Stegnography through Spatial Fusion for Security using M-Health Care in Teleradiology of Multimodal Biometric Data

PA.Vivitha[1] A.Vidhya[2] T. Lakshmana Kumar[3]
[1,3]P.G. Scholar [2]Assistant Professor
[1,2,3]Department of Computer Science and Engineering
[1,2,3]Valliammai Engineering College, Chennai, Tamilnadu, India

Abstract— In medical images of clinical data interpretation are used to provide the M-health services is to present a security and privacy protection in Teleradiology. The transmission of medical images has been critical issues for licensing and credential, contracts for radiology information system, and picture archiving the communication system. A joint dual steganography system means a joint fingerprint/ encryption/dual steganography system. Emerging trends represents the evolution of e-health system for "Teleradiology" platform to wireless and mobile configuration. In the system combines the substitution dual steganography algorithm, spatial fusion algorithm, stream cipher algorithm and fingerprint verification algorithm. This paper aims to give access the outcomes of medical images in mobile computing are confidential and its origin. We present a multiple document maintenance for multiple patients such as computed tomography (CT), MRI, positron emission tomography (PET), X-rays, ultrasound, and mammography are maintained its processes. The dual steganography system, introduce two different schemas, one for patient data & other for fingerprint and face recognition features; it will reduced the difficulties of multiple documents. While using algebraic invariants to improves the robustness of the medical information is the encryption of patient data with face recognition system. One of the most critical sources of variations in face recognition is facial expression, especially in the frequent case only a single sample person is available for enrollment. The experiment result of proposed system scheme evaluated for priori protection is used to verify the confidentiality and reliability for Teleradiology in terms of inaudibility.

Key words: Mobile technologies, Wireless technologies, Embed, encryption, decryption, fusion, fingerprint verification, protection, face recognition, 3D facial animation, expression, verification

I. INTRODUCTION

M-Health service in Teleradiology is to maintain and transmit medical Transcriptions in mobile online for patients to provide efficient clinical data interpretation. In this Purpose, Patients without carrying the documents for diagnosis purpose [1]. But at present, security and privacy protection has been a critical issue for the patients such as image retention and fraud, privacy, malpractice liability, licensing and credentialing and contracts for radiology information system, and picture archiving and communication system [2]. In mobile, multiple document maintenance for single patient diagnosis results are maintained and transmitted online separately which needs more time to access. Teleradiology needs confidentiality, Availability, and reliability [3] which means only an authorized user can access patient data, guarantee access to medical information in normal scheduled conditions, proves that information has not been altered by unauthorized persons, and information origins of its attachment relate to one patient. Using Steganography can be avoided by merging the multiple document of a single person to a single document. All these aspects, Steganography requires efficient maintenance and transmission of medical data remotely.

In personal authentication for biometric system is widely used for face recognition and usually achieved by fingerprint recognition system. Face recognition stands with its favorable reconcilement between accessibility and reliability. It allows identification at relatively long distance for unaware subjects by matching the extracted patterns from 3D still image or a video with the templates previously stored in a database. Steganography helps strengthen data security by masking truly sensitive information within other data that is irrelevant to the task at hand. Today with mobile technology, patient records could be accessed by health-care professionals from any given location by connection to the institution's information system. Physicians' access to patient history, laboratory results, diagnosis data, insurance information, and medical resources would be enhanced by mobile technology, thereby improving the quality of patient care. In mobile technology, a patient increases the mobility of patients and medical personnel but also improve the quality of health care [4]. However, it is hoped that the current deployment of universal mobile telecommunications system (UMTS) networks globally will alleviate some of these issues and will provide a better and more effective platform for M- health care services.

Technically, steganography and encryption are merged in two ways; one is that steganography embedding is conducted during decryption processes. [5] - [6] [7]. And the other is after decryption process or in the encrypted domain. Many approaches and techniques have been proposed to benefit the priori and posterior protection mechanisms. The system approaches invariant fingerprint and face authentication with less error rate with the four step stream cipher and dual steganography using spatial fusion of medical images for Teleradiology without any distortion.

The contributions of the proposed approach are:

1) Dual steganography scheme;
2) Region based embedding scheme based on spatial fusion;
3) Maintains the medical image with good quality index;
4) Face and fingerprint verification system using Zφ invariant moments;
5) Solve all the verification and validation issues for Teleradiology system;
6) No loss of entering data;
7) Impact on mobile networks on m-health;

The rest of the paper is organized as follows. In Section II, describes related work in the field while Section III. We then detail the implementation in Section IV. The experimental results and the analysis of security issue are presented in Section V and finally, the conclusion is derived in Section VI.

II. IDENTITY RESOLUTION, AND DUAL SETGANOGRAPHY PRIMITIVES

An individual identity management system is to evaluate the critical challenge in authentication system, compare and correlate all the accessible and distributed attributes of the user. It uses a deterministic technique based on experts in combination with a probabilistic component to determine generic values for identifiers. In this work, an amplitude modulation scheme is used to encode the stenographic images. Amplitude modulation which embeds information multiple times into the spatial domain of an image is widely used in the field of communication and signal processing. This technique based on the work done in [7].

A. Fingerprint Primitives:

A key to access the information to prove the fingerprint acts as a individuality of the person which provides the medical information. *Zφ* moments are proposed for fingerprint authentication system is based on image based approach. The Fingerprint image is enhanced the invariants extracted the property of invariant to rotation, scaling, and translation [10] and are evaluated for authentication

B. 3D Face Primitives:

The facial surface together with the registered texture is preprocessed, firstly to extract the face region obtained by 3D shape. While the extracted facial surface, scanner-induced holes and spikes are cleaned and a bilateral smoothing filter is to remove preserving the edges.

After the hole and noise free face model is obtained, 21 feature points are automatically detected using either shape, texture or both, according to the regional properties of the face [8]. To simulate facial actions and expressions via an animation engine that is in accordance with MPEG-4 Face and body animation (FBA) specifications.

1) Data Preprocessing: 3D Scanner Outputs are mostly noise. The Purpose of the preprocessing step can be listed as:
   - To extract the face region (same in 3D images);
   - To eliminate spikes/holes introduced by the sensor;
   - To smooth the 3D surface;
   - Once the complete surface is obtained, a bilateral smoothing filter [9] is employed to remove white noise while preserving the edges. This way, the facial surface is smoothed but the details hidden in high frequency components are maintained.
2) Automatic Landmarking: The analysis of the 5 fiducial points on the midline are detected. Based on that information; face is spilt into sub-regions for the coarse localization of eyes, nose and lips. For those regions with non- informative texture 3d data is analyzed. As a result, 21 facial interest points are detected in total, consisting of 4 points for the lips. The steps are detailed in the following:
   - Vertical profile analysis: The landmarks are known, the face can be broken into more meaningful sub-images for locating or refining the locations of points of interest.
   - Eye Regions: The image is rotated one last time in the 2d image plane, if necessary, to horizontally align the two iris centers.
   - Nose region: The minimum curvature detection is applied on the minimum curvature map, those edges of the points on both sides of the nose tip.
   - Lip Region: A close mouth is always yields to a darker line between the two lips, based on this knowledge the contact point of the lip is applying vertical analysis
3) Animatable face model Construction: In order to construct an animatable face model for each enrolled subject, a mesh warping algorithm based on the findings in [10] is proposed. A generic face model, with holes for the eyes and an open mouth is strongly deformed to fit the facial models in the database, using the TPS method. 17 points to be automatically detected together with the rest of the FDP points for MPEG-4 compliant animations are annotated for the generic face (Fig. 9). MPEG-4 specifications and the mathematical background of the TPS method will be briefly explained before going into details about the proposed animatable face construction method

C. Spatial Fusion:

The spatial fusion, is according to the splitting the components of medical image according to the range of intensity [11] to embed for medical images. Each region count is defined to predict the maximum counted region to embed a finite set of possible medical text information or ROI. For that initially the medical image M is represented by 1-D row vector sorted in ascending order defined by denoted by MR ∈ M. The levels of image Li ∈ MR is determined by thresholding the intensity level of the image vector (1)

$$3\forall \quad i=1\ Li = MIR\ (l \times i) \text{ where } l = N/4 - 1. \qquad (1)$$

By comparing the limit Li, the image is decomposed into different level of images Dd with labeling depend upon the condition, if i = 1, then d = S; i = 2, then d = R; i = 3, then d = Q else d = P by using (2)

$$N \quad N \quad Dd\ (x, y) = \sum \sum MI(x, y) < Licounti\ ++. \qquad (2)$$
$$x=0\ y=0$$

The decomposed regions are composed into single image by using (3)

$$N \quad M \quad F(x,y) = \sum x=0\ \sum y=0 Dd\ (x, y) > 1 \qquad (3)$$

The algorithm is very simple, resulted less computation for efficient composition and decomposition of the medical image. It is used in the watermarking system for efficient selection for region of embedding. The knowledge of the size of region to which M_w belongs is sufficient to identify the *Ie* to ensure the availability of information

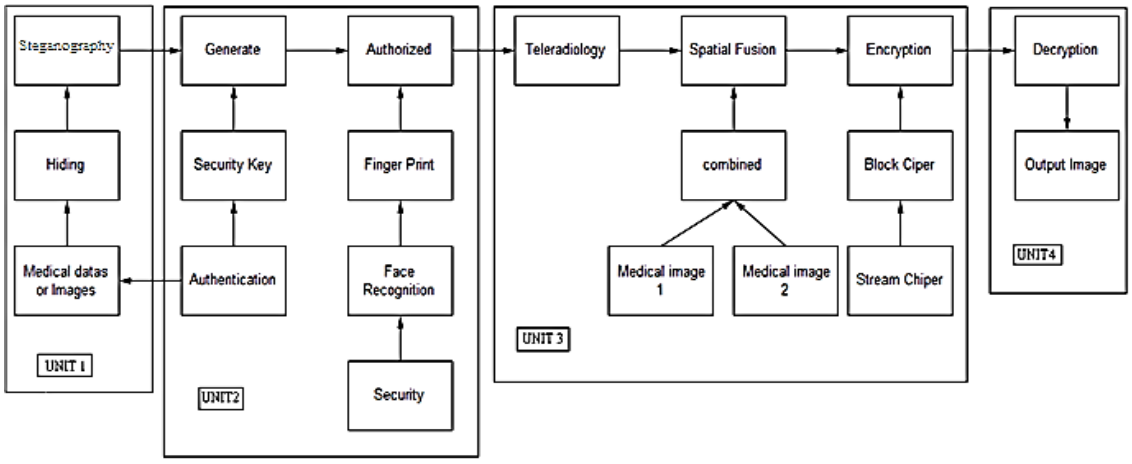

Fig. 1: System Structure for Feature Set Creation

D. Dual Steganography Primitives:

In this work, an amplitude modulation scheme is used to encode the steganographic images. Amplitude modulation, which embeds information multiple times into the spatial domain of an image, is widely used in the field of communication and signal processing. The approach to the steganography used in the framework is described. This technique is based on the work done in [12].

1) Encoding:

In this typical steganography scheme, pixels in the blue channel of a color image are altered to diminish the visible effects of the steganography. Based on the value of the bit, and its proportionality to the luminance, this value can be assistive or subtractive.

PWM(I,j)=P(i,j)+ (2s-1) PAV (i,j)q(1+ PSD(i,j)/A)(1+ PGM(i,j)/B) β(i,j) (1)

However, in the field of biometrics, color images are often replaced with grayscale images. Therefore, a new scheme must be implemented to work appropriately on grayscale images. The process is presented to alter the pixel values in a grayscale image in adjusting the strength of the standard deviation and the gradient image around point respectively

2) Decoding:

In order to achieve and retrieve the embedded bits in order, a decoding scheme must be used. In order to do this, this location of the embedded bits must be known. This can be done via a secret key that was found during the encoding stage. It is important to note that an original, non-steganography image is not used during decoding. First, to increase robustness to compression, affine transformations, added to every bit stream that was encoded in the previous section. Secondly, by estimating a linear combination of pixels in a cross shaped area around an encoded bit, the decoded bit can be extracted by the following:

$\hat{P}_{i,j}=1/4C\ (c\sum k=-c\ P\ WM\ (i+k,j) + c\sum k=-c\ P\ WM\ (i,j+k)-2PWM(i,j))$ (2)

Because decoding is based on an estimation procedure, the decoding of the bits can produce erroneous bits. This, in turn, can fail to extract the correct, original pixel value and lead to switched b0069ts during decoding

III. IMPLEMENTATION OF MULTIMODAL IDENTITY IN MOBILE MANAGEMENT SYTEM

The MIMMS will consist of several components both physical and conceptual, configured to optimize resources and maximize efficiency. The figure below shows the conceptual identity modeling and analysis architecture of the system with physical components located in the hospital management of the model. The main components of the MIMMS in terms of functional requirements are described in this section

A. Fingerprint Scanner and Camera:

To access the MIMMS terminal which is used to allow the user to submit credentials to the system and also the system can be automatically detect the device information from the terminal. One or more terminal can be allowed to access the system, in the corresponding sets of scanners and cameras.

A device which is finger scanning device is used to acquire the user fingerprints, and camera submits the sets of attributes database to the MIMMS for authentication. Communication between the scanner and system via hospital network.

A camera device is used for face recognition of the user and fingerprint scanner, submits the sets of attributes to the MIMMS for authentication, encryption and decryption of medical images to communicate with the hospital server

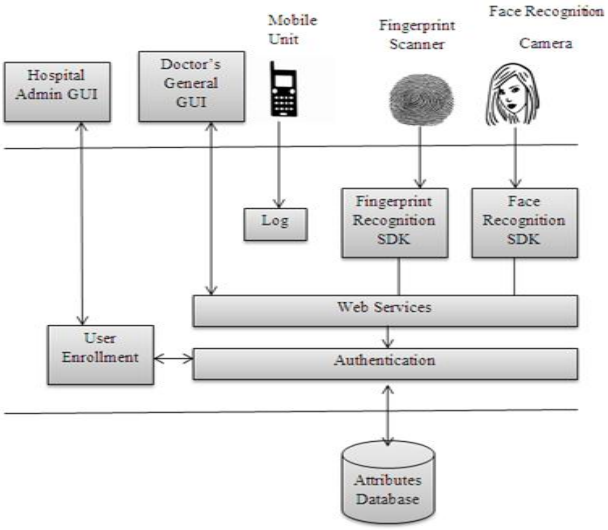

Fig. 2: General Scheme of the proposed multimodal system

B. Fingerprint and Face Recognition SDKs:

Fingerprint SDL Biometric recognition library is a component package responsible for the retrieval, verification, patient database and identify fingerprints. Fingerprint data is stored on the secure enclave of the Apple A7, A8, or A8X chip of the device, Android, Windows and is not stored on Apple servers, nor on iCloud or other servers. This component consists of libraries of classes to be used by the MIMMS

C. Database:

A secure database was developed in MySQL which takes four inputs and store in the database. This current system is the first stage of the MIMMS in which a secured database will be developed.

D. Verification User:

At Sending the patient data to the other hospital for medical clarification, is required to submit the full details of the subjects which are: full name, email address, patient name and password. The choice of finger to scan should be made appropriate and if necessary several fingerprints maybe used but this is not required for accuracy, rather for strengthening of the MIMMS. The system user then scans the user fingers and capture the image by clicking on verify. The user wanting to gain access to the service is verified against the details of the user already stored during the processing stage.

E. Successful Verification:

Generally, mobile user touches on verify and all user inputs are matched against the details in the database. If invalid input is entered a popup message specifying which attribute is invalid/or missing is presented. Depending on the security threshold set by the admin during the processing stage a subject will be accepted/rejected as a verified person.

IV. Experimental and Performance Evaluation

The experiments are conducted by medical image of dataset, DICOM digital imaging [15], and communications in a medical image of 512*512 pixels of 8 bit depth is used as a source medical image M and the IEEE visualization contest of [16] 8 bit depth 8*8 to 80*80 is used as the ROI to embed in the medical image. The Proposed method is evaluated in terms of image distortion by spatial fusion and steganography with capacity of embedding.

A. Image Quality and Embedding Capacity:

In this image quality analysis and capacity of embedding is to evaluate the hiding different sizes of patient images or text in the medical images. From this evaluation, that maximum size of 1bit per pixel is 75% of cover image can be

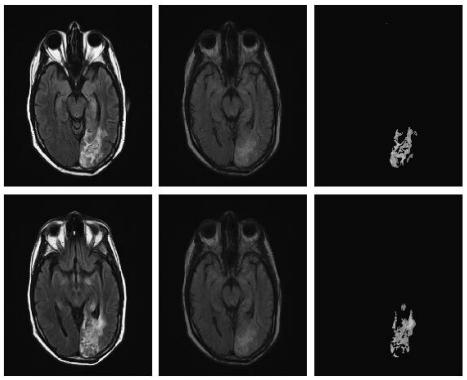

Fig. 3: Decomposed Images

In this error the medical images can be evaluated between the medical image and steganography image by means of the mean root square error, and also absolute error. Hence the Whole, the subjective qualities of the steganography images based on the evaluation of the modification rate provided best among the seven LSB methods as illustrated in Table I.

The QI ranges reaches +1 it is determined as best quality of image obtained. In this evaluation, if the value is high the steganography image is maintained with the original image. Compared to other approaches the LAP and DWT has given high values and our approach is provided the highest value than that of the other approaches embed in the host image. The evaluation of image quality is analyzed in the region of embedding, secret data, peak signal noise ratio, and error and modification rate of secret data of the watermarked medical images. The graph shows that, the average of the steganography image by the proposed method as a spatial fusion is lower compared to least significant bit are readjusted for the correct data extraction.

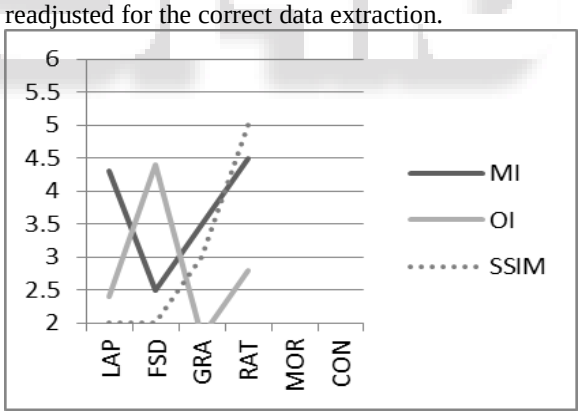

Fig. 4**:** Comparative result with various fusion Schemes

Can be provides the medical image information is maintained without alteration.

Method	VR	EER	IR
PCA-O	29,27%	20,15%	47,02%
PCA-S	33,84%	18,85%	52,98%
LDA-O	39,41%	16,23%	59,51%
LDA-S	42,33%	13,91%	64,96%
LBP-O	59,63%	10,83%	76,89%
LBP-S	65,82%	8,82%	84,21%

Table 1: Face Recognition Accuracies with The Original (O) And The Sythesized (S) Galleries

IMAGE	RMSE	MAE	PFE	Entrophy
CR	0.0065	4.20E-05	0.0046	0
CT	0.0021	5.34E-05	0.0047	0.0008
MR	0.0076	6.10E-05	0.00165	0.0056
US	0.0055	2.34E-05	0.0067	0.0012
XRAY	0.0023	2.34E-05	0.0038	0.0023
SCAN	0.0062	3.81E-05	0.0051	0.02377

Table 2: Image Error Analysis

The Information, measure the structure of similarity (SSIM), and universal quality index(QI) are used to measure the quality of the medical image. So the fusion technique are used for steganography, spatial fusion is compared and popular existing method such as LAP, DWT, shift variant, DWT, and morph graphic fusion process. The QI ranges reaches +1 it is determined as best quality of image obtained. In this evaluation, if the value is high the steganography image is maintained with the original image. Compared to other approaches the LAP and DWT has given high values and our approach is provided the highest value than that of the other approaches can be provides the medical image information is maintained without alteration. But the MR and US images provided comparably less higher error rate than CT,CR, XRAY, and SCAN. If the MAE is low, it determines the close prediction of eventual outcomes, which is comparably low during evaluation predicted to medical images fusion the patient data bits are embedded.

B. Mobile Unit:

The mobile unit in this study is comprised of a designed vital-sign signals acquisition module. According to user commands, the mobile unit can display waveforms in real-time, store data locally, and trigger an alarm. With regard to remote monitoring, the Pocket PC transfers these physiological data to a remote management unit in real-time by its built-in WLAN device.

V. Conclusion

In this paper, the mobile patient sharing medical images based on the joint FED system which is integrated on fully controlled environment for double priori-posteriori protection of medical images to solve all the verification and validation issues for Teleradiology system. The Clinical evaluation reveals that this mobile patient e-health care access the patient data system is user friendly, convenient and feasible. If the system gives the medical text data in spatial and encrypted domain with fingerprint and face authentication. In the face recognition which is widely encountered single sample problem for identification of faces with expression is augmenting the dataset of faces with synthesized images. For steganography verifies the availability and reliability of the medical text conducted jointly in the dual spatial fusion.

The experiments are conducted and two or more large and accepted databases; 3D Bosphorous and FRGC face database. If the experimental results that fuses the medical images can be encryption, embedding and spatial fusion algorithm are resulted in less time and computation complexity compared to other approaches. In the realistic synthesized face images improves the performance of the identification system. In the medical images using dual embedding scheme is different location with or without spatial fusion verifies the security issues for Teleradiology with maintain and computation complexity.

References

[1] P. Ruotsalainen, "Privacy and security in teleradiology," Eur. J. Radiol., vol. 73, pp. 31–35, 2010.
[2] S. A. Al-Damegh (2005, Oct./Dec.). Emerging issues in medical imaging. Indian J. Med. Ethics [Online]. 2(4). Available: http://www.ijme.in/134co123.html
[3] N. Hussain, W. Boles, and C. Boyd, "A review of medical image watermarking requirements for teleradiology," J. Digital Imag., vol. 26, no. 2, pp. 326–343, Apr. 2013.
[4] G. Pajares and J. M. de la Cruz, "A wavelet-based image fusion tutorial," Int. J. Pattern Recognit., vol. 37, no. 9, pp. 1855–1872, Sep. 2004.
[5] D. Bouslimi, G. Coatrieux, andC.Roux, "A joint encryptionwatermarking system for verifying the reliability of medical images," IEEE Trans. Inf. Technol. Biomed., vol. 16, no. 5, pp. 891–899, Sep. 2012.
[6] R. Anderson and C. Manifavas, "Chameleon: A new kind of stream cipher," Fast Softw. Encrypt., vol. 1267, pp. 107–113, 1997.
[7] A. Adelsbach, U. Huber, and A. S. Sadeghi, "Fingercasting-joint fingerprinting and decryption of broadcast messages," in Proc. IEEE Inf. Security Privacy, 2006, pp. 136–147.
[8] L. Shiguo et al., "Joint fingerprint embedding and decryption for video distribution," in Proc. IEEE Int. Conf. Multimedia Expo, 2007, pp. 1523– 1526.
[9] P. Viswanathan and P. VenkataKrishna, "Fusion of cryptographic watermarking medical image system with reversible property," Comput. Netw. Intell. Comput. Commun. Comput. Inf. Sci., vol. 157, no. 1, pp. 533–540, 2011.
[10] B. Woodward, R. S. H. Istepanian, and C. I. Richards, "Design of a telemedicine system using a mobile telephone," IEEE Trans. Inform. Technol. Biomed., vol. 5, pp. 13–15, Mar. 2001.
[11] P. Viswanathan and P. VenkataKrishna, "Cryptographic text watermarking medical image system with reversible property," Int. J. Inf. Process., vol. 5, no. 3, pp. 74–80, 2011.
[12] S. Fischer, T. E. Stewart, S. Mehta, R. Wax, and S. E. Lapinsky, "Handheld computing in medicine," J. Amer. Med. Inform. Assoc., vol. 10, no. 2, pp. 139–149, Mar./Apr. 2003.
[13] N. Erdogmus and J.-L. Dugelay, "Automatic extraction of facial interest points based on 2D and 3D data," in Proc. Electron. Imag. Conf. 3D Image Process. (3DIP) Appl., San Francisco, CA, USA, Jan. 2011, pp. 1–13.
[14] J. R. Tena, M. Hamouz, A. Hilton, and J. Illingworth, "A validated method for dense non-

rigid 3D face registration," in Proc. IEEE Int. Conf. Video Signal Based Surveill., Nov. 2006, p. 81.
[15] R.Capelli, M.Ferrara, A. Franco, D. Maltoni, "Fingerprint Verification competition 2006", Biometric Technology Today, vol.15,no. 7-8, pp 7-9, july- august 2007.
[16] P. Szeptycki, M. Ardabilian, and L. Chen, "A coarse-to-fine curvature analysis-based rotation invariant 3D face landmarking," in Proc. Int. Conf. Biometrics, Theory Appl. Syst., Sep. 2009, pp. 1–6.
[17] T. Maurer et al., "Performance of geometrix activeID 3D face recognition engine on the FRGC data," in Proc. Comput. Vis. Pattern Recognit. Workshops, 2005, p. 154.
[18] G. Pajares and J. M. de la Cruz, "A wavelet-based image fusion tutorial," Int. J. Pattern Recognit., vol. 37, no. 9, pp. 1855–1872, Sep. 2004.

