Securing Traffic at QoS-aware Residential Gateway Using Biometric Signatures

Pei-Chen Tseng, Jing-Wein Wang, *Member,* IEEE, and Wen-Shyang Hwang, *Member,* IEEE

Abstract —*Home networks are becoming ubiquitous. Multimedia is a primary home network application that is challenging bandwidth capabilities with respect to QoS and also creating issues regarding authorized access to the home network and its digital content. To deal with these issues, this study presents an embedded QoS-aware residential gateway (EmQRG) in the home network which classifies forwarded traffic for optimal use of bounded network bandwidth resources and, instead of traditional password methodology, requires bimodal biometric recognition of users. A laboratory EmQRG testbed with bimodal biometric recognition system (BBRS) is implemented via class-based queuing (CBQ) bandwidth management in a 3-PC network including a real DiffServ-capable CBQ-capable router, CCD camera and optical fingerprint reader. Novel computational methods are used for face and fingerprint analysis and recognition. It is confirmed that combining two biometric modalities improves performance, particularly for the false acceptance rate (FAR) that is considered the most serious home security problem. Experimental results demonstrate efficiency and robustness of both the EmQRG and the BBRS*[1].

Index Terms — Home Network, QoS, Embedded System, Biometric Identification.

I. Introduction

The number of microprocessor-embedded network-capable devices is increasing rapidly in the home. This together with broadband convergence networking (BcN) and inter-networked home devices is making the digital home network a ubiquitous 24-7 computing and communication environment [1]-[2]. A home gateway/residential gateway (HG/RG) is needed to interconnect multiple home devices to one another and to the Internet. Further, multimedia issues necessitate a means to manage user accounts for legal access to digital contents whether stored within the home network or stored in commercial libraries. Such security tasking must have suitable priority but without unnecessary disruption in the rest of the network. Good QoS should include suitable allocation of resources in the network (e.g. bandwidth, priority) so that data gets to its destination quickly and consistently. Real-time applications such as video play and VoIP are usually given higher priority than other applications. However, exceptionally high priority must be given to security tasks such that they have the right to interrupt many but not all media and similar data tasks.

Various groups including OSGi, DHWG, CELF, DLNA, UPnP forum, and RIAA are driving convergence of the digital home network for interoperability of multimedia networking and legal security/action in the home network. Their emphases can be summarized as follows:

- Interoperability of media management and control between different types of multimedia devices;
- QoS management for digital content, especially bandwidth and delay sensitive applications such as audio/video (AV) streams, voice, and games;
- User recognition based on biometric signatures.

This paper supports these objectives in a twofold manner. Firstly, based on our previous work [3] on a DiffServ-QoS bandwidth management mechanism during network congestion, we introduce an embedded QoS-aware residential gateway (EmQRG) in the home network to classify forwarded traffic for optimal use of bounded network bandwidth resources. EmQRG is verified experimentally in real-time via class-based queuing (CBQ) bandwidth management in a real DiffServ-capable CBQ-capable router, whereas our earlier QRG system was implemented only via Mrouter-PC emulation. Secondly, this paper protects digital content by a bimodal biometric recognition system (BBRS) using combined face and fingerprint traits. BBRS in conjunction with EmQRG is evaluated experimentally by the system shown in Fig. 1.

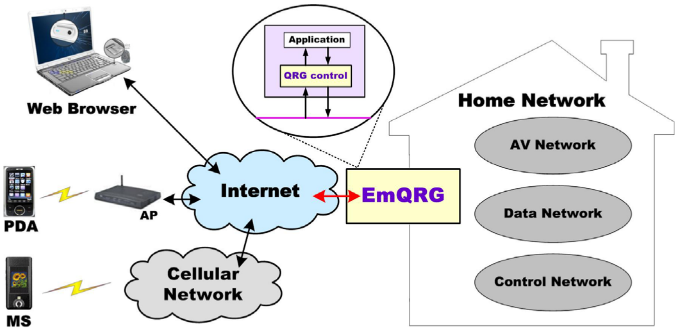


Fig. 1. Network architecture of EmQRG. Peripheral units are equipped with one or more biometric recognition devices (e.g. CCD camera, fingerprint reader, etc) for access control of home network digital content.

The architecture shows that the EmQRG interconnects the Internet and a home network that includes an AV network, a data network and a control network. Legal access from within

[1] Supported under Grant No. MoE 0940071581N by National Kaohsiung University of Applied Sciences and the Ministry of Education, Taiwan, ROC.

Pei-Chen Tseng and Wen-Shyang Hwang are now with Department of Electrical Engineering, National Kaohsiung University of Applied Sciences, Kaohsiung, Taiwan (e-mail: peichen@wshlab2.ee.kuas.edu.tw, wshwang@mail.ee.kuas.edu.tw).

Jing-Wein Wang is now with Institute of Photonics and Communications, National Kaohsiung University of Applied Sciences, Kaohsiung, Taiwan (e-mail: jwwang@cc.kuas.edu.tw).

Contributed Paper
Manuscript received June 10, 2008

or without the home is ensured by bimodal biometric recognition of the user prior to sharing of home network data. This is similar to using a user name and password, but BBRS uses biometric data to perform identification. Under BBRS, both the user's face and fingerprint biometric data are captured by suitable hardware that is connected to a host computer. In this study, CCD camera and optical fingerprint reader connect to a generic host computer (Fig. 1 "web browser"). BBRS security initialization requires that each authorized user provides clear images of face and fingerprints (two, one finger each hand). Screen display with sample data can be seen in Fig. 9(a) for the Client and Fig. 9(b) for the Data Server. The Data Server facial image includes both visible and invisible watermarks, to help prevent insertion of false identification into the BBRS database [4]. Face and fingerprint data are fed to the Data Server computer (Fig. 6) via the EmQRG through the home Ethernet. The EmQRG serves as a control center which performs security tasks, coordinates information sharing of digital content, translates communication protocols among the various home devices, works as a gateway to external networks and performs the DiffServ-QoS traffic classification mechanism. The EmQRG assigns forwarded traffic to an appropriate class for optimized treatment in compliance with user-specified priorities. The classified traffic is then sent to the appropriate destination through a DiffServ-capable CBQ-capable network.

CBQ provides fine granularity of bandwidth sharing and traffic priority control, including session level, thereby enabling service level guarantees for individual flows and aggregate traffic. In Fig. 1, received data come from the web browser and are processed by the Data Server. The Data Server contains a database of selected features for authorized users. The Data Server generates GO/NG decisions for the web browser by comparing its database with the biometric data that accompanies any new request for data access.

Traditional computer-based identification relies on user-remembered data such as a password or pin code. Alternately, the user carries an identifying physical object e.g. a card, key, token or RFID. Biometric identification relies on biological traits intrinsic to the user, for example the (relatively) unique patterns contained the user's face, fingerprint, palmprint, palm-dorsa, pores, veins or iris. Face and fingerprint are the most common biometric traits used for personal identification. Fingerprint identification is the oldest scientific biometric identification method. The high level of data in a fingerprint allows quick reduction of possible matches to a small number, even in a large database. Facial recognition is more difficult because of the relatively low levels of data and data-contrast available in the face. The third most common biometric ID uses voice patterns, but voice biometrics have proven difficult to employ reliably.

Fingerprint-based methods have proven so reliable that some commercial mobile devices and e-notebooks incorporate built-in fingerprint recognition devices. Fingerprints can be used in home networks [5]-[6], but digital fingerprinting requires contacting a communal physical surface, which presents contagion issues like during the recent SARS epidemic. Further, reliance on a single biometric provides only limited security. Improved security is obtained by using a second biometric. This study uses both fingerprint and facial recognition, i.e. a two-mode or bimodal biometric recognition system (BBRS). If voice or other parameters such as iris or skin pore pattern can be brought into play, then the system could be expanded to higher x-modal levels. Multi-modal biometric recognition shows great promise for access security in the home network.

This paper considers only a bimodal face/fingerprint system. Section II presents the DiffServ-QoS mechanism and the bimodal recognition algorithm. Implementation and experimental results are in sections III and IV. Finally conclusions and future work are summarized in section V.

II. DiffServ-QoS Mechanism and Biometric Algorithm

A. *DiffServ-QoS Mechanism*

The proposed DiffServ-QoS service architecture is based on a methodology whereby the EmQRG classifies forwarded traffic, marking each data packet for special treatment according to preset behavior aggregates. Each behavior aggregate is identified by a single DiffServ codepoint (DSCP) contained in the packet header. Within the DiffServ-capable network, packets are forwarded according to the per-hop behavior (PHB) associated with the DiffServ codepoint.

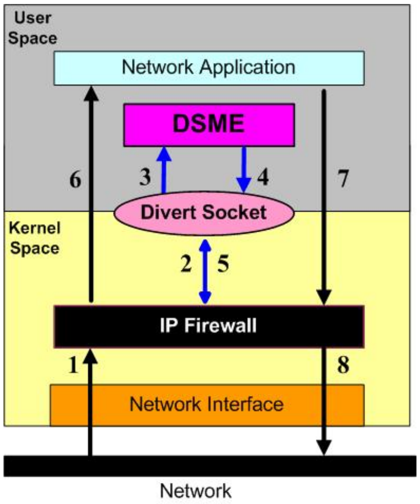


Fig. 2. Packet processing scenario by DSME via IP firewall.

Generally, traffic coming into the home network is already packetized with an IP header. It is passed to the kernel stack according to the network, after which the packets are injected into the network. In the employed OS, the IP firewall is located in the bottom of the IP stack. The IP firewall can filter incoming and outgoing IP packets that travel through the IP stack according to the firewall rules. To allow or deny IP packets to the IP stack, the IP firewall also provides flow accounting, flow shaping and flow redirection. Consequently the IP firewall is used to implement the so-called *DSME*

(DiffServ Marker Engine), as shown in Fig. 2, within the EmQRG system. Under Linux kernel version 2.4.18_eixp425, iptables are developed to support the IP firewall.

DSME is a mechanism which performs DiffServ-QoS. The following details the DSME packet processing scenario for traffic forwarded via the IP Firewall shown in Fig. 2, while the outgoing traffic is described in our earlier work [3]:

(1) Traffic (packet) forwarding through the EmQRG is intercepted by the IP firewall.
(2) DSME requests the IP firewall to redirect matched packets (e.g. IP packets that have the same destination address and the same port number) to the specific system port in conformance with the firewall rules.
(3) Once the packet is redirected to the specific system port, it does not travel directly forward.
(4) DSME adopts divert socket to bind the specific port, then reads raw packets (the whole IP packet including the IP header). The TOS (type of service) fields of the IP header of raw packets are modified by the DiffServ-TOS conversion values in DSME. The modified packets are sent back to divert socket.
(5) Then the modified packets are sent back to the firewall.
(6) The modified packets are then sent to the appropriate network application for further processing if needed. Otherwise, they go directly to step 8.
(7) The modified packets are sent to the firewall again.
(8) Finally, the modified packets continue to travel forward.

This mechanism utilizes a special type of RAW socket called divert (IPPROTO_DIVERT) that allows receiving and sending just like regular sockets. The difference is that a divert socket is bound to a specific system port, so the firewall can be instructed to send only certain packets, i.e. the firewall can filter out packets for the divert socket.

TABLE I
TRAFFIC CLASSIFICATION IN THE EMQRG

Traffic class	Protocol categories	Divert port	DiffServ setting
Security traffic (HTTP:8088)	TCP:8088	9988	EF
Web traffic (HTTP:80)	TCP:80	9980	AF22
File transfer traffic (FTP)	TCP: 21 TCP: 20	9921 9920	AF 31
Interactive traffic (SSH, TELNET)	TCP:22 TCP:25	9922 9925	AF21
Multimedia traffic (UDP)	UDP	9990	EF
Ping (ICMP)	ICMP	9910	BE

In the general home network environment, applications with very different characteristics and network requirements compete for bounded network resources. The proposed EmQRG can classify forward traffic flow as (but not limited to) security traffic, multimedia traffic, ICMP traffic, file transfer traffic, web traffic, interactive traffic, and BE traffic (traffic types listed in Table I). The EmQRG then assigns each class of traffic a preset DiffServ-QoS value. Herein, multimedia traffic, which belongs to the UDP transport service protocol, is marked as "EF" (expedited forwarding, typically DSCP value 46) to minimize delay and jitter and provide the highest level of aggregate QoS. This is performed by DSME via the IP firewall, which filters out the UDP traffic and redirects it to the specific system port 9990. DSME uses the divert socket to bind this port and modifies the TOS field to 184 in the IP header. After that, the EF bandwidth is reserved when the multimedia application is running.

B. *Elliptic face segmentation and face recognizer*

The proposed face segmentation method, designated FCExtractor for facial component extractor, uses a robust wavelet-based technique combining image- and feature-based methods. First the eyes and mouth are extracted, including the width of the mouth and the distance (width) from the outside of one eye to the outside of the other. Then, unlike prior methods which use rectangles, FCExtractor uses best-fit ellipses to enclose the facial region since use of rectangles tends to include unnecessary data such as hair, ears, neck, shirt collar, background, etc [7]-[9]. The elliptic region circumscribes the eye-mouth triangle. Moreover, a head orientation estimation is generated for estimating the view angle and is the basis for FCExtractor's multiview face recognition. FCExtractor requires no manual parameter adjustment for input images, can be implemented in real time and its underlying assumptions are minimal. The algorithm input information is a color head-and-shoulders view of a person. Background data is permissible. The facial region can be as small as 24 × 24 pixels. The FCExtractor algorithm consists of five operation stages and is outlined in Fig. 3. It begins with a low-level process like color detection. Then it uses higher level operations that involve some heuristic knowledge about the local connectivity of the face texture in the later stages. Thus, each stage makes full use of the results yielded by its preceding stage to refine the output.

Color information is used for the initial face-locating problem since human faces have a special color distribution that differs from most background objects, clothes, hair, etc [10]. FCExtractor performs a chrominance-based segmentation using a $Y C_b C_r$ color model, i.e. Y represents luminance while C_b and C_r represent chrominance components. When a face image is presented to the system (Fig. 3(a)), a modified $Y C_b C_r$ model [11] is applied to Fig. 3(a), producing Fig. 3(b). This image strongly emphasizes the color distribution found only in the human face and not found elsewhere, generating a strong clue as to the probable face location in an otherwise unconstrained environment. Next, one level overcomplete D4 wavelet decomposition [12] is performed on each probable (candidate) face area in Fig. 3(b) after mapping that candidate area to Fig. 3(a). Each candidate retains only the horizontal subband filtered images that contain wavelet coefficients since the wavelet transform provides divisions of the spectrum with sensitivity to horizontally distributed facial components. The cumulative results are shown in Fig. 3(c).

The next step considers the human T-shape face region, i.e. the smallest elliptical area that can be superimposed on a face that includes eyes and mouth. A novel nine-rectangle feature template (9RFT) derived from anthropometry is introduced for rapid computation at all scales. The 9RFT as defined for the face assumes that the T-shape part of the template (corresponding to the eye sockets and the mouth) has wavelet coefficients larger than the region corresponding to the cheeks. Previous studies commonly obtained multiple findings of the same face at different scales after small displacements horizontally and/or vertically. This makes it necessary to merge feature templates that can be counted as enclosing the same face. The decision criterion is devised to determine whether or not there is a substantial overlap between two or more templates. Merging two or more templates means averaging the size and the starting coordinates of the templates. The resultant effect of the merging process is the removal of the original windows and replacing them with the average. This process is repeated until all the templates marked for this stage of processing have been used. In our approach, a square block is used to represent each possible face candidate (Fig. 3(d)). Face candidates with different sizes that located in any part of an image can be located using this approach. In order to improve the detection reliability and accuracy, each of the selected possible face candidates is then processed to compensate for non-uniform lighting on the face region. After the normalization process, the image is passed to the support vector machines (SVM) [13] for further verification. The polynomial kernel is given a threshold value of -0.4 for this paper (Fig. 3(e)). An entropy-based smoothing filter is introduced to move the center from pixel to pixel in the rectangle of Fig. 3(e) to remove the coefficients located outside the facial component regions. This continues until all pixel locations have been covered and the facial component objects are ready for extraction. In the following we perform inter-orientation projection along the horizontal and vertical axes, respectively, to locate the eyes and mouth. Finally an adaptation is carried out to mark the eyes and mouth positions and refine the bounding rectangle into an ellipse that fits the facial shape (Fig. 3(f)). Details and face segmentation performance for benchmark databases are presented in [14].

The proposed face recognition system is composed of FCExtractor, lighting compensator, log-polar mapper and a genetically selected self-eigenface recognizer which gets the most discriminative feature subset as determined by the acceptance/rejection threshold value. The presented recognizer has two special merits. First, we present the derivation of the likelihood fitness function for the selection of discriminative self-eigenfaces with the concomitant threshold for recognition. Second, the selected self-eigenface subset on one hand maximizes the distances between the face images of different persons and on the other minimizes the distance between the face images of the same person.

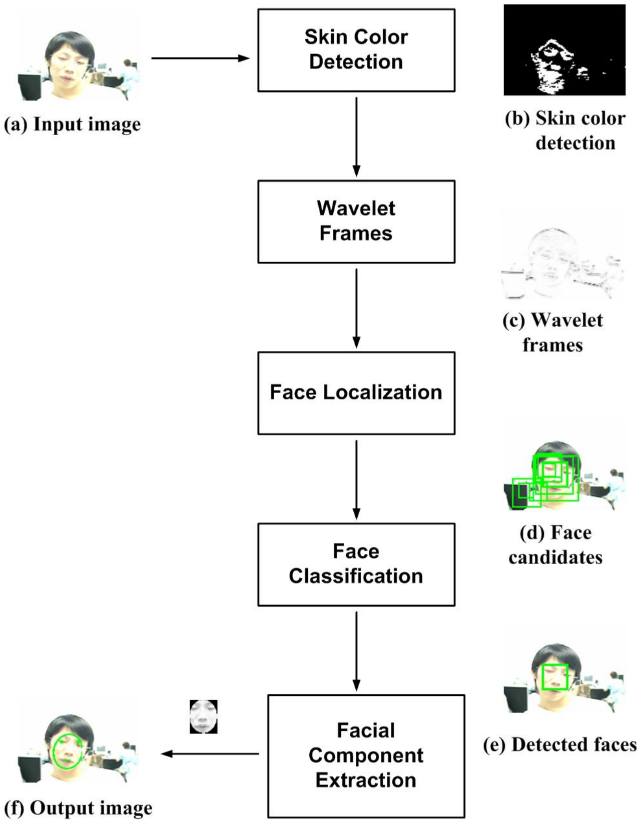


Fig. 3. Block diagram of proposed elliptic face segmentation.

The recognizer (Fig. 4) consists of several components. First, a lighting compensation scheme combines histogram specification and local normalization to confine the intensity distribution of each detected face to a desired dynamic range of illumination. This alleviates uneven illumination. Second, log-polar mapping is applied to obtain a reduced dimensional representation. Third, independent principal component analysis (PCA), also known as the self-eigenface technique [15], is performed on the log-polar images. This produces for each subject a set of eigenfaces whose dimension is larger than the number of samples in the training set. An innovative fitness function then uses genetic algorithms (GA) to select a discriminative self-eigenface subset to be used to recognize each subject [16]. The GA evaluation rule exploits the importance of individual features in optimal recognition and can be interpreted as maximizing *AAR* and *ARR*, while minimizing *FRR* and *FAR*. The formula is as follows:

$$\vartheta = \frac{\alpha_1 \cdot AAR - \alpha_2 \cdot FRR}{\alpha_3 \cdot ARR - \alpha_4 \cdot FAR} \cdot \left(1 - \frac{J}{K}\right) \qquad (1)$$

The ratio *J*/*K* of the selected feature number *J* to the total feature number *K* is *a priori* knowledge. There are four possible outcomes in a recognition system operating in an identification mode: accurate acceptance rate (*AAR*), accurate rejection rate (*ARR*), false rejection rate (*FRR*), and false acceptance rate (*FAR*). The fitness function security level is adjusted by tuning the action factors (α_1, α_2, α_3, and α_4). The values for α_1, α_2, α_3, and α_4 are experimentally determined and are set to $\alpha_1 = 100$, $\alpha_2 = 1$, $\alpha_3 = 1$, and $\alpha_4 = 100$.

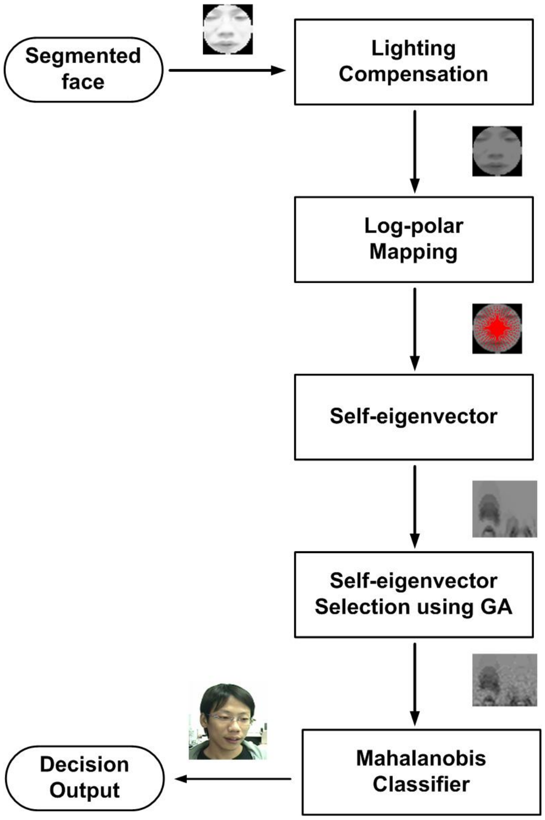


Fig. 4. Proposed self-eigenface recognizer.

C. *Fingerprint recognition by kernel subregion algorithm*

Fingerprint recognition herein is based on the kernel subregion. The kernel point is defined as the point in the fingerprint that has the maximum direction change. The kernel subregion is the 100 × 100 pixel area surrounding the kernel point. Log-polar mapping is used to extract the translation-invariant features derived from the discrete wavelet frame transform (DWFT) [12]. The formula of (1) genetically selects the most discriminative log-polar feature subset by disregarding redundant features via SVM classification. This reduces final error at the decision stage as the result of minutiae extracted at earlier stages [17]-[19]. An alternative filter-based method [20] works well but is not suitable for on-line systems because of expensive computation.

Use of the fingerprint kernel subregion accelerates identification. The initial threshold is set as the mean of the energy image. Then the threshold value is gradually changed until the observed pixel-of-threshold (point) density of the whole image is around 50% ~ 60%, which is good representation for objects we are detecting [21]. The novelty of our framework comes from:

(1) the kernel-based method has good tolerance for image noise and capture-to-capture irregularities;
(2) use of a feature alignment line to minimize feature variations in the feature extraction stage;
(3) derivation of a fitness function for selection of discriminative features and threshold values.

The block diagram in Fig. 5 operates as follows:

- Off-line phase:

Each fingerprint's kernel subregion is segmented in a preprocessing module and then fed to the feature extraction module. The module rejects features with no discriminative information, thus producing near-optimal feature subsets which are then stored as Fingercode at the Data Server.

- On-line phase:

The fingerprint reader captures an image. The kernel subregion is segmented as in the off-line phase and then fed to the feature extraction module. The extracted fingerprint features are compared to the pre-stored Fingercode.

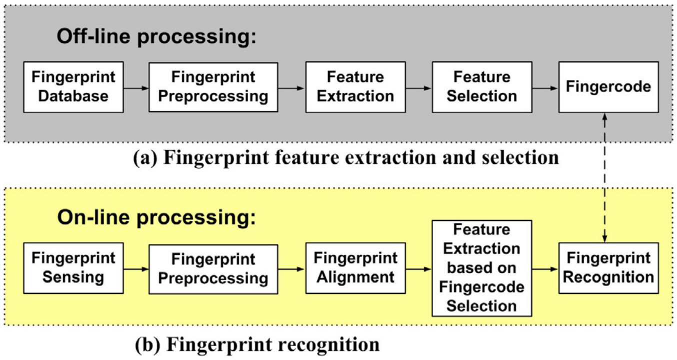

Off-line processing:
Fingerprint Database
Fingerprint Preprocessing
Feature Extraction
Feature Selection
Fingercode
(a) Fingerprint feature extraction and selection
On-line processing:
Fingerprint Sensing
Fingerprint Preprocessing
Fingerprint Alignment
Feature Extraction based on Fingercode Selection
Fingerprint Recognition
(b) Fingerprint recognition

Fig. 5. Flowchart of proposed fingerprint recognition algorithm.

III. System Implementation

A BBRS-enabled experimental home network based around an EmQRG is implemented. The EmQRG itself is embedded in an Intel-based mainboard running a Linux OS. As seen in Fig. 7, our network contains a CCD camera and an optical fingerprint reader and three PCs. The Internet is simulated by four real DiffServ-capable routers [22].

The EmQRG functions as the heart of the home network, and interconnects a wide variety of devices. Multimedia and game devices have wide bandwidth and high priority. However, movie downloading for storage can have a much lower priority. A digital home will have a large number of sensors (e.g. fire, smoke, refrigerator temperature) and switches (e.g. lock/unlock door, turn on/off lights). Some of these, for example fire sensors, have extremely high priority, but their bandwidth demands are small. Regardless, EmQRG must coordinate these various data streams reliably.

Since every device in the network has its own IP address, basic network functionality is confirmed by pinging all the devices. Pinging however involves only tiny and momentary bandwidth. Multimedia is a primary issue in the home network, so next we watch a movie on the second PC that is stored on the hard disk of the first PC. Success at this task confirms bandwidth capabilities, but only for a non-congested traffic situation. So then we test different congestion problems, such as streaming two or three movies at the same time, first without and then with CBR (constant bit rate) periodic background traffic. Good QoS for a multistreaming media under concurrent heavy periodic traffic lets us be sure the DiffServ-QoS mechanism is successfully analyzing, classifying and forwarding the various types of traffic.

Testing the BBRS system requires initial setup. Threshold values must be set for both face and fingerprint. A database containing face/fingerprint data for authorized users must be established. We also set up a database for specifically non-authorized users such as known threats to local security, for example a child with a history of accessing the parents' adult video.

The authorized user database starts with image capture of an authorized user via the Client's (Fig. 6) video camera. The current BBRS trains the system with 100 near-frontal pictures of each authorized user. In fact, these 100 pictures could be extracted from a short video sequence with suitable variation of the user's image, e.g. varying user facial angles, putting on and removing eyeglasses, modulation of lighting, etc. However, we used a slightly different method in the laboratory tests. First we select 5 of our laboratory colleagues as authorized users and make 100 video single-frame captures of each person, for a total of 500 pictures. These images are collected on three different days, namely the first, 8th, and 15th days. A similar database of anti-authorized persons is made from 10 other laboratory colleagues, 10 images of each, a total of 100 pictures. Authorized and non-authorized facial images together make a total of 500 + 100 = 600. All facial images are collected in frontal (0°) or near-frontal view (pan and tilt ±30°). Each facial image is elliptically segmented as shown in Fig. 3 and then fed to the Data Server with size normalization to 64 × 64 pixels. Thus the recognizer is trained with 600 video captures. The Data Server applies the initial processing steps (Fig. 4) to each face, namely lighting compensation and log-polar mapping. The resulting 600-face data group is trained by self-eigenvector, thus producing a 64 × 64 matrix representing the extracted features of the 15-person database (5 authorized, 10 anti-authorized). The extracted features are further refined through training by genetic representation. Three runs by different GA seeds to produce an optimized extracted feature set for the recognizer system. The parameters for the designed GAs are determined experimentally: population size = 20, number of generation = 1000, probability of crossover = 0.5. A mutation probability value starts with a value of 0.1 and then is varied as a step function of the number of iterations until it reaches a value of 0.001. The recognition rate is averaged for the three different-seed runs. Next a Mahalanobis distance classifier [23] extracts the optimized features for authorized and anti-authorized user, completing the database for the faces.

The fingerprint database begins with fingerprint images from our five authorized users, 600 for each user, 300 left and 300 right, any finger acceptable but the user needs to continue to use the same finger. Herein we use exclusively index fingers. The fingerprint reader provides an image of 300 × 260 pixels. Like the faces, the fingerprints are collected three times (first, 8th, and 15th days), 200 prints per session (100 per finger). For the anti-authorized database, 20 fingerprints (10 per finger) are collected at 3 sessions (as above) for a total of 60 prints per anti-authorized user. Our fingerprint collection procedure produced a total of 3000 (5 × 3 × 200) fingerprint images for authorized users and 600 (10 × 3 × 20) for anti-authorized users. An experimental database of authorized and anti-authorized users is now completed.

IV. Experimental Results

The schematic layout and the laboratory physical installation are shown as Figs. 6 and 7, respectively. The DiffServ-capable network is composed of four real DiffServ-capable routers [22], designated R1, R2, R3, and R4, which are configured as DiffServ routers and incorporate the functions of policing flows and forwarding data according to the DiffServ field markings. A network processor IXP425 embedded system functions as the EmQRG. Three PCs function in the system, one as the Client computer in the home network, one as a traffic generator called H1 and one as a traffic receiver called the Data Server. The EmQRG and H1 are each connected by its own 100 Mbps Ethernet link to the router R1. The link between the two DiffServ routers is a 10 Mbps Ethernet link, i.e. a bottleneck. This bottleneck is intentionally designed into our testbed to challenge and verify the QoS capabilities of the EmQRG. The router R2 then connects to the end system Data Server over a 100 Mbps Ethernet link. The router R1 with CBQ traffic control of bandwidth management is for optimized use of bounded network resources. The bandwidth allocation for each DiffServ-QoS traffic classification at the router R1 is as shown in Table II. In a real home network situation, the Data Server would probably be located inside the home network, possibly within the Client itself. For laboratory test we chose to locate the Data Server outside so as to simulate an Internet or large LAN environment both without and with background traffic, with QoS potentially compromised by the above-mentioned bottleneck. This situation is further complicated by security tasks requiring the Client to access a database outside of its local network, a case that could easily occur if a home network were linked into a community security system.

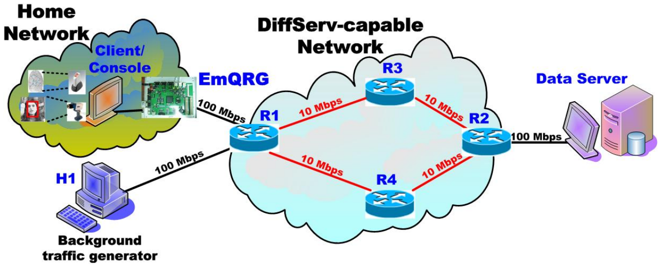


Fig. 6. Logical layout of testbed.

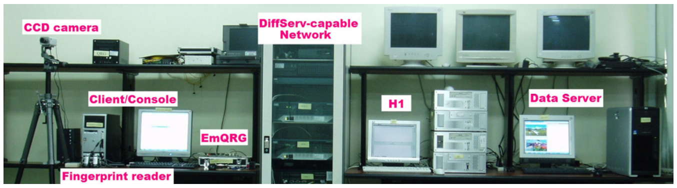


Fig. 7. Physical layout of testbed.

TABLE II
BANDWIDTH ALLOCATION AT DIFFSERV-CAPABLE CBQ-CAPABLE R1 ROUTER

Flow Type	AF1x	AF2x	AF3x	EF	BE
Bandwidth Allocation (Mbit)	1	1	1	4	3

Experiment 1: The Fig. 7 links the real DiffServ-capable routers by 5 isolated channels with the non-sharable bandwidths shown in Table II and a total bounded bandwidth of 10 Mbps. The Client and H1 separately deliver UDP multimedia film by vlc to the Data Server, which contains two different IPs for the two different senders. To simulate congested conditions, H1 also sends a background traffic (i.e. BE traffic) streams, 750 pkts/s, 512 bytes/pkt shown in Fig. 8(a), to the Data Server. If the EmQRG activates the DiffServ-QoS mechanism for classifying forwarded traffic priorities, then the packet header of any UDP traffic is changed by DSME to EF according to the EmQRG traffic classifications shown in Table I.

In experiment 1, the results of statistical analysis by the command “sh interfaces accounting” at the router R1 and by the PRTG Traffic Grapher at the Data Server show that total traffic equals 160417 packets (111615562 bytes) with 29936 packet drops to be sent. BE traffic equals 146284 packets (92422948 bytes) with 29936 packet drops. EF traffic equals 14133 packets (19192614 bytes) with 0 packet drops. This means the film is showing at the Data Server with a *18.66%* packet drop rate. Comparative QoS during network congestion is seen in Fig. 8(b). The upper image is from the Client under EmQRG with DiffServ-QoS activation, showing high QoS *without* packet loss. The lower image is from H1 without DiffServ-QoS activation, showing poor QoS and a *20.46%* packet drop rate. The lack of DiffServ-QoS activation clearly results in unacceptably low image quality, but with EmQRG and DiffServ-QoS the QoS is excellent. Numerically, the relative QoS’s can be evaluated in Fig. 8(c) by a Live Graph display of experiment 1 as generated by PRTG Traffic Grapher packet sniffing at the Data Server.

Experiment 2: An authorized user captures his current face/fingerprint data at the Client, watermarks the facial data and sends it (as in Fig. 9(a)) to the Data Server. The Data Server performs feature extraction on the face/fingerprints and compares the results with its database. The Data Server finds a positive match and displays Fig. 9(b), showing the watermarked picture in the lower left and the database picture in the lower right, with the invisible watermark to the left. Below that is the bit error rate (BER) of the picture’s invisible watermark relative to the original watermark stored in the database. Below that is the computation time in milliseconds. The two recently captured fingerprints are shown in the upper left, with the user’s database face in the upper right. Input and database fingerprint/face data match so access is granted. The user’s database file photo along with approval of the access request are sent to the Client as Fig. 9(c).

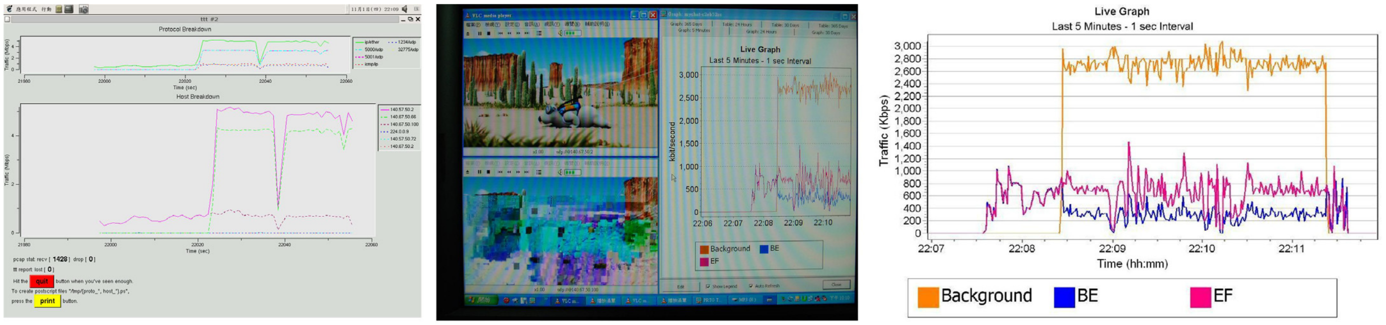
Fig. 10 shows results for an unauthorized user. Initial data capture is as Fig. 10(a). The Data Server finds a non-match for both face and fingerprints and shows Fig. 10(b). Fig. 10(c) is returned to the Client, rejecting the access request. In fact, if either fingerprint or face fails the match test, the Data Server immediately stops the recognition process and returns a rejection to the Client.

Experiment 3: Over one week our laboratory group repeatedly tried to access the BBRS-protected system. 600 authorized and 1000 unauthorized access attempts were made. Data analysis is made for the two monomodal cases and the bimodal case. Face-only monomodal data show authorized users had 562 correct acceptances, 12 incorrect acceptances and 26 incorrect rejections; unauthorized users had 965 correct rejections and 35 incorrect rejections. Fingerprint-only monomodal data show authorized users had 578 correct acceptances, 10 incorrect acceptances and 12 incorrect rejections; unauthorized users had 973 correct rejections and 27 incorrect acceptances. Face + fingerprint bimodal data show authorized users had 553 correct acceptances, 6 incorrect acceptances and 41 incorrect rejections; unauthorized users had 991 correct rejections and 9 incorrect acceptances. The experiments provide the values in Table III, showing improved performance from bimodality, particularly for the FAR (false acceptance rate) parameter, which is the most important factor for safeguarding the home network.

Recognition/decision execution time is directly related to size and background complexity of the image being processed. Execution time also depends on computer speed and the efficiency of the recognizer algorithm. Processing time on a 3.0 GHz Pentium PC was around 1 second per face and 0.5 second per fingerprint. These speeds meet the requirements of on-line recognition, but the recognizer algorithm could be further optimized and parallelized for increased speed.

TABLE III
RECOGNITION RATES OF THE PROPOSED METHOD

Biometric signature	Face	Fingerprint	Face + Fingerprint
AAR	93.67%	96.33%	92.17%
ARR	96.50%	97.30%	99.10%
FAR	**2.94%**	**2.31%**	**0.94%**
FRR	4.33%	2.00%	6.83%

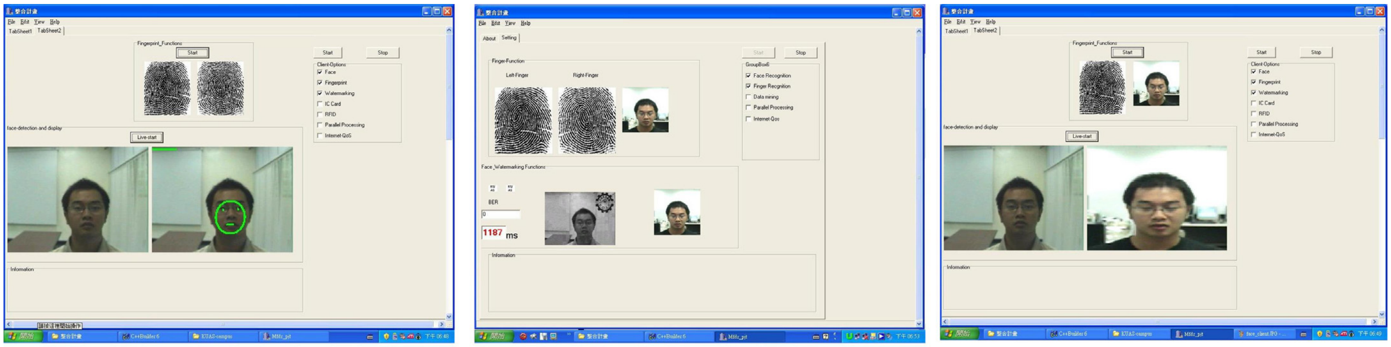


(a) The ttt graph displayed at H1

(b) Film displayed at Data Server: upper image is from Client through EmQRG with DiffServ-QoS activation, while lower is from H1 without DiffServ-QoS activation.

(c) Live Graph displayed via PRTG at Data Server

Fig. 8. The result of experiment 1.

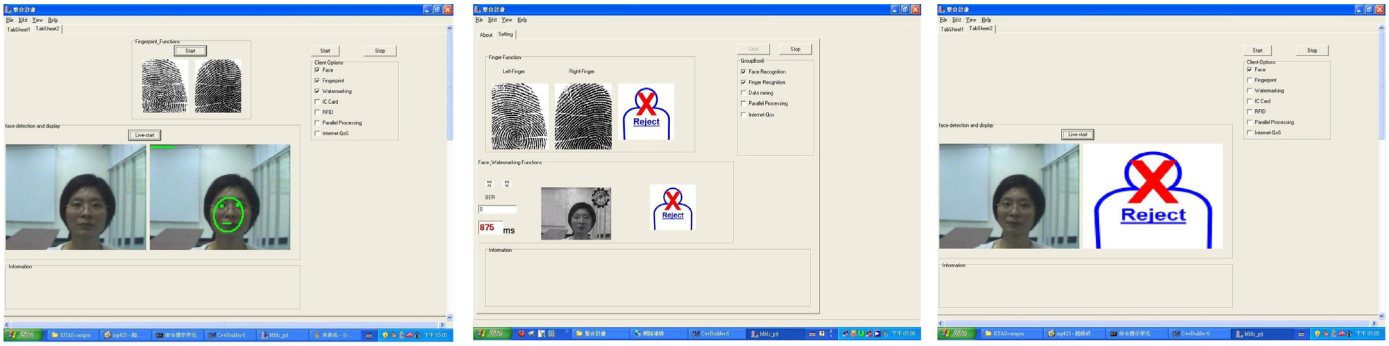


(a) Biometrics captured at Client

(b) Result after processing at Data Server

(c) Biometrics result at Client

Fig. 9. Results indicating match of input and stored biometric data, hence access approval.



(a) Biometrics captured at Client

(b) Result after processing at Data Server

(c) Biometrics result at Client

Fig. 10. Results indicating mismatch of input and stored biometric data, hence access rejection.

V. Conclusions and Future Work

A QoS-aware Residential Gateway (EmQRG) was embedded in an experimental home network implemented in real-time via class-based queuing (CBQ) bandwidth management in a real DiffServ-capable CBQ-capable router. The EmQRG classified forwarded traffic under congested bandwidth-limited experimental conditions. Experimental results showed EmQRG maintained excellent QoS. A bimodal (face and fingerprint) biometric recognition system (BBRS) was embedded in the EmQRG testbed. BBRS authorized users were correctly accepted in *92.17%* of a series of real-time experiments, while false acceptance rate (FAR) was a low *0.94%*. Recognition speed of our laboratory testbed BBRS was easily adequate for real-time use. Further improvements in speed and accuracy are believed easily attainable but were not investigated in this proof-of-concept study. It is confirmed that combining two biometric modalities improves performance, particularly for the FAR parameter that is so important in home network security. The present BBRS requires the capture/analysis of 100 or more facial images, each with slightly different pose and lighting. Future work will reduce system training requirements, possibly by employment of a generic learning approach [24].

References

[1] J. Park, K. Lee, D. Park, and K. Moon, "QoS-aware bridge for high-speed powerline communication and ethernet," *IEEE Transactions on Consumer Electronics*, vol. 53, no. 1, pp. 50-54, Feb. 2007.

[2] S. G. Choi, D. O. Kang, and J. W. Lee, "A media distribution system supporting priority-based QoS in a home network," *The 8th International Conference on Advanced Communication Technology, ICACT 2006* , vol. 3, pp. 1532-1536, Feb. 2006.

[3] W. S. Hwang and P. C. Tseng, "A QoS-aware residential gateway with bandwidth management," *IEEE Transactions on Consumer Electronics*, vol. 51, no. 3, pp. 840-848, Aug. 2005.

[4] A. Lumini and D. Maio, "Adaptive positioning of a visible watermark in a digital image," *IEEE International Conference on Multimedia and Expo, ICME 2004*, vol. 2, pp. 967-970, Jun. 2004.

[5] P. Corcoran and A. Cucos, "Techniques for securing multimedia content in consumer electronic appliances using biometric signatures," *IEEE Transactions on Consumer Electronics*, vol. 51, no. 2, pp. 545-551, May 2005.

[6] P. Corcoran, C. Iancu, F. Callaly, and A. Cucos, **"**Biometric access control for digital media streams in home networks**,"** *IEEE Transactions on Consumer Electronics*, vol. 53, no. 3, pp. 917-925, Aug. 2007.

[7] L. F. Chen, H. Y. Mark Liao, J. C. Lin, and C. C. Han, "Why recognition in a statistics-based face recognition system should be based on the pure face portion: a probabilistic decision-based proof," *Pattern Recognition*, vol. 34, pp. 1393-1403, 2001.

[8] A. Martinez, "Recognizing imprecisely localized, partially occluded, and expression variant faces from a single sample per class," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, no. 6, pp. 748-763, Jun. 2002.

[9] K. Messer, J. Kittler, M. Sadeghi, M. Hamouz, A. Kostyn, S. Marcel, S. Bengio, F. Cardinaux, C. Sanderson, N. Poh, Y. Rodriguez, K. Kryszczuk, J. Czyz, L. Vandendorpe, J. Ng, H. Cheung, and B. Tang, "Face authentication competition on the BANCA database," *ICBA, Lecture Notes in Computer Science*, vol. LNCS 3072, pp. 8-14, Jul. 2004.

[10] M. St¨orring, "Computer vision and human skin colour," PhD dissertation, Faculty of Engineering and Science, Aalborg University, 2004.

[11] C. Garcia and G. Tziritas, "Face detection using quantized skin color regions merging and wavelet packet analysis," *IEEE Transactions on Multimedia*, vol.1, no. 3, pp. 264-277, Sep. 1999.

[12] S. Mallat, *A Wavelet Tour of Signal Processing*, 2nd ed., Academic Press, 2001.

[13] Christopher J. C. Burges, "A tutorial on support vector machines for pattern recognition," *Data Mining and Knowledge Discovery*, vol. 2, no. 2, pp. 121-167, 1998.

[14] J. W. Wang, "Precise face segmentation for recognition," *IEEE International Conference on Image Processing, ICIP 2006*, pp. 2045-2048, Oct. 2006.

[15] L. Torres and J. Vilá, "Automatic face recognition for video indexing applications," *Pattern Recognition*, vol. 35, pp. 615-625, Mar. 2002.

[16] Z. Sun, G. Bebbis, and R. Miller, "Object detection using feature subset selection," *Pattern Recognition*, vol. 37, pp. 2165-2176, Nov. 2004.

[17] A. Ross, S. Dass, and A. Jain, "A deformable model for fingerprint matching," *Pattern Recognition*, vol. 38, pp. 95-103, Jan. 2005.

[18] Y. Chen, S. Dass, A. Ross, and A. Jain, "Fingerprint deformation models using minutiae locations and orientations," *Proceedings of the seventh IEEE Workshop on Applications of Computer Vision, WACV/MOTION*, vol. 1, pp. 150-155, Jan. 2005.

[19] L. Sha, F. Zhao, and X. Tang, "Fingerprint matching using minutiae and interpolation-based square tessellation fingercode," *IEEE International Conference on Image Processing, ICIP 2005*, vol. 2, pp. 41-44, Sep. 2005.

[20] D. Batra, G. Singhal, and S. Chaudhury, "Gabor filter based fingerprint classification using support vector machines," *Proceedings of the IEEE INDICON 2004, First India Annual Conference*, pp. 256-261, Dec. 2004.

[21] C. Y. Hsu and J. W. Wang, "Fingerprint recognition using kernel subregion of fingerprint image," *CVGIP2006*, Oral Section, Taoyuan Taiwan, Aug. 2006.

[22] P. C. Tseng, J. K. Shiung, C. T. Huang, S. M. Guo, and W. S. Hwang, "Adaptive car plate recognition in QoS-aware security network," *The Second IEEE International Conference on Secure System Integration and Reliability Improvement, SSIRI 2008*, Jul 2008.

[23] R. O. Duda, P. E. Hart, and D. G. Stork, *Pattern Classification*, 2nd ed., Wiley Press, 2000.

[24] J. Wang, K. N. Plataniotis, J. Lu, and A. N. Venetsanopoulos, "On solving the face recognition problem with one training sample per subject," *Pattern Recognition*, vol. 39, pp. 1746-1762, 2006.

Pei-Chen Tseng was born in Hualien, Taiwan, in 1968. She graduated from National Taipei Institute of Technology in Electronic Engineering in 1990. From 1990 to 2001 she worked for Siemens as a telecommunication engineer, including five years as a testing engineer in EWSD switching systems, one year as a technical support engineer in switching systems, one year as a technical specialist in mobile telecommunication systems, and almost five years as a RF engineer in mobile telecommunication systems. Studying at the National Kaohsiung University of Applied Sciences, Kaohsiung, Taiwan, she received a B.S. in electrical engineering in 2002, a M.S. in 2004, and is currently pursuing a Ph.D. with a focus on communication, protocol, multimedia, and networking. Her research interests include home networking, network security, and GSM/GPRS/CDMA telecommunication systems. She is a student member of IEEE.

Jing-Wein Wang received B.S. and M.S. degrees in Electronic Engineering from National Taiwan University of Science and Technology in 1986 and 1988, respectively, and a Ph.D. degree in Electrical Engineering from National Cheng Kung University, Taiwan, in 1998. From 1992 to 2000 he was a principal project leader at Equipment Design Center of PHILIPS, Taiwan. In 2000, he joined the faculty of National Kaohsiung University of Applied Sciences, where he is currently an associate professor in the Institute of Photonics and Communications. His current research interests are combinatorial optimization, pattern recognition, wavelets, and biometric applications. He is a member of IEEE.

Wen-Shyang Hwang received B.S., M.S., and Ph.D. degrees in Electrical Engineering from National Cheng Kung University, Taiwan, in 1984, 1990, and 1996, respectively. He is currently a professor of Electrical Engineering, and the chairman of department of computer science and information engineering in National Kaohsiung University of Applied Sciences, Taiwan. His current research interests are in the fields of storage area networks, WDM Metro-ring networks, performance evaluation, multimedia wireless communication, mesh networks, software design for embedded systems, Internet QoS, and Internet applications. He is a member of IEEE.