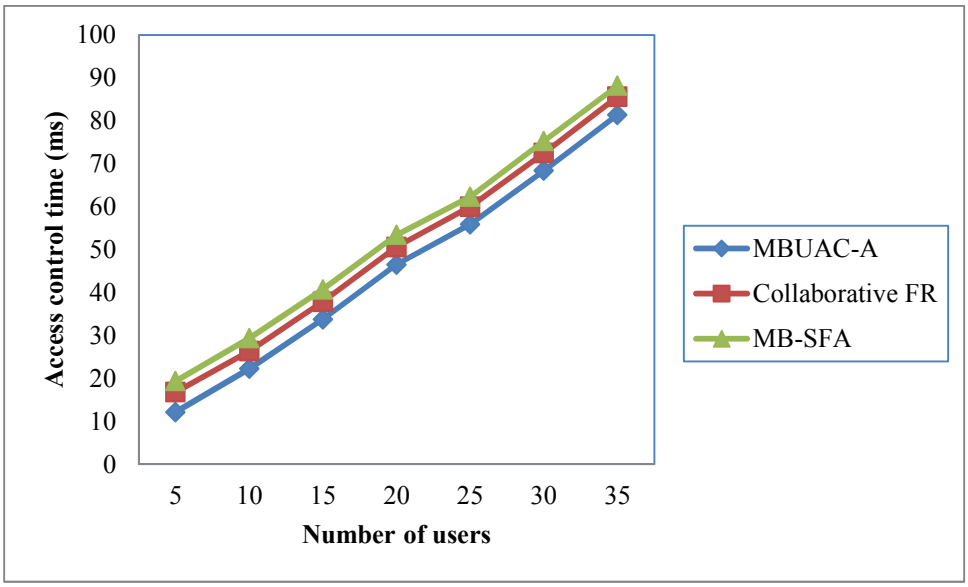


Figure 5 Measure of Access Control Time

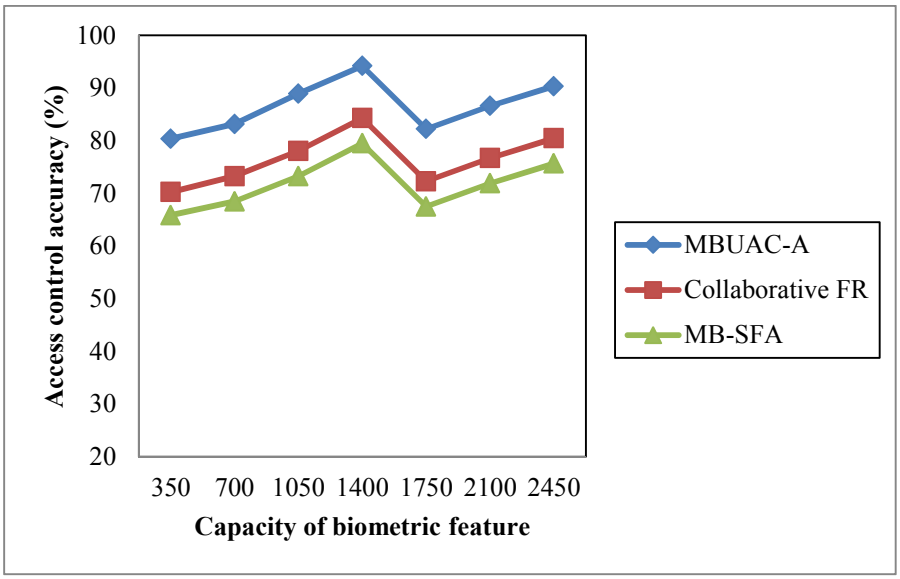


Figure 6 Measure of Access Control Accuracy

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

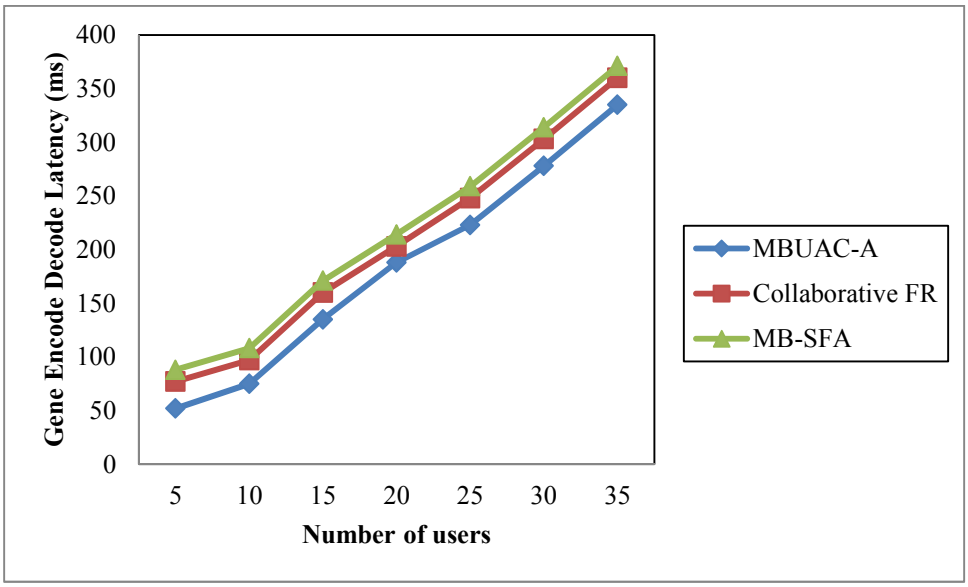


Figure 7 Measure of Gene Encode/Decode Latency

Table 1 Access Control Time Using MBUAC-A, Collaborative FR, MB-SFA

Number of users	Access control time (ms)		
	MBUAC-A	Collaborative FR	MB-SFA
5	12.14	16.82	19.35
10	22.23	26.33	29.34
15	33.78	37.88	40.69
20	46.51	50.61	53.42
25	55.89	59.99	62.33
30	68.37	72.47	75.28
35	81.39	85.59	88.14

Table 2 Access Control Accuracy Using MBUAC-A, Collaborative FR, MB-SFA

Capacity of biometric feature template (KB)	Access control accuracy (%)		
	MBUAC-A	Collaborative FR	MB-SFA
350	80.35	70.24	65.83
700	83.14	73.25	68.45
1050	88.92	78.03	73.23
1400	94.16	84.27	79.47
1750	82.19	72.28	67.48
2100	86.57	76.68	71.88
2450	90.32	80.43	75.63

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 3 Gene Encode/Decode Latency Using Mbuac-A, Collaborative Fr, Mb-Sfa

Number of users	Gene Encode Decode Latency (ms)		
	MBUAC-A	Collaborative FR	MB-SFA
5	52	77	88
10	75	97	108
15	135	160	171
20	188	203	214
25	223	248	259
30	278	303	314
35	335	360	371