ISSN 1345-3041

MITSUBISHI ELECTRIC Jun. 2005／Vol.111

ADVANCE

Evolving Mobile Phones

MITSUBISHI ELECTRIC

Changes for the Better

Jun. 2005 / Vol. 111

MITSUBISHI ELECTRIC ADVANCE

Evolving Mobile Phones

Cover Story

Following the introduction of first-generation mobile phone service in 1979 and second-generation in 1993, third-generation service (based on W-CDMA) was launched in October 2001. 3G offers high-speed, high-data, and high-quality services. Furthermore, modern multimedia services, which are accessible to many, are driving generation changes in the mobile industry.

In 2003, many mobile manufacturers released the FOMA 900i series. Mitsubishi led this trend by introducing the D900i, a 3G handset that enables users to instantly enjoy high-speed data communication and multimedia services.

The following technical reports portray the future of evolving mobile telephony, emphasizing technology development, new services and networks.

• **Editorial Inquiries**
Keizo Hama
Corporate Total Productivity Management
& Environmental Programs
Fax 03-3218-2465

• **Product Inquiries**
Kazuhiko Takase
Research & Development Department
Mobile Terminal Center
FAX 06-6495-6522

Mitsubishi Electric Advance is published on line quarterly (in March, June, September, and December) by Mitsubishi Electric Corporation.

CONTENTS

Technical Reports

Overview

Author: *Kazuaki Murota**

Over the past 100 years, wired and wireless communication have repeatedly extended the distance and transmission speed by competing with each other. I myself was in the vortex of this race, yet without knowing what we should have been targeting. With the help of progress in semi-conductors and computers in the past several years, I can now see the exquisite alliance between wired and wireless communication and belatedly understand the direction we should be heading, namely, a ubiquitous network society in which the surrounding environment spontaneously serves us.

The infrastructure for ubiquitous networks lies in technological innovations such as optical fiber, mobile communications, IP networks and short-distance wireless systems. Among them, mobile communication systems, especially the third-generation mobile system, will probably serve as the most accessible device from a macro perspective, because we can carry a mobile all the time, both indoors and outdoors. Further discussions on fourth-generation mobiles have already started. In the future, different systems instead of a single system are preferable depending on the situation. The key words are mobility, security, broadband and low cost.

Recently, a trial to connect physical space and virtual intelligent space accumulated on the Internet has been started. If this virtual cyber space could be connected to the coordinates of actual space, the frontiers of knowledge would be dramatically extended. In fact, detecting tags placed in actual space or accessing the related intelligent space based on GPS (Global Positioning System) data are already being conducted. This flow may well reverse in the future, in which the actual space will find users and provide them with custom-made services. In other words, if a sensor network capable of detecting weather changes or dangerous objects on the streets provides users with information, the demands placed on and expectations for the communication infrastructure will become more versatile.

Thanks to the information society today, we are now able to know what is happening on the other side of the world or have an instant grasp of history. This epoch-making technology has made it possible to "conquer time". The past development trend can be summarized as conquering two dimensions (distance), three dimensions (space) and four dimensions (time). We are now developing a fifth technology that will liberate us from the problems of social and/or personal inconsistencies, in which numerous subjects existing in the same time in the same coordinates still disagree with each other.

In a ubiquitous network society, reforms of business and work style are being considered, but this is only a simple example. By overcoming inconsistencies, I look forward to new technology enabling us to create a fair democratic society where there is neither conflict nor individual barriers, thus contributing to society in the future.

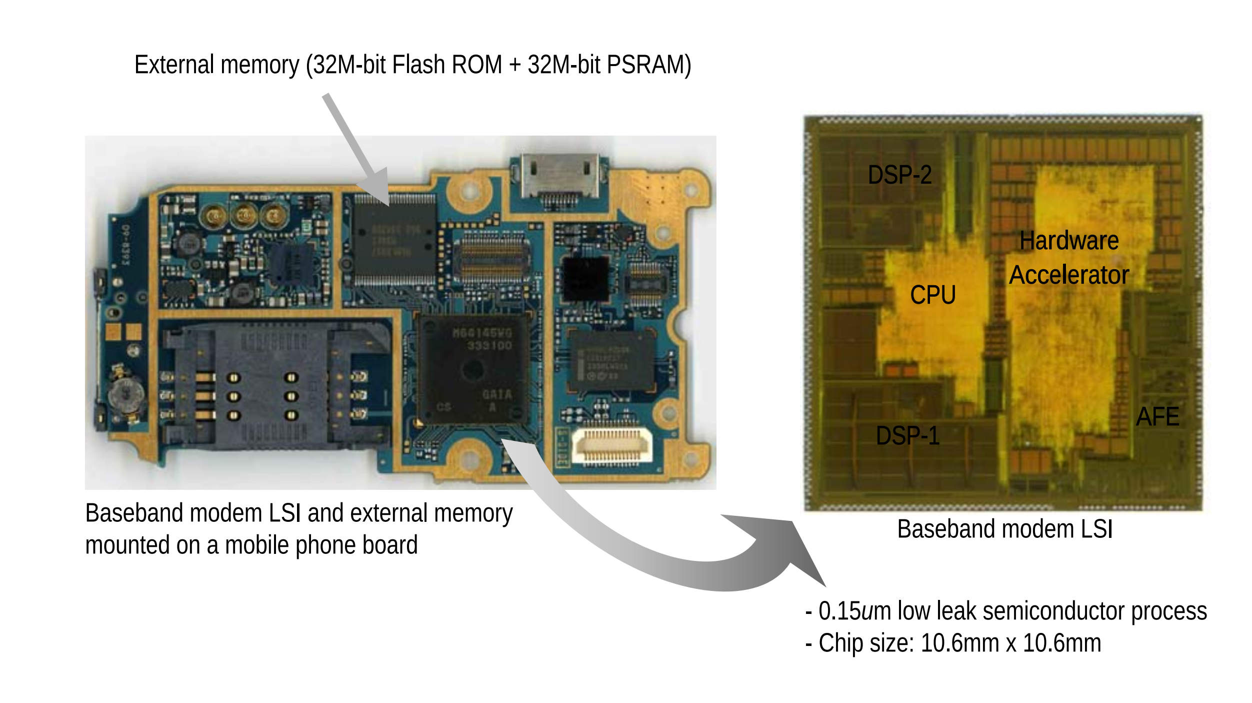
** Communication Systems Group*

Low Power Baseband Modem LSI

Authors: *Masayuki Yamamoto*[*] and *Ryosuke Takeuchi*[*]

Mitsubishi Electric Corporation has developed a low power baseband modem LSI for W-CDMA mobile phones. The LSI was installed in D900i, achieving approx. 170/90 minutes of continuous talk time for voice/video phones, and approx. 550/420 hours of continuous standby time in stationary/moving states respectively. The architecture of this LSI is similar to that of the baseband modem LSI chipset used for D2101V, which was optimized for lowering power consumption. To realize this LSI, 0.15 um low leak semiconductor process technology was applied to integrate an AFE (Analog Front End), a CPU, two DSPs and a hardware accelerator on a 10.6mm-square silicon chip. Then the chip was packed into a 15mm-square, 513-ball FBGA, and along with an external memory package (stacking 32M-bit Flash ROM and 32M-bit PSRAM), the LSI enables baseband modem processing for W-CDMA mobile phones.

To extend talk time, talk current was reduced by means of (1) minimizing the hardware (to fit into one chip) by optimizing the algorithm and the required memory size for each function; (2) shortening the circuit operation time by thoroughly applying a clock gating technique to each circuit; and (3) decreasing the internal power voltage of the LSI (from 1.8V to 1.5V) by applying optimized semiconductor process. As a result, the operating current for baseband modem processing, which previously accounted for 35%-40% (200mA) of total talk current was reduced by 85%. The standby time was also extended with reduced standby current by means of (4) shortening the processing time by modifying the software for standby processing in communication control, which decreased 90% of the operating current that previously accounted for over 60%(7mA) of the total standby time; (5) reducing the leak current (to half) by partly turning on/off the internal power of the LSI; etc.


External memory (32M-bit Flash ROM + 32M-bit PSRAM)

Baseband modem LSI and external memory mounted on a mobile phone board

Baseband modem LSI

- 0.15*u*m low leak semiconductor process
- Chip size: 10.6mm x 10.6mm

Baseband modem LSI and external memory mounted on a mobile phone board

With 0.15 um low leak semiconductor process, an AFE, a CPU, two DSPs, and a hardware accelerator were integrated on a 10.6mm-square silicon chip. Then the chip was packed into a 15mm-square, 513-ball FBGA, and along with an external memory package (stacking 32M-bit Flash ROM and 32M-bit PSRAM), the LSI enables baseband modem processing for W-CDMA mobile phones.

[*] *Mobile Terminal Center*

1. Foreword

The third-generation W-CDMA mobile phone system has been providing commercial services since 2001, offering advanced features such as video phone and high speed packet communications that are more attractive than the services based on the second generation system. However, for this new system to become widely adopted, the continuous talk time and standby time had to be extended.

This article describes the low power baseband modem LSI developed as a solution to this need, starting with an overview of its basic structure and characteristics, followed by details of the low power technology.

2. Baseband Modem LSI

This baseband modem LSI applies 0.15um low leak semiconductor process technology to integrate an AFE, a CPU, two DSPs, and a hardware accelerator on a 10.6mm square silicon chip. Figure 1 shows its architecture. The internal power supply of this LSI consists of one part that is constantly set on (for the CPU, two DSPs, and AFE) and the other part that can be switched on/off for the hardware accelerator. The architecture of this hardware is similar to that of the baseband modem LSI chipset(1)(2) used for D2101V.

General functionality of the LSI is described below.

The AFE contains AD/DA converters, transmits /receives analog IQ signals, etc. to/from the RF block, and converts between analog and digital signals.

The CPU is a 32-bit RISC(M32R) that processes communication protocol every 10ms frame, and uses the external memory (32M-bit Flash ROM and 32M-bit PSRAM) as well.

Each of the two DSPs is a 16-bit DSP microcomputer (D10V) which controls the RF block, the hardware accelerator, and part of the digital signal processing for communications in cycles of 667 us.

The hardware accelerator is divided into the channel encoder, modulator, demodulator, and decoder as described in (1)-(4) below:

(1) Encoder

The encoder performs channel encoding and interleaving by executing convolutional/turbo encoding on the transmitted data, and outputs the results to the modulator as a transmitted bit sequence.

(2) Modulator

The modulator performs data mapping and spreading on the transmitted bit sequence to generate the chip sequence, and outputs the results to the AFE as transmitted digital IQ signal within a limited bandwidth of 5MHz.

(3) Demodulator

The searcher performs cell search and path timing detection for the received digital IQ signal input from the AFE. The finger performs RAKE receiving to execute despreading and pilot coherent detection on each of the detected delay paths, and outputs the obtained bit sequence to the decoder block.

(4) Decoder

The decoder performs channel decoding (error correction) through deinterleaving and Viterbi/Turbo decoding and obtains the received data.

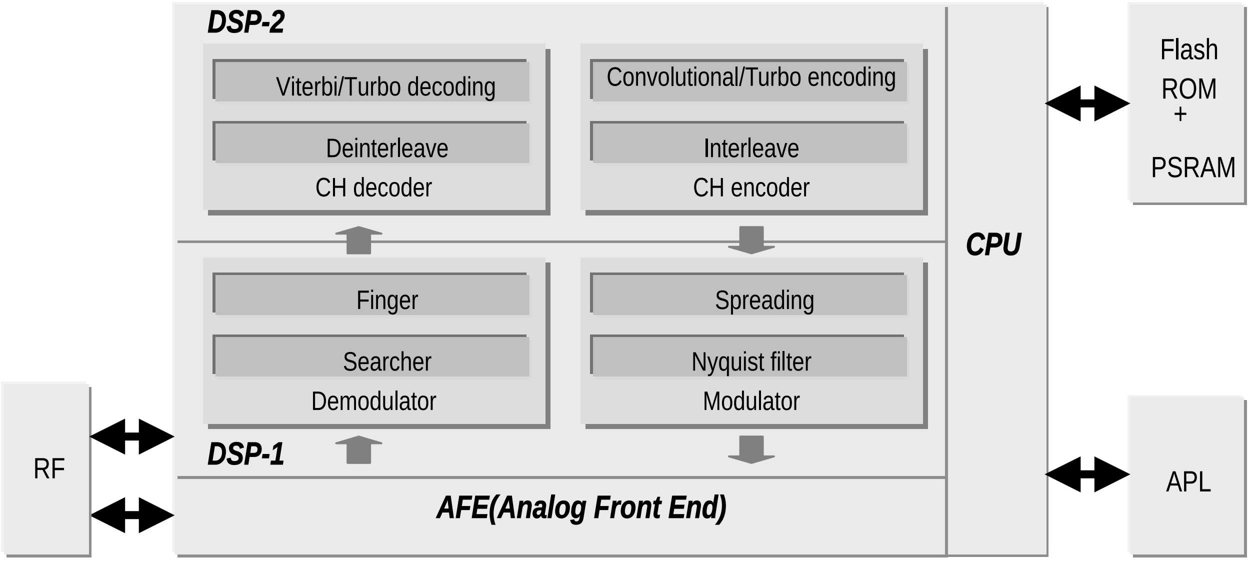


Fig. 1 Baseband modem LSI

A typical example is shown below to describe the characteristics of this LSI.

Figure 2 shows measurement results regarding the performance in the birth-death propagation condition at RMC12.2kbps (see 3GPP TS25.101 Annex B B.2.4). The required DPCH_Ec/Ior that satisfies BLER=1E-2 has secured a 3.4dB margin from 3GPP specification.

Generally speaking, securing such characteristics and lowering power consumption by reducing circuit volume are considered contradictory, but through efficient algorithm techniques and other factors, this LSI achieves a fair level of demodulator performance.

3. Low Power Technology

Table 1 shows the targets and achievements in extending talk time and standby time. Compared to the previous model (D2101V), the targets were set to two or three times longer for the talk time, and six to ten times longer for the standby time. The low power technologies applied to achieve these targets with reduced talk/standby current are described below.

3.1 Talk Current Reduction

This LSI contributes to reduce talk current mainly in terms of operating current (charge/discharge current for the internal circuit), which is calculated using the following formula.

Operating current(I)

~ Quantity of electric charge (Q) x Time(t)

~ Capacity(C) x Voltage(V) x Time(t)

The following (1)-(3) techniques were applied to reduce the operating current.

(1) Reduction of capacity(C)

Optimized the algorithm and required memory size for each function, and reduced the hardware volume to fit into one chip.

(2) Shortening of time(t)

Thoroughly applied clock gating technique to each circuit and reduced the circuit operation time.

(3) Reduction of voltage (V)

Applied the optimized semiconductor process, and reduced the internal power voltage from 1.8V to 1.5V.

As results of these techniques, the operating current for baseband modem processing, which previously accounted for about 35%-40%(200mA) of total talk, current was reduced by 85%.

Figure 3 shows the clock gating technique applied here. For example, the processor turns the operating clock on/off at function level (Signal A), and the block control sequencer of each function turns the operating clock on/off (Signal B) at block level, and the circuit sequencer of each block turns the operating clock on/off at circuit level (Signal C). Unlike the type of processor that shares and repeatedly uses a small number of computing units or registers, this type of hardware accelerator has various computing units operating in parallel, which enables hierarchical clock gating to effectively reduce the operating current.

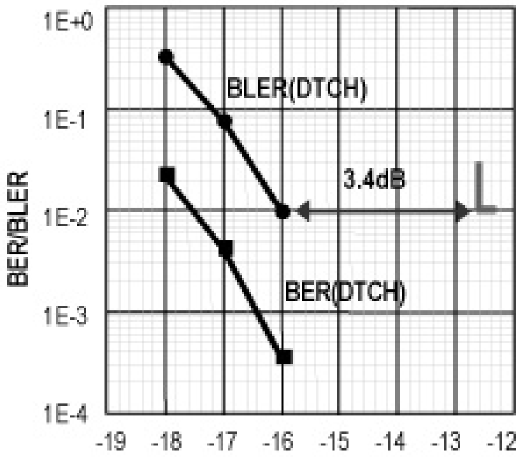


Fig. 2 RMC12.2kbps birth-death performance

Table 1 Targets and achievements of low power LSI

Item	Previously	Target	Results (D900i)
Talk time (voice)	60 min	x 2-3	170 min
Talk time (videophone)	50 min	(ditto)	90 min
Standby time	55 hrs	x 6-10	550 hrs (stationary) 420 hrs (moving)

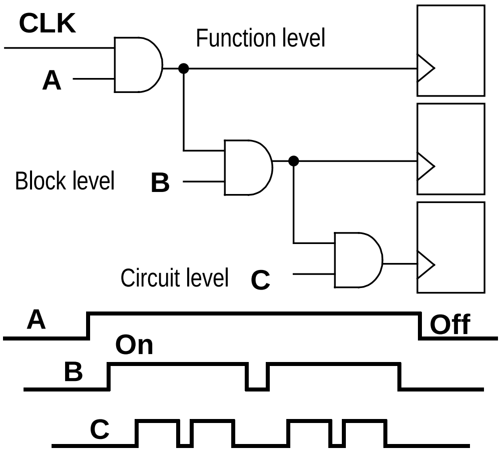


Fig. 3 Clock gating technique

3.2 Standby Current Reduction

Other than (1)-(3) in Section 3.1 Talk Current Reduction, the following (4)-(5) techniques were applied to reduce the standby current.

(4) Shortening of standby processing time

Modified the software to reduce standby processing time in communication control.

Figure 4 shows an example of observing such current profile during standby time (receiving PICH + acquiring SFN). The upper three signals indicate operating status of DSP-2, DSP-1 and the CPU respectively. (The DSP operates at L level; the CPU at H level.) The lower signal reflects current waveform. Each processor was activated when necessary. By shortening the processing time in this way, the operating current of communication control, which previously accounted for over 60%(7mA) of total standby current, was reduced by 90%.

(5) Reduction of leak current

Partly turned off the internal power of the LSI, which reduced the leak current by half.

About half of the chip area of this LSI is used for the hardware accelerator, and the power for this part of the chip is turned off while operation is not required during standby.

4. Conclusion

Mitsubishi Electric Corporation has developed a low power baseband modem LSI for W-CDMA mobile phones.

To extend talk time, talk current was reduced by means of (1) minimizing hardware (to fit into one chip) by optimizing the algorithm and the required memory size for each function; (2) shortening the circuit operation time by thoroughly applying a clock gating technique to each circuit; and (3) decreasing the internal power voltage of the LSI (from 1.8V to 1.5V) through optimizing the semiconductor process. Moreover, the standby time was extended with reduced standby current by means of (4) shortening the processing time by modifying the software for standby processing in communications control; (5) reducing the leak current by partly turning on/off the internal power of the LSI; etc. By applying such techniques to lower power consumption, the operating current for baseband modem processing, which previously accounted for about 35-40%(200mA) of talk current, was reduced by 85%. Also, the operating current for the communication control, which previously accounted for over 60% (7mA), was reduced by 90%.

Thus, D900i equipped with this LSI has attained a performance level of approx. 170/90 minutes for continuous talk and approx. 550/420 hours for continuous standby in stationary/moving states respectively.

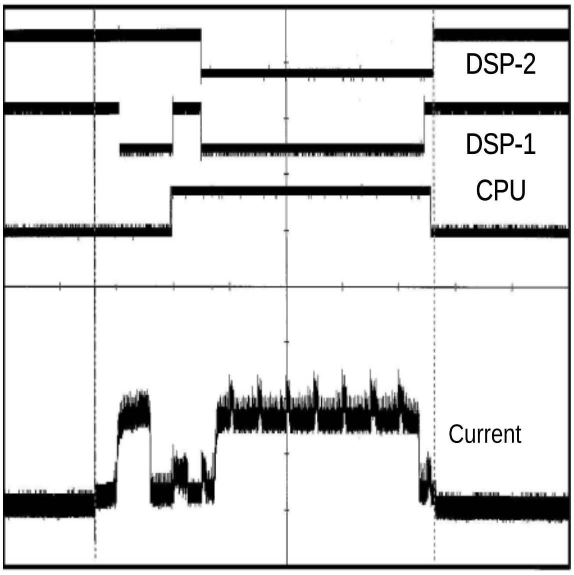


Fig. 4 Example of observed current profile

References

[1] Takahisa Aoyagi, Takahiko Nakamura, Yasuhiro Yano, and Kazuaki Ishioka: "Baseband modem technology for W-CDMA mobile phones", MITSUBISHIDENKIGIHO, Vol.77, No.2, 11(121) ~ 14(124) (2003)

[2] Toyohiko Yoshida, Masayuki Yamamoto, Takahiro Kanbara, and Ryosuke Takeuchi: "Baseband LSI for W-CDMA mobile phones", MITSUBISHIDENKIGIHO, Vol.77, No.2, 15(125) ~ 18(128) (2003)

Image Processing in Mobile Handsets

Authors: *Yoshihiko Hatano*[*] and *Shigeo Ando*[*]

Imaging functions in mobile handsets are widely accepted by a broad range of users, and rising demand for higher quality functions is on par with those for AV equipment. However, different from AV equipment, mobile handsets have two handset-specific features: (1) Restrictions need to be set on the performance of camera modules and LCD display devices (for miniaturization and low power operation), and (2) Two different modes need to be concurrently implemented: Storage Mode (for saving images in superfine quality), and Communication Mode (for effective and low-delay transmissions of images via transmission lines, such as for video-phones).

Image processing in mobile handsets can be broadly classified into four phases: Image-Capture, Encode, Decode/Playback, and Display. For the realization of a much higher image quality, various ideas have been proposed for each of these four phases.

In this paper, we introduce the following image processing technologies that have been implemented in Mitsubishi Electric's mobile handsets: [For the categories of Encode and Decode/Playback]: (1) Video Coding for various video sizes and image processing in Storage or Communication Mode, (2) JPEG File Size Control, for efficient compression of still images into transmittable sizes, (3) Synchronized AV Playback, [For the categories of Image-Capture and Display]: (4) Hand-Shake Detection, for decrease of hand-shake effects when capturing images with camera, (5) Tonal Control, for better visibility of the still images that are captured, and (6) NCM (Natural Color Matrix), for improvement of LCD color reproduction.

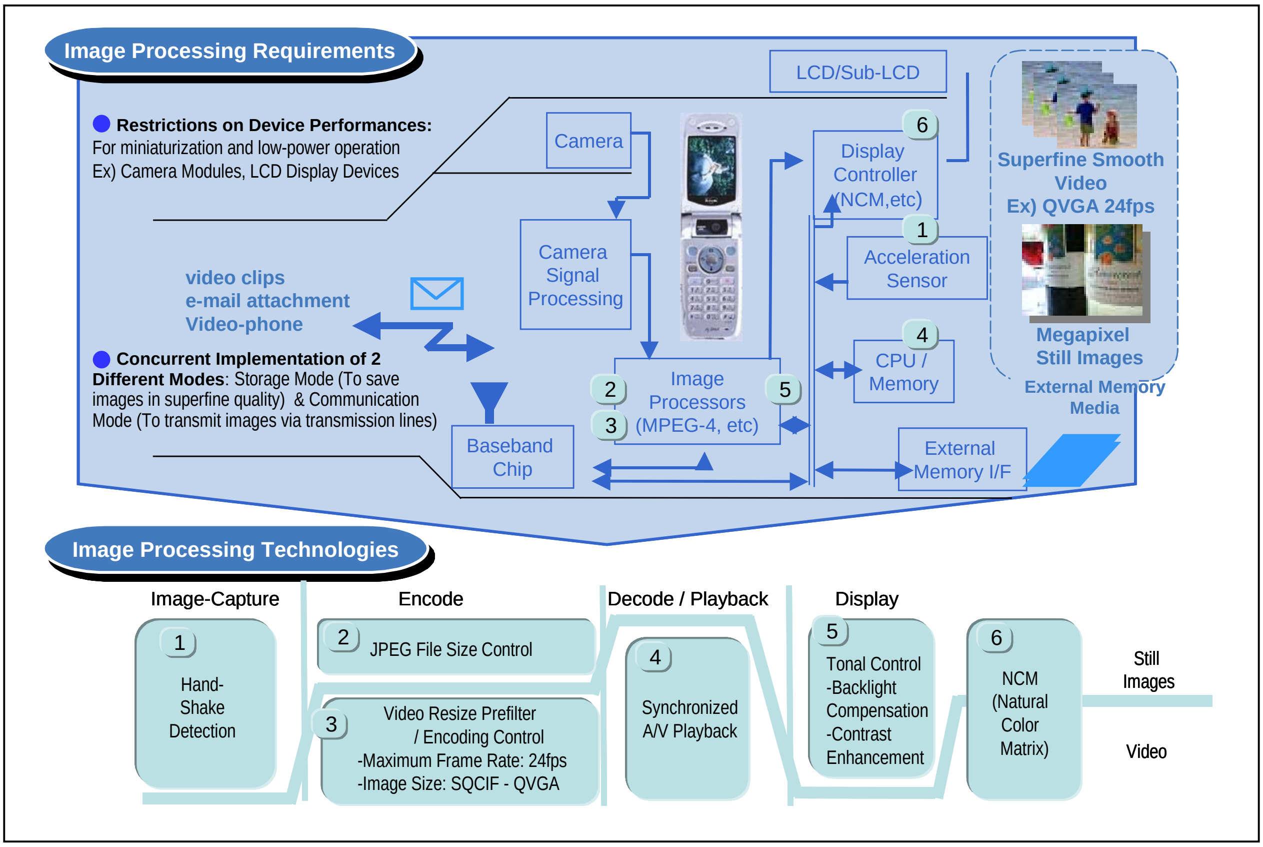


Image Processing Requirements
Restrictions on Device Performances:
For miniaturization and low-power operation
Ex) Camera Modules, LCD Display Devices
video clips
e-mail attachment
Video-phone
Concurrent Implementation of 2 Different Modes: Storage Mode (To save images in superfine quality) & Communication Mode (To transmit images via transmission lines)
LCD/Sub-LCD
Camera
Camera Signal Processing
Baseband Chip
Image Processors (MPEG-4, etc)
2
3
5
6
Display Controller (NCM,etc)
1
Acceleration Sensor
4
CPU / Memory
External Memory I/F
Superfine Smooth Video
Ex) QVGA 24fps
Megapixel Still Images
External Memory Media
Image Processing Technologies
Image-Capture
Encode
Decode / Playback
Display
1
Hand-Shake Detection
2
JPEG File Size Control
3
Video Resize Prefilter / Encoding Control
-Maximum Frame Rate: 24fps
-Image Size: SQCIF - QVGA
4
Synchronized A/V Playback
5
Tonal Control
-Backlight Compensation
-Contrast Enhancement
6
NCM (Natural Color Matrix)
Still Images
Video

"Image Processing Technology in Mobile Handsets", Summarized:

Mitsubishi Electric developed image processing technologies for the four image processing phases in mobile handsets (Image-Capture, Encode, Decode/Playback, and Display), and succeeded in realizing high-quality images. Features to be noted in particular, are: (1) Video-Capture, with the application of video coding technology that can simultaneously support several modes, (2) Display of tonally-controlled still images, (3) Display of NCM-processed video and still images.

[*] *Advanced Technology R&D Center*

1. Introduction

Demand for higher-quality image processing functions for mobile phones is increasing. Different from AV equipment, mobile handsets have two handset-specific features. First, the performance of camera modules and LCD display devices needs to be restricted for miniaturization and low power operation. Second, two different modes (Storage, for saving images of superfine quality, and Communication, for effectively transmitting images with low delays through transmission lines, such as for video-phones) need to be concurrently implemented. In order to realize image processing of higher quality in mobile handsets, technology that realizes these two features is indispensable.

2. Image Processing System Architecture in Mobile Handsets

Figure1 shows the architecture of a mobile handset's image processing system. Image processing in handsets can be broadly classified into four phases: Image-Capture, Encode, Decode/Playback and Display. In the first phase, Image-Capture, the built-in camera captures an image. In the second phase, Encode, the image processor codes the captured image. (The coding algorithms used are JPEG for still images, and MPEG-4 for video). The data of the coded image is either (1) saved in nonvolatile memory such as external memory (Storage Mode), or (2) transmitted via transmission lines (Communication Mode). In Storage Mode, data of high quality can be handled, since restriction on the amount of data is less strict compared to Communication Mode. In contrast, restriction on the amount of data is strict in Communication Mode, and for video-phones, low delays are required. In the third phase, Decode/Playback, the coded and saved data are decoded and played back, and in the fourth phase, Display, the decoded and played back images are finally displayed on the LCD.

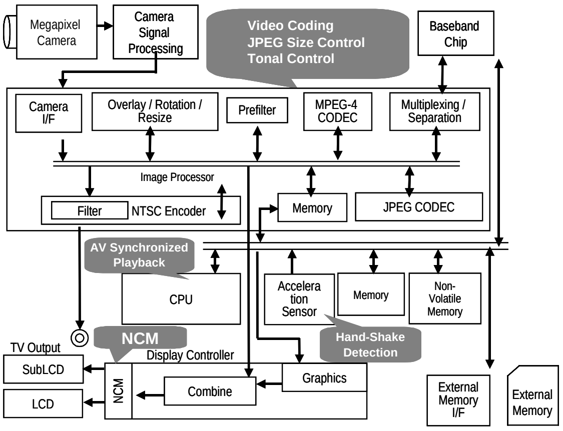


Fig. 1 System Architecture

3. Concurrent Implementation of Communication and Storage Technologies

3.1 Video Coding

In video coding, the MPEG-4 encoder's parameter settings and its encoding control unit greatly affect image quality. (For example, Table 1 shows the MPEG-4 encoder parameters that were implemented in 3G mobile handsets.) The MPEG-4 encoder has eleven different modes for coding, classified according to image size, bit rate, and selection of Storage or Communication Mode.

First, how coding is controlled differs significantly depending on the selected mode (Storage or Communication). That is, in Communication Mode, quantization is controlled so that the amount of code to be generated is kept constant for each frame. This is in order to reduce delays caused by buffers. Also, bit allocation for coding is determined based on the amount of stream data that are read from the buffer. This is in order to adjust the amount of code to be generated in accordance with the actual communication rate. On the other hand, in Storage Mode, delays are no problem, and to produce high-quality images, bits are dynamically allocated in accordance with the total amount of code to be generated.

Also, in Communication Mode, the user is able to select from the following modes for video quality: "Smoothest Motion", "Normal", and "Sharpest Image". If "Sharpest Image" is selected, the frame rate is lowered, and in cases when quantization becomes coarse, coding is controlled so that frames are skipped (a control pattern specific to the "Sharpest Image" mode). In contrast, if "Smoothest Motion" is selected, coding is controlled to reduce frame-skipping (a control pattern specific to the "Smoothest Motion" mode).

Furthermore, as shown in Fig.2, the MPEG-4 encoder consists of an encoding control unit whose operation is linked with a prefilter unit. This prefilter filters the input image through temporal and spatial filters, and

Table 1 MPEG-4 Encoder Parameter Settings

Mode		Image Size	Bit Rate (kbit/s)	Maximum Frame Rate (1/sec)	Encoding Control
Communication Mode	64k	QCIF	60	15	Smoothest Motion
				7.5	Normal
				5	Sharpest Image
	32k	QCIF	30	15	Smoothest Motion
				7.5	Normal
				5	Sharpest Image
Storage Mode	Standard	QCIF	32	10	Smoothest Motion
	Small/Fine	SubQCIF	64	15	Smoothest Motion
	Fine	QCIF	64	15	Sharpest Image
	Ultra-Smooth	QCIF	256	24	Smoothest Motion
	Widescreen	QVGA	384	15	Smoothest Motion

also calculates the signal difference in the each pixcel between the current frame and the previous frame. The image output from the prefilter moves onto the encoder unit. On the other hand, the encoding control unit decides whether to perform or skip the coding process for the current frame, depending on the prefilter-calculated signal difference, buffer occupancy, and the amount of data of past coding. In case coding is to be performed, parameters for quantization are set. The encoding control unit also calculates the filter coefficient for the next frame, and sets this value to the prefilter.

As described above, the prefilter unit has a variable characteristic due to its connection to the encoding control unit. Therefore, if the amount of code to be generated needs to be small, a parameter is set for a coarser quantization, and the bandwidth for spatial filtering is restricted so that block distortions are suppressed. In contrast, if the amount of code needs to be increased, bandwidth restriction is eased and image resolution is saved. Also, by calculating bit difference between the previous frame and the current frame, optimal bit allocation and quantization control are performed, enabling fine-quality images.

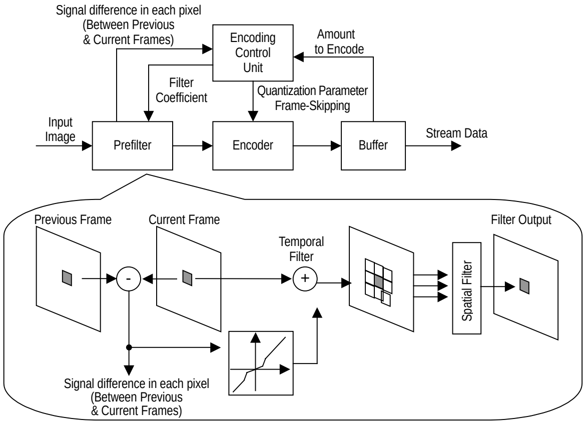

Signal difference in each pixel (Between Previous & Current Frames)
Encoding Control Unit
Amount to Encode
Filter Coefficient
Quantization Parameter Frame-Skipping
Input Image
Prefilter
Encoder
Buffer
Stream Data
Previous Frame
Current Frame
Temporal Filter
Filter Output
Spatial Filter
Signal difference in each pixel (Between Previous & Current Frames)

Fig.2 MPEG-4 Encoder Configuration

3.2 JPEG File Size Control

When handling still images in Communication Mode (that is, when sending e-mails with images attached), a mechanism to obtain a JPEG image of a file size nearest to the transmission line capacity is necessary, in order to send an image of the finest possible quality. For this purpose, file size is controllable by modifying the values of the quantization table used for compression. To explain in detail, the relation between file size and quantization table values (more specifically: multiplier coefficients that are multiplied to the values of the standard quantization table) can be reflected in a simple equation that includes two constants. Therefore, if these two constants are found, the multiplier coefficients required to obtain the JPEG image of the target file size can also be found. As shown in Fig. 3, a method has been developed to find these two constants by calculating the differences among pixel values from a number of different areas on a precompressed image. By this method, file size can be controlled within the standard 5% deviation from the target file size.

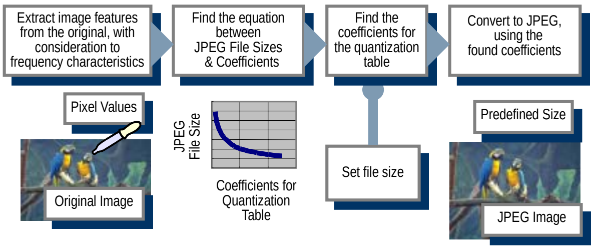

Extract image features from the original, with consideration to frequency characteristics
Find the equation between JPEG File Sizes & Coefficients
Find the coefficients for the quantization table
Convert to JPEG, using the found coefficients
Pixel Values
Original Image
JPEG File Size
Coefficients for Quantization Table
Set file size
Predefined Size
JPEG Image

Fig.3 Flow of JPEG File Size Control

3.3 Synchronized A/V Playback

High-quality video saved in Storage Mode needs to be played by maintaining Audio-Video synchronization in strict accordance with the timing recorded at the time of video-capture. The timing for video output can be controlled based on how the audio output is progressing. Figure 4 shows how the CPU directly controls the timing to display the decoded video images. This method has two characteristics: First, the CPU directly controls the timing to display video images, thus significantly reducing display timing fluctuations, usually caused by decoding time fluctuations. Second, since the display timing becomes the controlling factor, special playback functions (such as fast-forward and frame-advance) become possible without requiring any special instructions to the image processor.

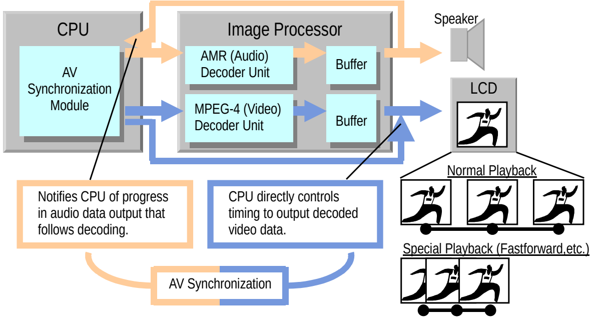

CPU
AV Synchronization Module
Image Processor
AMR (Audio) Decoder Unit
MPEG-4 (Video) Decoder Unit
Buffer
Buffer
Speaker
LCD
Normal Playback
Special Playback (Fastforward,etc.)
Notifies CPU of progress in audio data output that follows decoding.
CPU directly controls timing to output decoded video data.
AV Synchronization

Fig.4 Synchronized A/V Playback

4.Image Correction Technologies

4.1 Hand-Shake Detection

Recently, cameras with higher resolutions have been installed in mobile handsets. However, this is causing a decrease in camera sensitivity, due to restrictions in the image sensor and the lens size. Therefore, indoor images under low-light conditions are captured with even slower shutter speeds, most likely resulting in an image blurred due to hand-shake. Also, since most users hold the handset one-handedly when taking pictures, the built-in camera is likely to shake the moment the user presses the shutter button thus blurring the captured image. To solve this problem, Mitsubishi Electric developed a mode called the "Shake Detection Mode". When in this mode, the built-in camera detects if there is any shaking caused at the moment that the shutter button is pressed. A blurred picture can be prevented even if shaking is detected, since the camera is programmed to capture that certain image after it senses stabilization. By using this "Shake Detection Mode", the start and the settling down of shakes can be sensed and detected on the handset, since it is programmed to sense and detect sudden changes in the acceleration sensor output as the shake begins, and the changes that follow afterwards in periodic intervals.

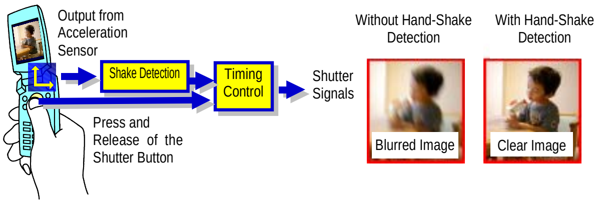

Output from Acceleration Sensor
Shake Detection
Timing Control
Shutter Signals
Press and Release of the Shutter Button
Without Hand-Shake Detection
With Hand-Shake Detection
Blurred Image
Clear Image

Fig.5 Hand-Shake Detection

4.2 Tonal Control

For the latest expensive flat-panel televisions, implementation of tonal control technology (that improves tonal gradation by histogram equalization) is starting to spread for better visibility. For mobile handsets, a method more dynamic than the one implemented for television is necessary, since it is more important to improve the visibility due to the restrictions set on LCD display devices (to lower power consumption), such as lack of contrast in the LCD screen when seen outdoors, and frequent occurrences of whiteout and blackout effects when capturing backlit images.

This time, in order to solve these problems, Mitsubishi Electric developed a tonal control technology (as shown in Fig.6) that conducts tonal conversion, in which, first, the image is analyzed, and then, tonal conversion is carried out (mapping curves are dynamically and successively created within the display screen). By implementing this technology, the following effects can be achieved:

(1) Contrast Enhancement

The effects of contrast enhancement surpass those achieved by the usual on-screen tonal histogram equalization method. Most particularly, visibility is improved for images seen on the display screen when outdoors, despite the lack of contrast

(2) Backlight Compensation

Backlight compensation improves visibility for both dark and light parts of images captured in backlit conditions. Image quality can be improved without the usual lack of tonality at middle range. (See Fig.7) Also, since scene analysis enables smooth and automatic switchovers between contrast enhancement and backlight compensation functions, backlight compensation can be applied to images fairly easily.

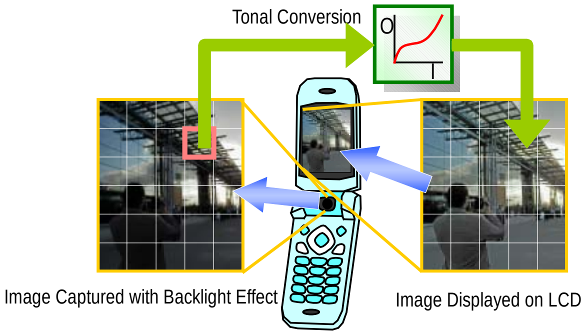


Fig.6 Tonal Control

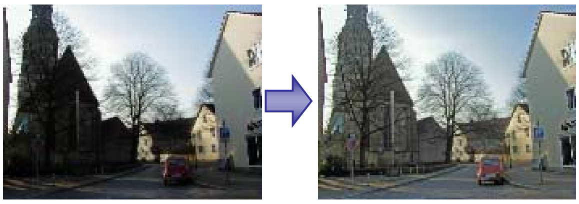


Fig.7 Example of Backlight Compensation
(Left: Before Compensation, Right: After Compensation)

4.3 NCM (Natural Color Matrix)

Color reproduction is one of the elements that determine onscreen image quality. For images to have excellent color reproduction, not only wide color space, but also appropriate color allocation is critical. In most cases, color reproduction quality of images displayed on mobile handsets is inferior (compared to those displayed on LCD television, for example), since their display device performances are restricted for low power operations. However, appropriate color allocation by the way of signal processing realizes color reproduction that is sufficient for perception by the human eye.

The "Natural Color Matrix (NCM)" color conversion technology that Mitsubishi Electric developed and implemented, is a newly-developed method based on matrix calculation, and does not require a large amount of memory in contrast to the 3D-LUT (3 Dimensional Look-Up Table) method, commonly used for printers. Therefore, from the aspect of circuit complexity, the NCM method can be easily implemented in hardware. Thus, being hardware-based, this method is suitable for and applicable to displays, whose typical requirements are to show video images and to provide real-time processing

In NCM technology, matrix calculation is conducted with the achromatic component data and the chromatic component data (this data is further converted into "hue region data" and "inter-hue region data") as the calculated elements (See Fig.8). The "hue region data" consists of six colors, RGB (the primary colors of Red, Green, and Blue) plus Cyan, Magenta, and Yellow, and the "inter-hue region data" consists of 6 colors, each coming in-between two adjacent "hue region" colors. By conducting matrix calculation, all these colors can be adjusted independently of one another, enabling smooth color reproduction (hue, saturation, and intensity). That is, a number of memory colors with different hues can each be independently adjusted for color reproduction. For example, a lawn's green color and skin color can each be independently adjusted to improve color reproduction, while having no degrading effect on the other colors.

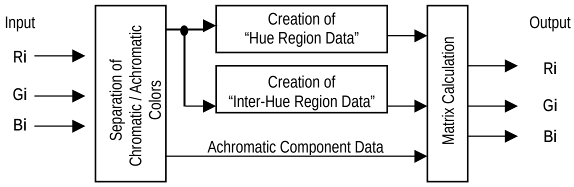

Input
Ri
Gi
Bi
Separation of Chromatic / Achromatic Colors
Creation of "Hue Region Data"
Creation of "Inter-Hue Region Data"
Achromatic Component Data
Matrix Calculation
Output
Ri
Gi
Bi

Fig.8 NCM Configuration

Based on the above findings, NCM is a versatile technology that flexibly enables color conversions of various combinations. With the implementation of this technology, colors can always be allocated in the most appropriate manner, in accordance with the characteristics of the display device that is used. Display devices for mobile handsets are no exception, and images of excellent color reproduction are produced onscreen.

5.Conclusion

Demand will continue to rise for mobile handsets with enhanced imaging functions, such as those of higher resolution cameras, higher definition displays, and mobile digital televisions. As mentioned above, for imaging functions to evolve within limits specific to handsets, image processing technologies that support the performance of these functions will become increasingly important.

References

(1) Sugiura H., et al: Development of New Color Conversion System, Proceedings of SPIE, 4300, 278~289 (2001)

(2) Hatano Yoshiko, et al: W-CDMA Mobile's Imaging Technology, Mitsubishi Electric Technical Report, Vol. 77, No. 2, 2003, 36~39

(3) Ono Yoshiki, et al: A Study of Image Tone Curve Optimization for Mobile Phones, The 2004 ITE Winter Annual Convention.

(4) Shinohara Junko, et al: Development of Scene Change Detection for the MPEG-4 Video Encoder, The 2004 ITE Winter Annual Convention.

Technologies for Image Applications on Mobile Phone

Authors: *Tomohiro Kimura*[*] and *Kohtaro Asai*[*]

In recent years, the liquid crystal display (LCD) and camera for mobile phones have gradually improved with higher resolutions and better display colors. Using mobile phones, we can now enjoy high quality images.

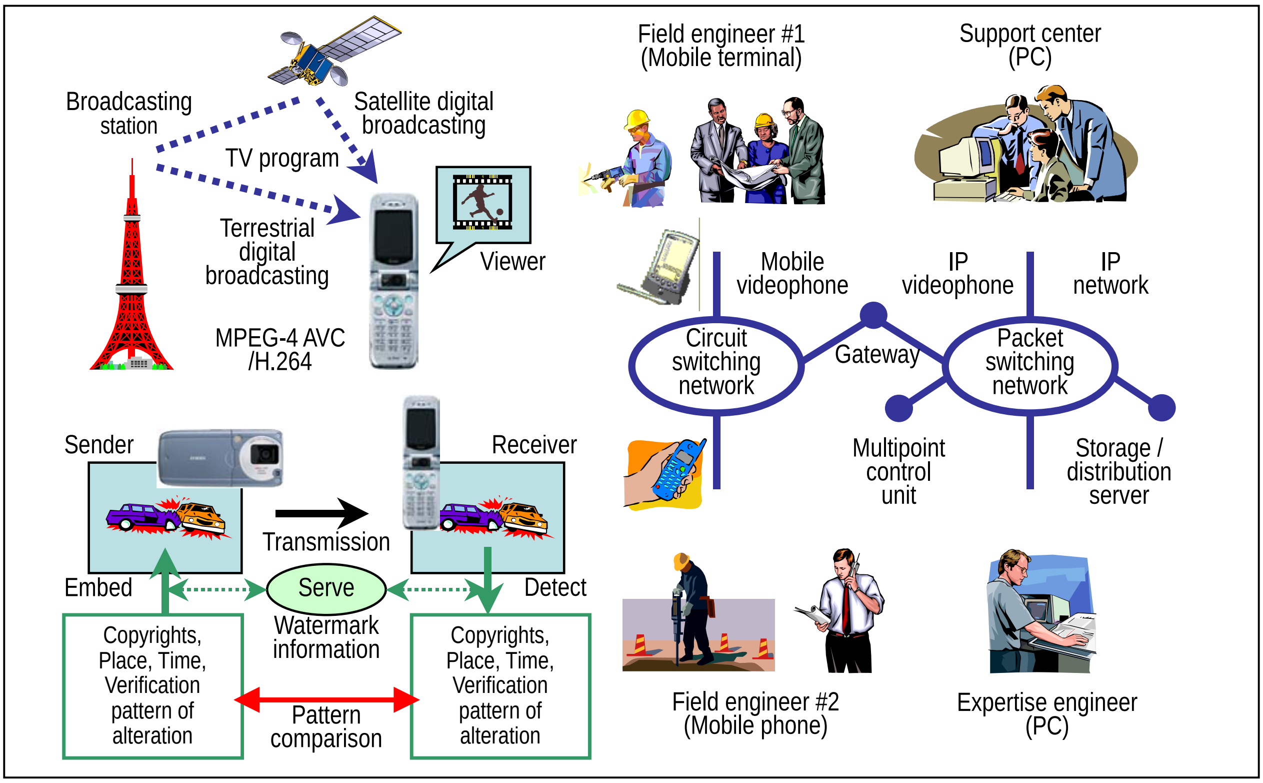
This paper describes the technologies for mobile terminal-oriented broadcasting, digital watermarking and multipoint visual communication with the summaries of expected image services.

In the chapter on broadcasting technology for mobile terminals, we introduce the circumstances and summarize the standardization for an MPEG-4 AVC/H.264 video coding system. This system was adopted for one segment broadcast, which was expected as the terrestrial digital broadcasting service for mobile terminals.

In the chapter on digital watermarking technology for mobile phones, we present the application and service of watermarking, which embeds auxiliary information into images obtained via the Internet or the digital camera functions of mobile phones. In addition, we describe the future prospect of watermarking application to mobile phones.

In the chapter on multipoint visual communication technology, we present new services such as interconnecting third generation mobile videophones (using circuit-switching network) and IP videophones (using packet-switching network), remote operating support and video storage / distribution. We also describe the trends for the future image communication.

MPEG: Moving Picture Experts Group,
AVC: Advanced Video Coding
IP: Internet Protocol


Broadcasting station
TV program
Satellite digital broadcasting
Terrestrial digital broadcasting
MPEG-4 AVC /H.264
Viewer
Field engineer #1 (Mobile terminal)
Support center (PC)
Mobile videophone
IP videophone
IP network
Circuit switching network
Gateway
Packet switching network
Multipoint control unit
Storage / distribution server
Sender
Receiver
Transmission
Embed
Serve
Detect
Watermark information
Copyrights, Place, Time, Verification pattern of alteration
Pattern comparison
Copyrights, Place, Time, Verification pattern of alteration
Field engineer #2 (Mobile phone)
Expertise engineer (PC)

Overview of image application technologies on mobile phone

Terrestrial digital broadcasting and satellite digital voice broadcasting are expected to begin soon by adopting an MPEG-4 AVC/H.264 video coding system. Also, watermarking services are expected so that auxiliary information can be embedded into photographic images on mobile phones and extracted from them when required. Furthermore, the connection between different types of phones (mobile video phones/IP video phones) and the linking of multipoint video communications are achieved, leading to service diversification such as remote operating support to increase the efficiency of field work.

[*] *Information Technology R&D Center*

1. Preface

Almost all mobile phones have a high-quality LCD and a high-resolution camera, which support Internet functions and camera functions.

Regarding video applications, a broadcast service for mobile terminals has been launched with the video-phone service to connect multi points. In addition, a service to apply watermarking to the image has also begun for still-images.

This paper outlines these techniques and related services.

2. Broadcast technology for mobile terminals

In Japan, the broadcast service for mobile terminals and portable devices started in 2004. The service "Mobile broadcasting", 2.6GHz belt satellite digital broadcasting was launched on October 20, 2004, using MPEG-4 SP (Simple Profile). Furthermore, the Association of Radio Industries and Businesses (ARIB) is working to standardize the video working system for 1-segment television broadcasting and 3-segment radio broadcasting, which are the services for digital terrestrial broadcasting. Currently, ARIB examines two video coding systems; one is MPEG-4 SP already used as a TV phone system for mobile phones and the other is a new video coding system BP (Baseline Profile) of MPEG-4 AVC/H.264 (referred to as AVC hereafter). This chapter describes the AVC method.

2.1 Standardization efforts for AVC

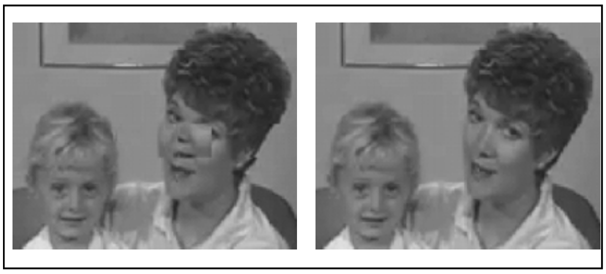
In 2003, the standards known as 14496-10 (MPEG-4 Advanced Video Coding) and H.264 were established through the efforts of JVT (Joint Video Team). JVT was a joint project of ITU-T subgroup VCEG (Video Coding Experts Group) and ISO/IEC subgroup MPEG (Moving Picture Experts Group). The standardization efforts for AVC were undertaken to acquire coding efficiency higher than the existing video coding methods such as MPEG-2 and MPEG-4.

2.2 Outline of the AVC system

The coding system currently discussed by ARIB is a subset of AVC, specified as the "Baseline Profile" and is equal to or less than "1.2 Level". This profile and level restrict coding parameters and tools. In the case of using QVGA (320x240) resolution video, 15 or lower frame rates and 384k or lower bit rates are permitted for broadcasting. Also, ARIB restricts some complicated coding tools whose effects are minor in broadcasting use.

Since AVC has developed aiming initially at low resolution and low bit rates, its coding performance for QVGA pictures at around 200 kbit / sec bit rate is relatively better resulting in less coding artifacts. On the other hand, AVC decoding needs about three times the processing compared with the conventional system. This is difficult for systems such as mobile terminals requiring lower power consumption.

We have been further improving our algorithm of error robustness and efficient implementation [(1)], based upon our results in the past development of MPEG-2 for digital broadcasting and high-rate surveillance, in addition to MPEG-4 for mobile terminals and low-rate surveillance.



(a) Without robustness (b) Enhanced robustness

Fig.1 Example of effect in AVC/H.264 error robustness

3. Watermarking technology for mobile phones

Digital watermarking is a technology that invisibly embeds information into images and detects the information when required. The image after embedding watermark information keeps the original format, so the watermarked image can be displayed on a general viewer without extracting embedded information from the image.

3.1 Service using the Internet functions

In the service form that uses the Internet functions of mobile phones, the pre-embedded watermark information in the images on web sites or images attached to E-mails can be detected.

(1) Detection of copyrights information [(2)]

Watermarking embeds copyright information into images, serving as a means to warn whether the images are being used illegally. This technology cannot prevent illegal use, but a psychological effect that suppresses such use is expected.

(2) Detection of information for alteration detection [(3)]

Surveillance images are required to be highly authentic. As a means to prove authenticity, it is effective to embed watermark information into images for alteration detection. For safety measures, it is desirable to photograph images and to embed watermark information simultaneously before any alteration is added externally.

3.2 Service using the camera functions

The latest mobile phones have a digital camera with the high resolution of 1 million to 3 million pixels. In the service form that uses the camera functions of a mobile phone, watermarking embeds or detects the metadata information in camera images.

(1) Embedding into the photography image

Two types of watermark information can be embedded into the images photographed by the camera functions of a mobile phone. One is automatic photography information, such as the place, date, time and fixed data. These can be embedded simultaneously when taking an image. The other is unformed information embedded after taking an image.

(2) Detection from the photographed image on the printed paper or the display screen

By using the camera function of a mobile phone, the images on the printed paper or the display screen can be photographed after watermark information is embedded. The pre-embedded information can be detected from its photography image.

3.3 Service form through the watermarking server

In the stage of initial watermarking application, the service form in which the server positioned as Fig.2 is suitable. This form does not require embedding watermark information into images but detects the information on existing mobile phones only with low throughput.

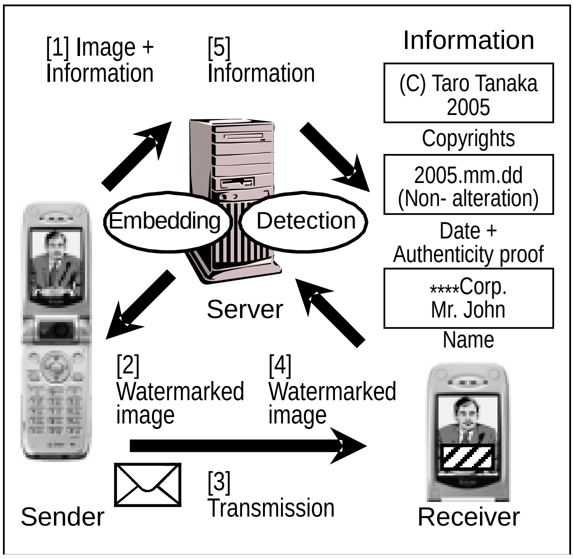


Fig.2 Example of watermarking service through server

4. Multi-point visual communication technology

We describe the deployment of the technology and application of the visual communication service for mobile terminals, such as videophone service for 3rd generation mobile phones (mobile videophones).

4.1 Visual communication using mobile phone

(1) Call between different-types of videophones

Visual communications between mobile videophone terminals over the circuit switching network are based on the 3G-324M standard established by the 3GPP. Visual communications between IP videophone terminals on the packet switching network, such as the Internet, are based on the SIP standard etc. established by the IETF. In order to intercommunicate between the different types of videophone terminals, a 3G-324M/IP gateway is needed to convert every protocol required per standard, such as a call control procedure, media coding method and transmission format. We have made a gateway prototype and plan verify the overall techniques, including error robustness against transmission errors with mobile phones and packet jitter absorption typical of the IP communication.

(2) Call between multiple videophones

When communicating among multiple points with IP videophone terminal, a mesh-shaped communication can be established on the IP network between each terminal and the services are provided on the application layer. However, with a mobile videophone terminal, a single communication to another terminal can be established over the circuit switching system, so it is necessary to build a dedicated system using the MCU (multi-point control unit) (4). While establishing a one-to-one communication with multiple videophone terminals, MCU performs media processing such as video mixing, video switching and/or audio mixing functions to share video and voice from a terminal with other terminals.

(3) Storage and distribution of video contents

Video contents pre-registered in the storage server are distributed to mobile videophone terminals by the service already available. In order to research multimedia stream processing technology, we made a prototype of the storage / distribution server that stores and redistributes multimedia streams from mobile videophone terminals. Furthermore, we built a model system in which mobile videophones and IP videophones are linked with the said 3G-324M/IP gateway, MCU and storage / distribution servers so that comprehensive technical verification and service verification be conducted for future communication services.

4.2 Application of multi-point visual communication

An increasing number of mobile videophones and IP videophones are being used at offices, homes, etc. The usage example applied in future communications services is shown in Fig.3.

(1) Field work support

When a field engineer who performs maintenance or repairs at a customer's premise works on site, operation support may be necessary from remote places, such as a support center. Previously, problems were explained by voice using a mobile phone. Currently you can easily explain situations using images with a videophone. Depending on the problem, you can also consult with experts by multi-point visual communication.

(2) Video storage / distribution service

Applications such as condition reports and video messages are achieved because the storage server stores and distributes the video contents from mobile videophone terminals. Furthermore, remote operation support can be deployed to obtain support from experts while using video manually by linking with more places.

4.3 Future multi-point visual communication

The progress in mobile phones is remarkable and visual communication by mobile terminal has become a standard service. At the same time, the trend in the broadband and IP communication has affected mobile phones. Various visual communication services are being realized with terminals, such as IP videophones at offices or homes and outdoor mobile videophones, exceeding the differences in the network or terminal environments. From now on, spatial and time diversification in visual communication will progress further by fusing with contents storage / distribution, etc.

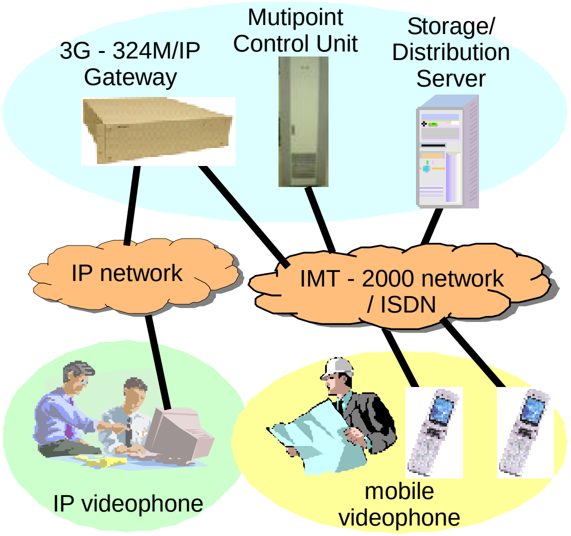


Fig.3 Example of multi-point visual communication

5. Conclusion

This paper described important component technologies that utilize images from mobile phone terminals equipped with an LCD and a camera. New services are expected along with the employment of the latest technologies; AVC/H.264 video coding, watermarking and multi-point visual communication are used on mobile phones.

Establishing the employment model of images is important. It is not easy to realize the requirements of the diversifying image services, but we will continue to propose new services and their commercialization for mobile phones.

References

(1) S. Sekiguchi, et al., "Evaluation of error robustness in AVC/H.264 video stream syntax," PCSJ, P-5.14, November, 2004

(2) M. Wada, et al., "Use of digital watermarking in distributing images as live programs," ITE Annual Convention, 11-7, August, 2004

(3) H. Ito, et al., "Watermarking scheme for JPEG-compressed image authentication," IEICE General Conference, D-11-33, March, 2003

(4) M. Sakai, et al., "Mobile Visual Communication System," Mitsubishi Electric R&D, Vol.78, No.2, pp.23-26, February, 2004

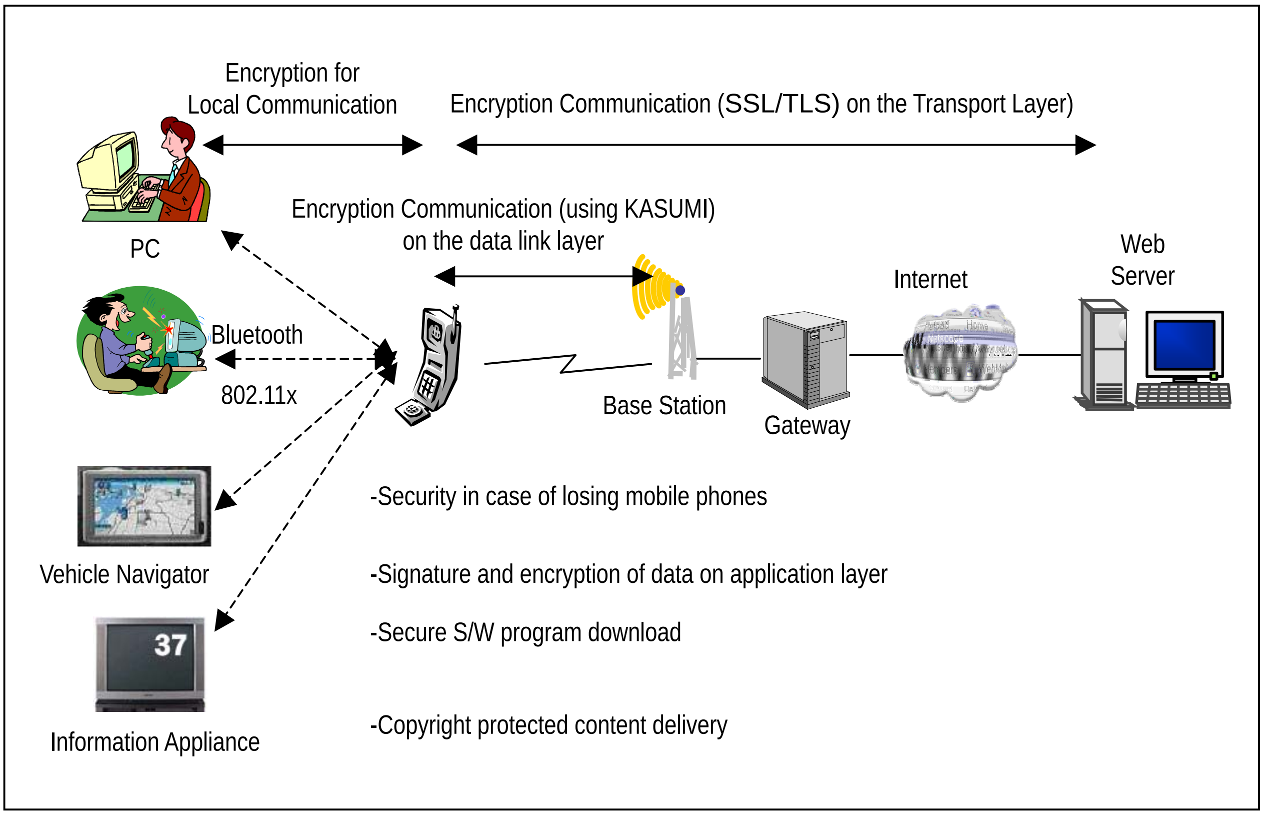
Information Security Technologies for Mobile Phones (User Authentication and Information Protection for Mobile Phones)

Authors: *Takeshi Yoneda*[*]

Mobile phones became widely spread as a tool to facilitate voice communication, and within a few years offered Internet browser and e-mail services. Now mobile phones can be used as digital camera, TV, radio, and music player.

As mobile phone technologies evolved, the need for security expanded from wireless and internet communication to application layer security.

In this paper, KASUMI and SSL (Secure Socket Layer) client authentication are described as mobile phone communication security. KASUMI is used for protecting wireless communication while SSL client authentication is used for internet communication whose implementation feasibility has been proven by Melco for the first time. Below, examples of application layer security are described whose implementation feasibility has been confirmed by Melco prototype.


Encryption for Local Communication
Encryption Communication (SSL/TLS) on the Transport Layer)
PC
Encryption Communication (using KASUMI) on the data link layer
Bluetooth
802.11x
Base Station
Gateway
Internet
Web Server
Vehicle Navigator
Information Appliance
37
-Security in case of losing mobile phones
-Signature and encryption of data on application layer
-Secure S/W program download
-Copyright protected content delivery

Security technologies for mobile phones are classified as communication security and application layer security.

The communication security includes the security of data link communication, TCP level end-to-end communication and communication between a mobile phone and a device in the near field.

The application layer security includes the security for preventing misuse of lost mobile phones, for preventing repudiation, for ensuring authenticity of downloaded S/W programs and for delivering copyrighted content.

[*] *Information Technology R&D Center*

1. Communication Security

1.1 Encryption communication between a mobile phone and a base station

Wireless communication between a mobile phone and a base station is easily intercepted. To prevent such radio interception, encryption technology is indispensable. Furthermore, two-way authentication should be applied to mobile phones and base stations to prevent masquerading. So KASUMI, based on MISTY is now used as the encryption algorithm for W-CDMA in order to provide a solution to the security threats.

1.1.1 KASUMI

KASUMI is MISTY-based symmetric key encryption algorithm customized for mobile phones so that low power consumption as well as security can be achieved.

KASUMI was initially designed by SAGE(Security Algorithms Group of Experts) of ETSI (European Telecommunications Standards Institute), in response to a request from 3GPP (The 3rd Generation Partnership Project). It was jointly completed by Melco. The name of "KASUMI" is a Japanese translation of MISTY. KASUMI proved its security strength against strong: linear cryptanalysis and is highly esteemed for its durability for 10 years.

1.1.2 Encryption and authentication communication between a mobile phone and a base station

Figure 1 shows an overview of encryption and authentication communication between a mobile phone and a base station specified by 3GPP, where KASUMI is used.

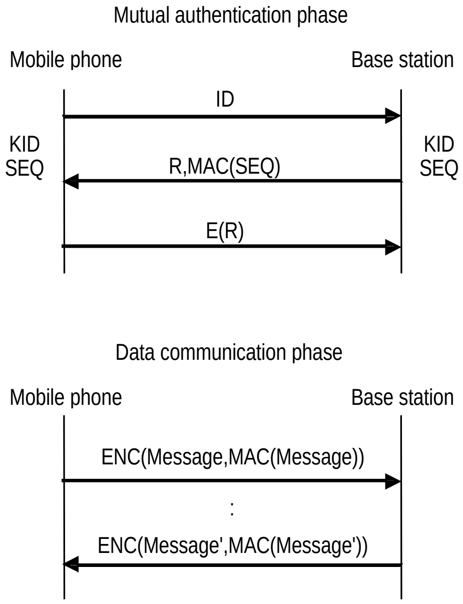


Fig.1 Encryption and authentication communication

A mobile phone and a base station share Key (KID) and sequence number (SEQ). SEQ is incremented whenever mutual authentication occurs. Encryption and authentication communication consist of two phases: a mutual authentication phase and a data communication phase.

In the mutual authentication phase, a mobile phone notifies its ID to a base station. The base station identifies the KID and SEQ of the mobile phone from the ID. It sends random number (R) and MAC (Message Authentication Code) of SEQ by KID to the mobile phone.

The mobile phone generates the MAC of retained SEQ by KID and compares it with received MAC. If they match, the mobile phone authenticates the base station. Next, the mobile phone encrypts R by KID and sends encrypted E (R) to the base station. The base station encrypts sent R by KID and compares it with received E (R). If they match, the base station authenticates the mobile phone. At this stage, mutual authentication is completed. Then the next data communication phase begins.

In the data communication phase, MAC is concatenated with data. Then they are encrypted and sent to the receiver.

The receiver, verifies the decrypted data to check that no wiretapping, interception have taken place, and confirms whether the sender is legitimate. In this respect, KASUMI is applied to various areas of MAC generation, verification, data encryption and decryption at communication phase.

1.2 Encryption and authentication communication between a mobile phone and a server on the internet

With the advent of i-mode, the internet browser became a basic function of mobile phones. When communication occurs between a mobile phone and a server on the internet, the communication path consists of two parts. 1) a mobile phone and the core network, 2) the core network and a web server on the internet.

The communication in the first part is protected by KASUMI. However, the communication in the second part, which uses the internet, is unprotected. Unless appropriate security measures are taken for the second part, eavesdropping, altering and masquerading may occur. To protect the second part of the communication, encryption and authentication communication protocol: SSL (Secure Socket Layer) between a mobile phone and a server was introduced.

1.2.1 SSL

The SSL is a secure communication protocol developed by Netscape Communications Corporation. The protocol supports server authentication and client authentication.

In server authentication, a client (a mobile phone) authenticates a server but the server does not authenticate the client. In the client authentication, a client and a server mutually authenticate each other. To authenticate the client, the client needs certificate and functions to generate a digital signature. The digital signature function and certificate storage function are implemented in the FOMA UIM Card that is embedded in NTT DoCoMo FOMA phones.

1.2.2 SSL handshake protocol

As shown in Fig.2, SSL handshake protocol consists of the following steps.

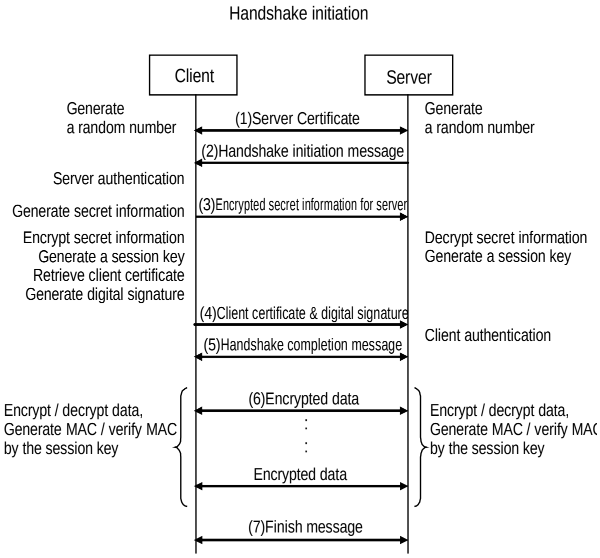

Handshake initiation
Client
Server
Generate a random number
(1)Server Certificate
Generate a random number
(2)Handshake initiation message
Server authentication
Generate secret information
(3)Encrypted secret information for server
Encrypt secret information
Generate a session key
Retrieve client certificate
Generate digital signature
Decrypt secret information
Generate a session key
(4)Client certificate & digital signature
Client authentication
(5)Handshake completion message
Encrypt / decrypt data,
Generate MAC / verify MAC
by the session key
(6)Encrypted data
Encrypted data
Encrypt / decrypt data,
Generate MAC / verify MAC
by the session key
(7)Finish message

Fig.2 Overview of SSL handshake protocol

(1) A client and a server exchange handshake initial messages.
(2) The server sends its certificate (chain) to the client and the client verifies the server certificate (server authentication).
(3) The client generates a random secret number, encrypts it with the public key included in the verified server certificate and sends it to the server. The server decrypts the encrypted random secret number with secret key. At this stage, the client and the server jointly generate and share the master key derived by the decrypted random secret number and random numbers exchanged in (1).
(4) The client sends its certificate (chain) and verifiable digital signature to the server. The server verifies the client's certificate and the digital signature using the verified certificate (Client Authentication).
(5) The client and the server exchange handshake finishing message
(6) The server and the client perform encryption communication with a shared master key.
(7) The server and the client exchange a encryption data communication message and end SL communication.

1.3 Local Communication Security

Recent mobile phones have a local communication interface such as IR (infrared), Bluetooth,802.11b. By using a local communication interface, mobile phones can communicate with devices in the near field. In Bluetooth and 802.11b, the authentication and its procedure based on common key are separately specified. Both of them perform encryption using a symmetric key after authentication.

2. Application Layer Security

This section describes the following application layer security topics: 1) digital signature for preventing repudiation, 2) digital signature for ensuring authenticity of downloaded S/W program, 3) license key distribution for copyright protection.

2.1 Digital Signature for Preventing Repudiation

Repudiation means the act of voiding agreed contracts by denying the order actually placed, or repudiating private information actually provided on online shopping.

An electric commerce system such as online shipping does not work if there is an option of repudiation.

In order to prevent repudiation, a digital signature is used. For example, request a user to attach a digital signature in order or confirmation and store them in a database (Refer to Figure 3). The user cannot repudiate because the private key used for creating the digital signature is only kept secret by the user. The digital signature for preventing repudiation will be promoted by XML Signature. It specifies the format of the digital signature and the procedure to generate the digital signature.

2.2 Digital Signature for Ensuring Authenticity of Downloaded S/W Program,

Recent mobile phones are capable of downloading additional S/W programs. However, downloading an S/W program poses a security threat because of malicious behavior.

The Java Runtime Environment provides a solution to that malicious behavior of downloaded Java applications. Another solution is the digital signature that is used by BREW applications.

BREW (Binary Runtime Environment for Wireless) is a platform provided by QUALCOMM. It functions as an interface or a layer of abstraction to the embedded chip's operating system. Because the BREW application is a native application, it can access critical H/W resources. In order to prevent malicious native applications to be downloaded and installed, the BREW application is attached with a digital signature generated and authorized by S/W quality evaluation institutes (at the moment, QUALCOMM is the institute). Verification of the digital signature assures the mobile phone that the S/W does not include malicious codes.

2.3 Key Distribution for Copyright Protection

Buying copyrighted content such as background picture, ring tone and music has become popular. Currently downloaded copyrighted content in mobile phones cannot be extracted (without encryption) so that the content cannot be viewed or listened to by other mobile phones or devices.

On the other hand, it is inconvenient when a user wants to change mobile phone, or share copyrighted content within a limited number of devices. Thus, encrypting contents serves as the best solution for both requirements.

The mechanism of encrypting contents is as follows: copyrighted content is encrypted with a key by a content provider. Then, a content key is distributed after encrypting so that the legitimate mobile can decode the content. In this case, only the user who bought the key can view or listen to the copyrighted content.

3. Future challenge

3.1 Security needed in case of losing mobile phones

The more critical features that mobile phones offer such as electric-purse or electronic-ID, the more users suffer from the impact of misuse of lost mobile phones. So security measures that mitigate the impact of the misuse of lost mobile phones are becoming more important.

Some kinds of mobile phones have a remote lock function but still the security is insufficient because the lost mobile phone can be misused until the user notices the lost mobile and sends the lock command to it. So a mechanism by which lost mobile phones authenticate the legitimacy of the user is needed without loss of usability.

3.2 Automatic key selection

The mobile phones of the near future will be able to handle several IC chips such as the embedded UIM (Uer Identity Module), Felica chip and other chipcards inserted in external memory card slots (ex SD slot, MS slot). Chips have several keys used for secure services such as secure communication, digital signature for non-repudiation, secure delivery of copyright protected content. To avoid degrading usability, automatic key selection is important. There are two approaches,

(1) several keys correspond to an application and an appropriate key is selected by the application dependent on the context of the application

(2) a key is allocated to an application and the application is automatically selected, depending on the situation.

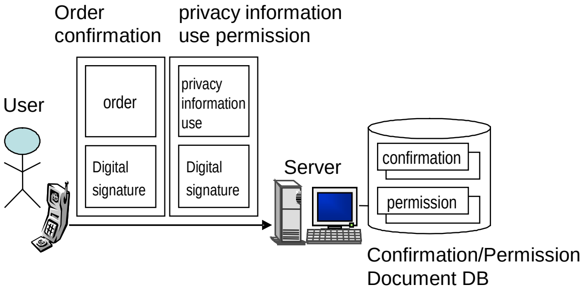


Fig.3 Digital signature for non-repudiation

In order to realize automatic key selection (described above), current software architecture used for mobile phones should be identified.

3.3 Less restricted copyright protected content delivery

Due to the popularity of iPod, it is recognized that, in order to prevail in the copyright protected content business, current strict copyright protection should be loosened so that users can share copyright protected content among family's devices or among their own devices. That is, if the copyright protected music content bought though a mobile phone can be listened to with a car stereo or their family's music players, the price of the content becomes reasonable, which may promote the copyright protected content business. Japanese MIAC (Ministry of Internal Affairs and Communication) has begun development of DRM (Digital Right Management) technologies that allow users to share downloaded copyright protected contents among users' devices such as TVs within the limit of content providers' permission. The technologies to allow the copy of protected content within the limit of the family phone or the user's own devices will be the requirement of DRM (Digital Right Management).

Security technologies for mobile phones are classified as communication security and application layer security. The next theme will be advanced security technologies such as automatic selection of keys kept in mobile phones dependent on situation and less restricted DRM.

Reference

[1] 3GPP TS 33.102 V6.2.0 (2004-09)

[2] RFC3275 ML XML-Signature Syntax and Processing, D. Eastlake 3rd,et al. March 2002.

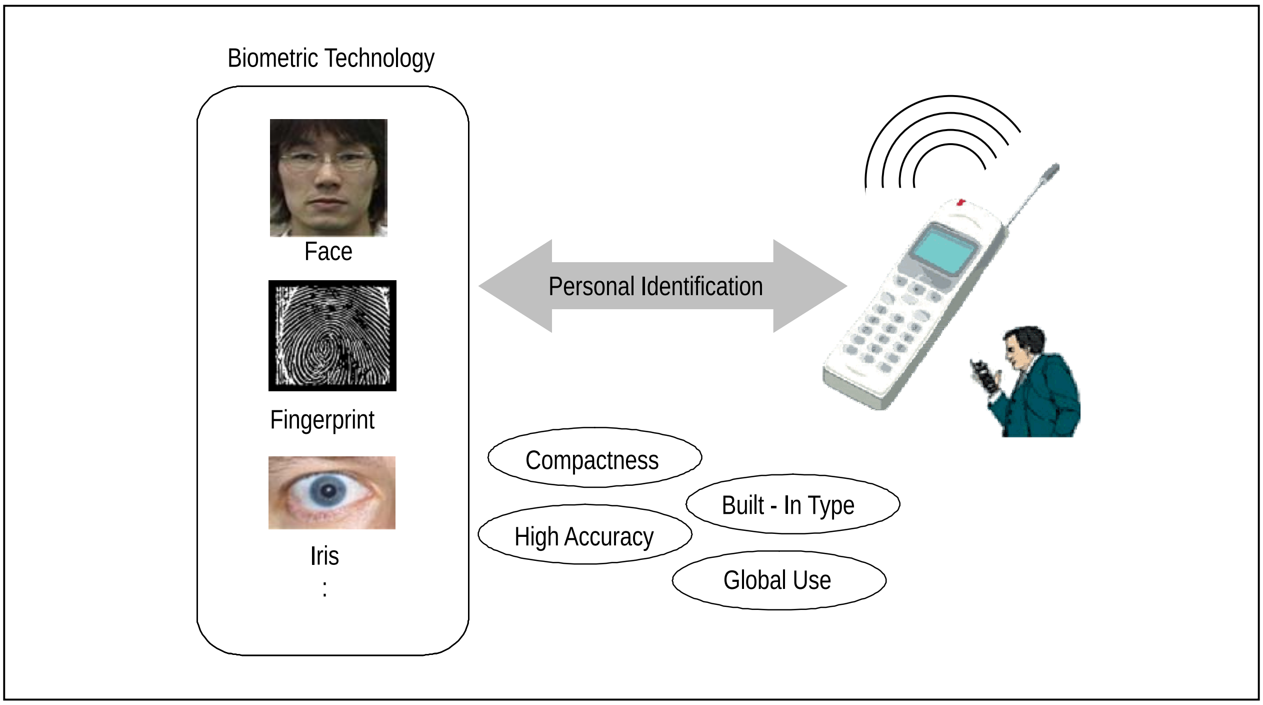
Biometrics in Mobile Handsets

Authors: *Manabu Hashimoto,*[*] *Shoji Tanaka*[**] and *Jay Thornton*[***]

The handset not only serves as a communication tool in the form of an integrated information terminal that keeps personal information (telephone numbers, e-mail addresses) but also serves as a high-value-added multifunctional tool that enables users to enjoy e-commerce through internet access, or carry out electric payment by using non-contact IC. With this technological progress, however, the risks in cases of loss, theft, and illegal use are becoming increasingly prominent. Consequently, security technology is vital in order to prevent these risks.

To date, the main security of the handset has been password protection, in which access is allowed by the input of several digit passwords. However, this type of personal identification is far from secure, since a "disguised" person can easily manipulate an identity through masquerading or identity theft. To solve this problem, biometric technology utilizing human biological characteristics has been drawing attention as a reliable method for personal identification. Biometrics technology relies on the patterns of various human characteristics, such as fingerprint, voice, face, palm, vein, hand, ear, iris, retina, handwriting, and walking, among which the fingerprint has long been the subject of study and has already been applied for verification purposes. This technology is currently being developed to fulfill various purposes, including those with importance focused on user convenience as well as reliability. When installing biometric technology into the handset, design and development need to be carried out with consideration of the restrictions on sensor size (required for inputting biological data) and on CPU resources (required for processing data for identification).

In this paper, we first consider biometric technology in general, from the viewpoint of sensor technology. Next, we introduce our company's approach to personal identification technology in handsets that use the face and the fingerprint, two human characteristics most popularly used for personal identification.



Connection between biometrics and mobile handsets:

Biometric technology uses human physical characteristics and is based on patterns of various human characteristics, such as face, fingerprint, voice, finger, palm, vein, hand, ear, iris, retina, and handwriting. The following mobile handset features are critical for applying biometrics: Robustness against illumination changes, high accuracy, realization of miniaturization even with sensor (input device) included in mobile, and global usability.

*Advanced Technology R&D Center **Information Technology R&D Center
***Mitsubishi Electric Research Laboratories

1. Foreword

Now that the handset serves not only as a simple communications tool (such as for making calls or exchanging e-mails), but also as a multi-functional tool (such as for using e-commerce to purchase products and settle payments online, and for using the electronic money function through non-contact IC cards), a more effective way to protect the handset from loss, theft, and illegal use is necessary. For this purpose, installation of biometric technology, which applies human biometric information for personal identification is being reviewed.

In this paper, we first consider biometric technology in general, from the viewpoint of sensor technology. Then, we introduce our company's approach to personal identification technology for handsets that use the face and fingerprint; the two human characteristics most commonly used for personal identification.

2. Overview of Biometric Technology

Biometric technology relies on the patterns of various human characteristics, such as fingerprint, voice, face, palm, vein, hand, ear, iris, retina, handwriting, and walking. Among them, the fingerprint has long been the subject of study and has frequently been used in the past.

There are two ways to make personal identification by using biometric technology. One is acquiring information without contact, such as from the face or the iris. Another is acquiring information through contact, such as from the fingerprint or the vein. In general, the contact type is more reliable and accurate. In Table 1, factors generally noted in biometric technology are shown for each of the human characteristics. Among these factors, User Acceptability is very important, along with the FR (False Reject) Rate and the FA (False Accept) Rate.

Table 1 Factors Generally Noted in Biometric Technology

Biological Information	FR Rate (%)	FA Rate (%)	User Acceptability	Cost
Fingerprint	~1	~0.1	○	◎
Face	1~	1~	◎	○
Voice	3~	3~	◎	○
Palm	1~	1~	◎	○
Vein	0.1	0.01	○	△
Iris	0.1	0.001	○	△
Handwriting	1~	1~	◎	○

3. Application of Face Recognition Technology

3.1 Targets to Meet

In general, handsets need to operate appropriately under any given lighting condition, since they are commonly used in various places, both indoors and outdoors. Moreover, when convenience is concerned, time required for face recognition processing should approximately be the same as the time required to input the current four-digit PIN code. Despite the fact that an increasing number of handsets are using faster hardware devices, in the aspect of performance, they are far from comparable to PCs. Furthermore, handsets are unable to secure sufficient work memory as PCs, due to restriction in memory. From the above, we can say that the handset's (1) operation in any given lighting condition and (2) realizations of higher speed and resource-saving, are important targets that need to be met.

3.2 Summary of Face Recognition Algorithm

Figure 1 explains the face recognition algorithm that was experimentally developed this time. This algorithm first detects the face region in an input image, and then detects the eye region. Then, by using measurements obtained for the position of the eyes and the distance between the eyes, it normalizes the size and position of the face region. For identification, this normalized face region is cut out and compared with the face registered in the handset. Feature vectors called "Rectangle Features"(1) enable detection of the face and the eyes, as well as matching with the registered image (see Fig.1). Also, detection the face and the eyes is made possible by applying the image to an identifier that is composed of a combination of several "Rectangle Features". An example of a feature vector is shown in Fig.2.

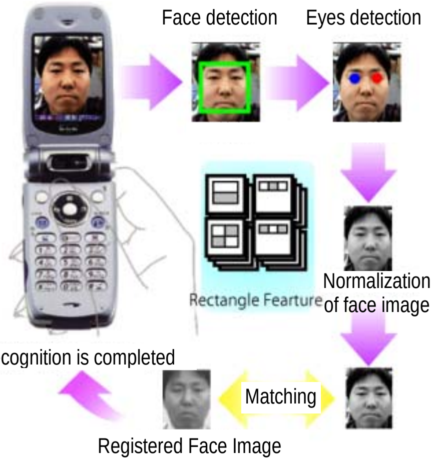


Fig.1 Flow of Face Recognition Process

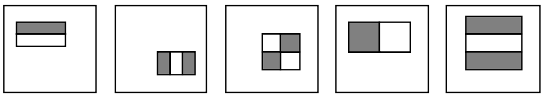


Fig.2 Example of Feature Vectors

3.3 Compliance with Given Lighting Conditions

One of the factors that influence the accuracy of face recognition is the shadow created on the face depending on the direction of lighting. Thus, we developed a method that minimizes shadow effects and normalizes image contrasts. In this method, first, the input image is logarithmically transformed, and the pixel values of dark areas are raised. Then, that image is differentiated, and strong and asymmetrical shadow edges (shadow areas) are removed. Finally, by integrating the differential image, a normalized contrast image least affected by shadow is obtained. By applying this normalization process to the "Face Recognition (Normalization) Process" (Fig.1), we were able to improve recognition accuracy.

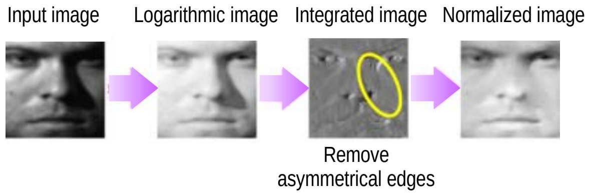


Fig. 3 Pixel Normalization
(From Face DB image by Yale University)

3.4 Compliance with Higher Speed and Resource-Saving

To detect the face and the eyes in an image, first, several resolution images of different scales are generated from the input image. Then, each of these generated images are scanned through a search window of a fixed size (24 x 24 pixels), and finally put through an identifier (mentioned in Section 3.2 above). Usually, only one face needs to be detected in an image for face recognition in handsets, and the face size in a handset-captured image is more or less predictable. Therefore, for detection, we used the image with the most appropriate resolution for detecting the largest face-size predictable. In other words, the image with the lowest resolution was processed for detection. Furthermore, we were able to significantly improve efficiency by stopping the processing the moment the face was detected. For the eyes, the most appropriate resolution for their detection was predicted from the size of the detected face, and by limiting processing only to the eye area, we were able to significantly reduce the amount of processing required. Also, for normalization, logarithmic transformation was sped up by generating a Look Up Table consisting of logarithmic values corresponding to the pixel values of 0-255.

For the identifier, the amount of data required for the detection and matching processes are 500KB for face, 200KB for eyes, and 50KB for matching. If these data are loaded to the heap memory all at once, 750KB worth of memory will be occupied instantly. To prevent this, we compressed each data (for the face, data was divided for compression) and arranged it so that only necessary data would be in the heap memory at each processing time. In this manner, we were able to hold down memory usage to 500KB for all the applications.

4. Application of Fingerprint Verification Technology to Mobile Handsets

4.1 Fingerprint Matching Algorithm

One of the popular fingerprint matching methods used for fingerprint verification is minutia matching, which regards ridge endings (end point of ridge) and ridge bifurcations (branch-off point in ridge, where a ridge further divides into other ridges) in fingerprints as minutiae, and measures their coordinates and angles. The general flow of the minutia matching process is as follows:

(1) Noise lines in the captured fingerprint image (such as cracks, cuts, scars, smudges, and wrinkles) are eliminated to restore the original true ridge patterns.

(2) The fingerprint image (with the ridge patterns restored) is transformed into a binary image, and then processed for thinning. Afterwards, the minutiae are extracted from the image.

(3) Using the coordinates and angles of the extracted minutiae, calculation is conducted to check the similarities between the captured fingerprint image and the registered fingerprint image. If the degree of similarity exceeds a certain value, the user is identified as the registered person.

Minutia matching is also the method used at Mitsubishi Electric for fingerprint matching, and matching performance depends on how accurate the minutiae are extracted in their true form. Due to this fact, Step 1 (Restoration of ridge patterns in the fingerprint image) in the above process flow is the most important. In the following section, we introduce a ridge pattern restoration method (2) that is highly effective.

4.2 Restoration of Fingerprint Ridge Patterns

A fingerprint image tends to contain various noise lines depending on the condition of the finger's skin surface (Examples include cracks due to dry skin, smudges due to excessive sweating, and ridge breaks due to wrinkles and scars). Since the forms of these noise lines change overtime, problems such as not being able to register the fingerprint, or not being allowed access even if registered, can occur at anytime. Therefore, to prevent these registration and access problems, a ridge pattern restoration process is applied to fingerprint images in order to correctly restore true ridge patterns that are permanent and unchanging thorough one's entire life.

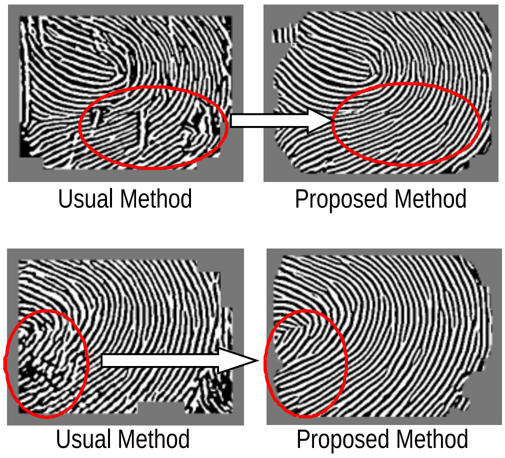


Fig.4 Results of Parallel Ridge Filtering (Proposed Method)

A new method using a "Parallel Ridge Filter" has been developed, and is giving highly satisfactory results in ridge pattern restoration by focusing on the parallelism of ridges. In this method, fingerprints are basically composed of parallel ridges, whereas noise lines are non-parallel. Therefore, in this method, multiple parallel lines are extracted as true ridges, and non-parallel lines are eliminated as noise lines. In this manner, parallelism is used to distinguish ridges from noise lines, making restoration of ridges easy for images with cracked or deformed fingerprints, usually considered difficult to register or match for identification.

4.3 Application to Mobile Handsets

Handsets are becoming increasingly popular among the general public, and they are also evolving more and more as multifunctional tools. Many handset manufacturers are considering the implementation of biometrics in their products as a way of preventing unauthorized accesses, and some manufacturers have already done so. To back this up, compact fingerprint sensors are currently being successively released for handset use. The type of sensor that is most commonly used in this field is the sweep-type fingerprint sensor, a type of linear sensor. As the user slides his/her fingertip over this sensor, it captures several sets of partial images (one set includes a defined number of successive images). The captured images are then reconstructed into two-dimensional images, and finally matched with the registered fingerprint.

4.3.1 Sweep-Type Fingerprint Sensors: Targets to Meet

When images from the sweep-type sensor and the two-dimensional-type sensor are compared, we can see that the sweep-type has the following advantages: The sensor is small and compact; Latent fingerprints do not remain on the sensor; High performance is offered at low cost; Any rotation or shift of finger positioning is accounted for. However, the user must be skilled, in order for the sensor to capture a fingerprint image of satisfactory quality. Also, in the aspect of image processing, the following targets need to be met for sweep-type sensors when compared with two-dimensional sensors:

(1) Two-dimensional images need to be reconstructed from partial images.
(2) Unnecessary parts (such as finger joints) need to be eliminated from the images.
(3) Since the image length changes each time an image is captured, the area processed for feature extraction and the range in which searches are made for matching, both need to be flexibly changed, accordingly.

4.3.2 Image Reconstruction Algorithm

The following explains the flow of image reconstruction (process of reconstructing two-dimensional images from partial images) using the Image Reconstruction Algorithm:

(1) Several sets of partial images are captured (One set includes a defined number of successive images) --> The algorithm calculates the contrast per partial image and also the contrast per set of partial images.
(2) The positions of the successive images are adjusted, and position shifts [Δx and Δy] are calculated.
(3) In case the contrast is low, position adjustment may not go well. In this case, position shifts [Δx and Δy] are corrected by the Relaxation Method so that finger sweep speed is maintained with reference to contrast values.
(4) By using the position shift values that are calculated by position adjustment, two-dimensional images are created by overlapping the partial images.

In our case, we performed position adjustments in units of sub-pixels, so as to improve accuracy. Also, we considered the position with the smallest inter-image difference to be the most appropriate position for image reconstruction.

Furthermore, we developed a method in which the directions and angles of ridges are referred to in small partial segments within an image, and are used to extract the position of a finger joint. By using this method, we were able to add a new process of eliminating the part below the finger joint from an image.

4.3.3 The Overall Results of Fingerprint Matching

By using the Image Reconstruction Algorithm as described above, we reconstructed a total of 2700 images (15 persons x 6 fingers x 30 times), and visually checked the reconstructed images. As a result, although several images showed breaks in the ridges, overall, the fingerprints were correctly reconstructed. Figure 5 shows an example of a two-dimensional image, reconstructed from partial images captured by a sweep-type fingerprint sensor (Sweep direction: Left to Right).

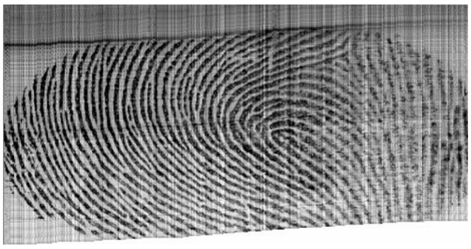


Fig. 5. An Example of a Reconstructed Fingerprint Image

We also checked how accurately the fingerprints were matched. For this purpose, we first modified a matching algorithm used at Mitsubishi Electric to comply with variations in the areas processed within an image for feature extraction, and variations in the sizes of ranges in which searches are made for making matches. Then, we performed tests to evaluate the accuracy of the matches. As a result, we found that the modified algorithm gave an accuracy that satisfied the target specification as follows: (Required that the user is skilled in sweeping his/her finger across the sensor) Access Allowed for Unauthorized User (FA (False Accept) Rate): 0.01%, Access Denied for Registered User (FR (False Reject) Rate): 1% or below.

5. Conclusion

In this paper, we present a broad overview of biometric technology, and introduce face recognition and fingerprint matching as identification technologies being developed for mobile handsets. We plan to make further improvements to these technologies in terms of user convenience and performance accuracy, and to encourage their use in mobile handsets.

References:

(1) P. Viola and M. Jones: Rapid object detection using a boosted cascade of simple features, Proc. IEEE Conf. CVPR, (2001)

(2) T. Nakamura, H. Fujiwara, M. Hirooka, K. Sumi: Fingerprint Image Enhancement using a Parallel Ridge Filter, Proceedings of ICPR2004, CD-ROM (2004)

(3) D. Maltoni, et al: "Handbook of Fingerprint Recognition," pp.65-69, (2003).

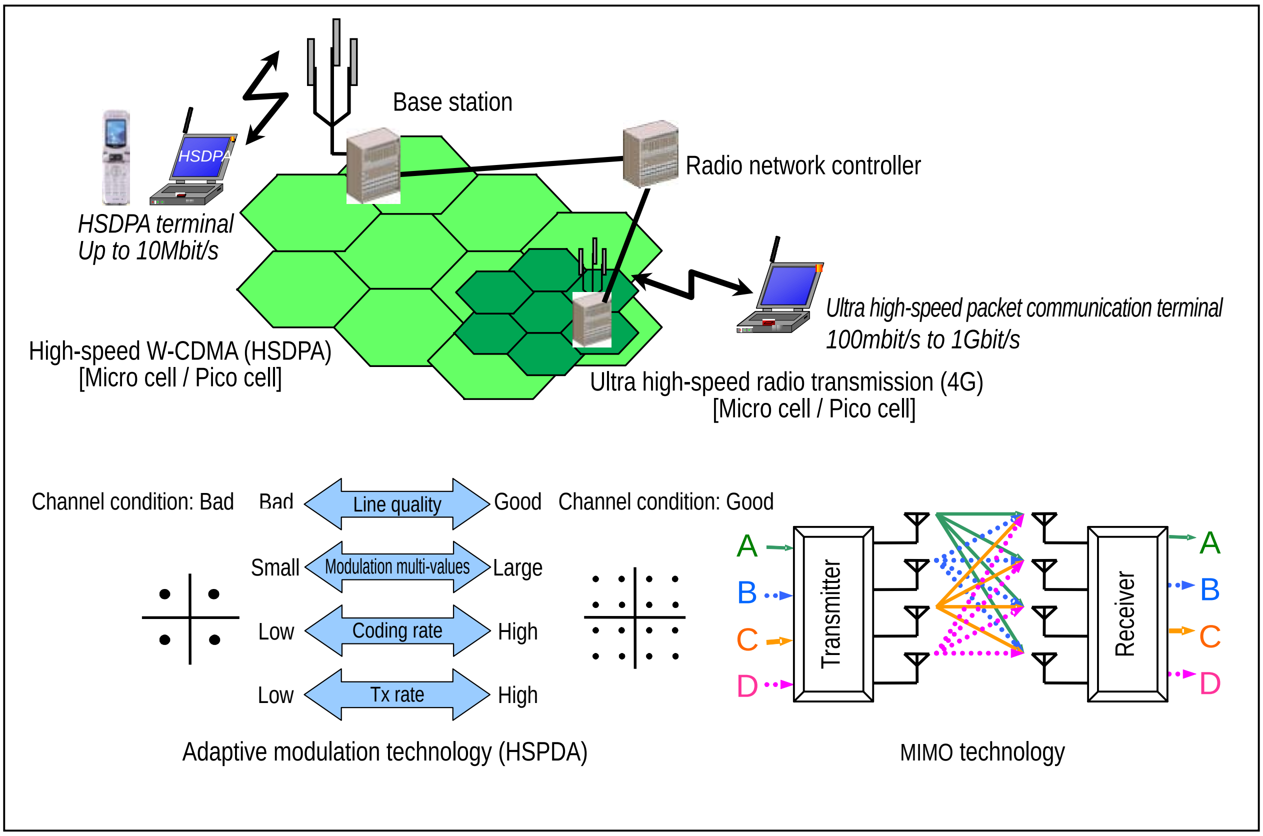
Broadband Wireless Transmission Technologies

Authors: *Fumio Ishizu**, *Akihiro Shibuya** and *Takahiko Nakamura**

With market penetration in excess of 70% and maximized profits per user, the Japanese mobile phone market is saturated. At the same time, demand for advanced services, such as supporting seamless access to images and sound with enhanced reality, has continued to grow. To meet this demand, the development of new and efficient wireless broadband radio access is vital.

The mobile phone system has shifted to the third generation era represented by FOMA, offering users services at the maximum transmission rate of 384 kbps. Upon the practical application of higher W-CDMA technology called HSDPA (High Speed Downlink Packet Access, standardized in Dec. 2002) with transmission rate up to 14.4 Mbps, megabit-class high-speed data communication service will be available. Into the further future, R&D activities are underway to achieve gigabit-class wireless packet transmission for fourth generation mobile communication systems. This packet transmission is being studied to further upgrade services with a target rollout in around 2012.

This paper describes the features of the 'HSDPA' system, presenting a key HSDPA technology 'turbo coding' from the hardware complexity viewpoint. It also introduces the HSPDA trial platform developed for throughput performance evaluation. In addition, it presents 'MIMO' (Multiple Input Multiple Output), a promising technology for fourth generation mobile communication systems.



Approach toward Wireless Broadband

To realize high-speed wireless packet transmissions, we employed technologies such as adaptive modulation technology, which speedily optimizes the parameters of modulation and coding schemes according to the conditions of radio transmission channels, and MIMO technology, which enables high-speed parallel data transmissions.

* *Information Technology R&D Center*

1. Introduction

Wireless broadband technologies are being studied to provide seamless reception and transmission of video contents and music distribution services. This article describes high-speed W-CDMA technology HSDPA (High Speed Downlink Packet Access) that realizes data transmission rate up to 14.4 Mbps. It also presents MIMO, a key technology for fourth generation mobile communications to realize the maximum transmission rate of around 1 Gbps.

2. HSDPA Technology

2.1 Features

Table 1 shows the key specifications of the HSDPA system. In order to increase peak transmission rate, enhanced throughput and low latency, the system employs HS-DSCH (high-speed downlink shared channels) that multiple users can share, resulting in higher peak transmission rate and improved selector throughput. The key techniques are listed below.

Table 1 Key HSDPA Specifications (Release 5 FDD method)

Multiplexing method	Frequency division duplex (FDD)
Access method	Code division multiple access (CDMA)
Frequency band width	5MHz
Modulation method	QPSK, 16QAM adaptive modulation
Channel decoding	Adaptive channel decoding
Chip rate	3.84Mcps
Data transmission rate	Up to14.4Mbps (960kbps x 15 codes)
Sub frame length	2msec (7680 chips/3 slots/sub frames)
Time slot length	3 slots (HS-DSCH)
Transmission interval	2msec (HS-DSCH)
Error correction	Turbo decoding:R=1/3(HS-DSCH)
Interleave	32 (L) x30 (W) fixed(HS-DSCH)

(1) AMC (Adaptive Modulation and Coding) Function: this supports enhanced throughput by adaptively and speedily changing modulation and coding parameters according to the channel estimation quality [(1)].

(2) HARQ (Hybrid Automatic Repeat reQuest) Function: this supports enhanced error retransmission efficiency by diversity combing of soft-decision data between original and retransmission data packets.

(3) Adaptive Resource Scheduling Function: this supports enhanced sector throughput by allowing multiple terminals to share a single physical channel. Every 2 ms, the resource scheduler measures each user throughput and determines the optimal time and code resources to maximize the whole throughput.

2.2 Turbo Coding Technology

Error correction in turbo coding involves more than four iterations of soft input/output processing to ensure sufficient performance. This requires to reduce processing delay in each repeated computation and to increase CRC detection speed, so that turbo code blocks delivered at the maximum rate of 14.4 Mbps per 2 msec are decoded and ACK/NACK signals are transmitted with low processing delay. Based on these requirements, we reduced processing delay to approximately 1/10 at the transmission rate of 14.4 Mbps by implementing parallelization on the decoding circuit configuration of turbo coding. This parallelization includes parallel processing per code blocks segmented in turbo encoding blocks and synchronous processing of forward and backward path-metric computations in each turbo decoding processing.

Furthermore, descramble processing and CRC error detection are implemented after turbo decoding processing. When error detection processing is followed once conventional decoded code blocks are temporarily stored in memory and connected to a CRC sequence, memory writing takes a certain period of time before CRC processing.

To solve this drawback, as Fig.1 shows, the outputs of the turbo decoding results per up to six code blocks are divided by descrambling with the CRC generator polynomial g(x). Each resultant remainder $z_0(x), z_1(x), \ldots, z_5(x)$ give the CRC result z(x) without storing the memory by linear transformation processing with equations (1) and (2)[(2)]:

$$z(x) = z_0(x)y_5(x) + z_1(x)y_4(x) + \cdots + z4(x)y1(x) + z5(x) \pmod{g(x)} \quad (1)$$

$$y_k(x) = x^{kN} \pmod{g(x)}\ (k=1,2,\cdots,5) \quad (2)$$

where N is the code block length.

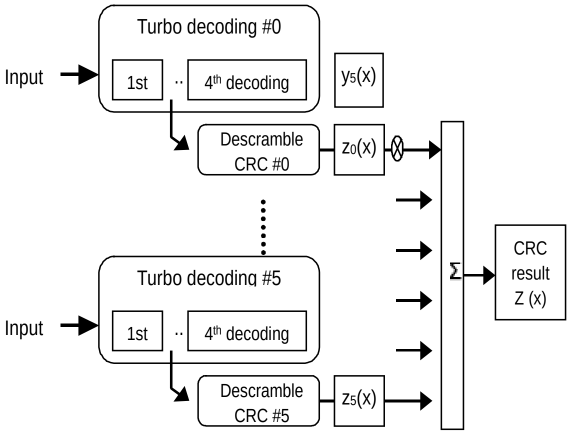


Fig 1. CRC Computation Parallel Processing

2.3 HSDPA Trial Platform

In order to evaluate the throughput and transmission delay performance of the HSDPA system, we developed a trial platform. Figure 2 shows the architecture of the HSDPA trial platform. The feature of the base station is that the plug and play configuration architecture is employed to handle both the HSDPA and the W-CDMA functionalities in the same hardware. The base station also has the feature of original resource allocation technique to minimize the transmission delay [(3)]. Regarding the terminal, the simplified core architecture is employed to reduce the hardware complexity.

3. MIMO Technology

Since the 3.5-generation technologies including HSDPA, faster transmission rates have been expected, which will lead to the exploitation of broadband as a solution to increased transmission capacity. In the 4th generation, broadband in the order of 100MHz are expected so that multi-carrier systems will be deployed to prevent delay waves due to higher clock speeds. Broadband is, however, limited because of scarce frequency resources, thus growing attention has been given to a new MIMO technology that increases spectral efficiency with multiple antennas.

Figure 3 shows the configuration of a 2-antenna MIMO system. The two transmit antennas Tx1 and Tx2 simultaneously transmit different signals x_1 and x_2 over the same frequency. The two signals interfere over transmission channels and are received at two receiver antennas as signals y_1 and y_2. If x_1 and x_2 are extracted from y_1 and y_2 at the receiver, doubled transmission speed is achieved without increasing frequency bands [(4)]. There are a number of algorithms for equations to estimate transmit signals x_1 and x_2 from receive signals y_1 and y_2. The simplest algorithm is called ZF (Zero Forcing), which reduces interference components to zero (when x_1 is extracted, x_2 is an interference component) by liner combining of y_1 and y_2.

In contrast, an algorithm focused on transmission performance is called MLD (Maximum Likelihood Detection), known to achieve optimal signal detection performance in theory. Compared to ZF, however, MLD is a 4-antenna system requiring computations 10,000 times or more. This is a major problem in computational reduction to realize real-time performance.

In this section, the ZF algorithm is summarized. In Fig.3 the MIMO system is described by the following equation:

$$Y = HX + N \qquad (3)$$

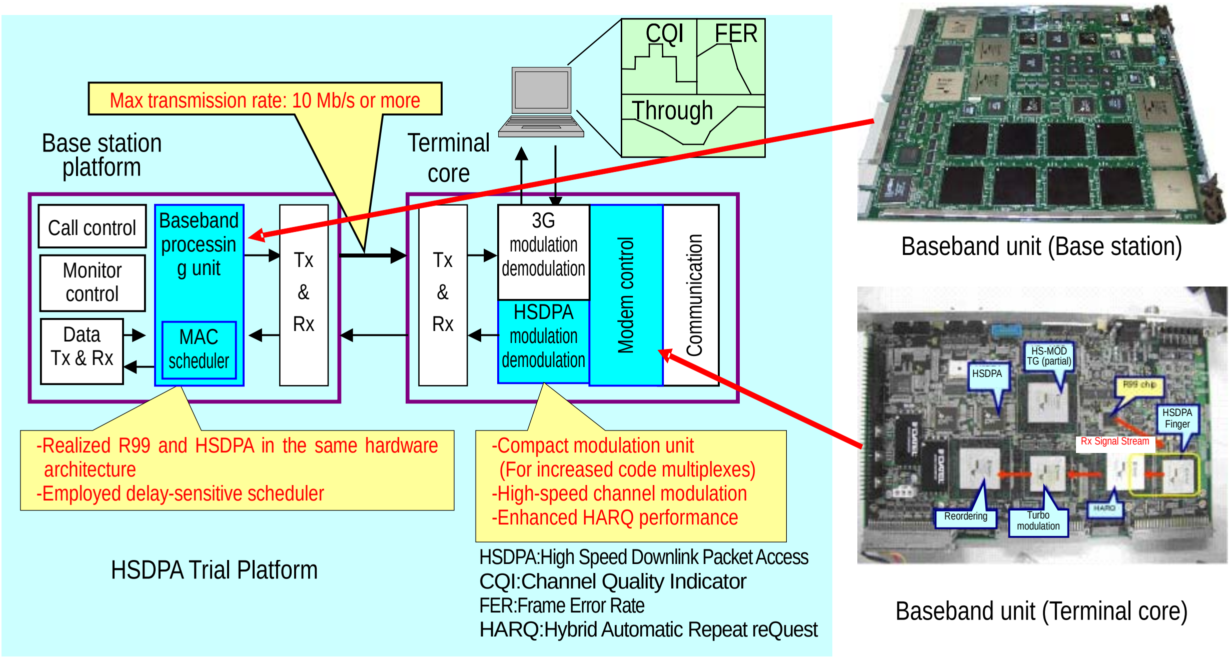
where X is a transmit signal vector, Y is a receive signal vector, H is a transmission channel matrix, N is a noise vector.

Note that the followings are denoted in the 2-antenna MIMO system in Fig.3:

$$Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \quad N = \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \qquad (4)$$

$$H = \begin{pmatrix} h_{11} & h_{21} \\ h_{12} & h_{22} \end{pmatrix} \qquad (5)$$

with n_1 and n_2 presenting a noise component per receive antenna. When an inverse matrix exists in the transmission channel matrix H, the estimated transmit signal value X' is expressed by the following equation:



-Realized R99 and HSDPA in the same hardware architecture
-Employed delay-sensitive scheduler

-Compact modulation unit
(For increased code multiplexes)
-High-speed channel modulation
-Enhanced HARQ performance

HSDPA:High Speed Downlink Packet Access
CQI:Channel Quality Indicator
FER:Frame Error Rate
HARQ:Hybrid Automatic Repeat reQuest

Baseband unit (Base station)

Baseband unit (Terminal core)

Fig.2 Architecture of HSDPA Trial Platform

$$X' = H^{-1}Y + H^{-1}N \qquad (6)$$

As shown above, the noise components after signal detection are given by $H^{-1}N$ with respect to the estimated signal value X'. It means the S/N of the estimated signal can be calculated.

Figure 4 shows the example of packet error performance of MIMO system. In this simulation, modified IEEE802.11a frame format is used. The simulation parameters are shown in Table 2. In the Figure, MLDR presents complexity-reduction MLD while the numbers present the reduction scale of computational complexity. Compared to ZF, MLD shows a steeper curve in transmission performance, which indicates that greater diversity gains are obtained. The MLD performance will degrade as the computational complexity is reduced.

Not only a parallel transmission system, but also MIMO is configured as a transmit diversity system, which allows the same data to be sent from multiple receive antennas and diversity gains to be obtained at the receiver. Since the transmit diversity system does not require multiple antennas at the receiver side and the computational complexity is low, it is gaining attention as a method of expanding the service areas of existing radio systems.

Research and development of MIMO systems are currently ongoing. A major problem of the systems is that they cannot be applied all the time. For instance, when telecommunicating (angular spread≒0) in a complete open space, the example in Fig.3 gives $h_{11}=h_{21}=h_{12}=h_{22}=1.0$. This shows the inverse matrix H does not exist, meaning parallel transmission is impossible. For the development in future radio systems, spectral efficiency is an issue that cannot be easily avoided, so there are great expectations for MIMO technology. Further intensive research will be conducted with consideration of the operating environments in actual systems.

Table 2 Simulation Parameters

FFT size	64
No. of carrier	52
Modulation scheme	OFDM-64QAM R=3/4
Packet length	12 OFDM symbols
No. of pilot	4 OFDM symbols
No. of antenna	3-signal detection scheme: ZF, MLD
Transmission channel	18-path Rayleigh Exponential decay model

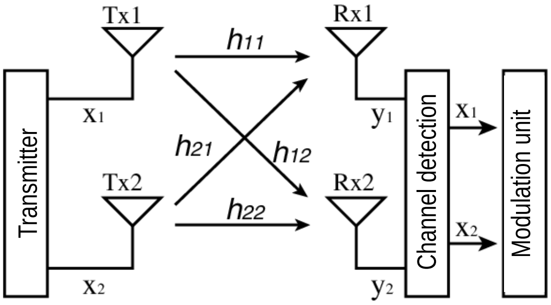


Fig.3 Configuration of 2-Antenna MIMO System

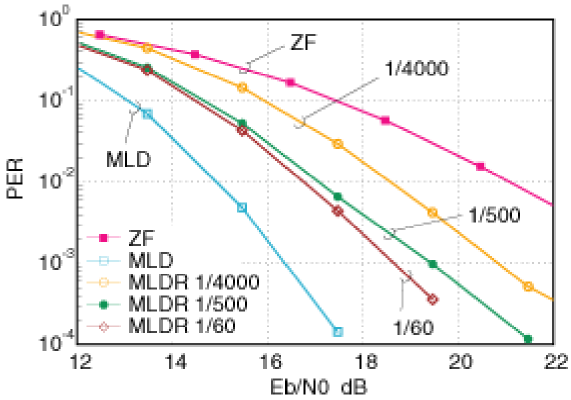


Fig. 4 Comparison of Transmission Performance using Signal Detection Algorithm

4. Conclusions

This paper presents the HSDPA system overview and key technologies to realize broadband wireless transmission technologies. In addition, the architecture of the HSDPA trial platform that we developed to evaluate the throughput performance is shown. The features and challenges of MIMO, a promising technology for increasing transmission capacity are also presented.

References

(1) Tanada, et al., "Study on Packet Combination for HARQ in HSDPA," The Institute of Electronics, Information and Communication Engineers, General Conference Proceedings B-5-25 (2003)

(2) Nakamura, et al., "Study on Turbo Coding for HSDPA," Society of Information Theory and its Application, SITA2004,21-1 (2004)

(3) Fujie, et al., "Application of Delay-sensitive Scheduling Algorithms to HSDPA," The Institute of Electronics, Information and Communication Engineers, General Conference Proceedings B-5-26 (2003)

(4) A.van Zelst, R.van Nee, G.A. Awater, "Space Division Multiplexing (SDM) for OFDM Systems," VTC 2000 Spring Tokyo, 2000 IEEE 51st, Volume 2, 2000.

MITSUBISHI ELECTRIC CORPORATION

HEAD OFFICE : MITSUBISHI DENKI BLDG., MARUNOUCHI, TOKYO 100-8310. FAX 03-3218-3455