Parallel Multimedia Signal Processing

Takao Nishitani, Makoto Iwata, Yoshimasa Kimura,
Keiichi Sakai and Takahiko Mendori

Department of Information Systems Engineering
Kochi University of Technology
Miyanokuchi 185, Toshayamada, Kami-Gun, Kochi Prefecture, 782-8502, Japan

E-mail:{nishitani.takao, iwata.makoto, kimura.yoshimasa, sakai.keiichi, mendori.takahiko}
@kochi-tech.ac.jp

要約：並列信号処理プロジェクトとしてオーディオやビデオの将来的応用を実現できる並列プロセッサアーキテクチャを検討している。これは将来的にはケイタイ電話用チップとして実現することを目指しており並列処理によるプロセッサの低消費電力化だけでなく、応用アルゴリズムとしても広域処理と局所処理に分割して処理効率をあげる。応用としてはメディア変換とヒューマンインタフェースを取り上げて研究を進めている。

Abstract：The Parallel Multimedia Signal Processing project will aim at establishing a multi-microprocessor platform as a driving force of diverse utilization of audio and video contents for cell-phone and mobile applications, and will then propose an application chip for future mobile systems. In this platform, the architecture is designed to realize efficient processing over both global and local multimedia signals which are used for small object recognition and matching in pictures, and high level compression processes. The architecture is also considered on efficient media conversion and friendly human interface as key functions for future cell phone.

1. Introduction

Considering about the trend of today's cell phone applications, future phones might have a lot of functions which include a high quality camera function, object recognition and so on. The required functions will be very similar to those of human eyes, ears and a mouth to communicate with a cell phone itself by its user. In order to achieve human like capability on object identification, such as face identification and moving object identification, nearly TOPS (Tera Operations per Second) processing capability is required. In addition, due to sever power dissipation requirement for a cell phone, the employment of multiprocessor approach is inevitable, where relatively low clock frequency with low supply voltage is attainable for high speed processing. Further power reduction is possible by employing multi-resolution processing, where the full resolution processing task is minimized and idle processing and elements under low resolution processing are controlled to be switched off from power supply.

The Parallel Multimedia processing project, presented here, will aim at establishing a multi-microprocessor platform, having the above mentioned features with TOPS capability with 500 mW of Power. In this project, the platform architecture is studied in two different ways. One is an Audio and Visual domain specific ASIC multiprocessor for short range applications and another is a data flow general purpose multiprocessor for future applications. These two approach may co-exist in the SoC (System on Chip) era. As a result, key applications for future parallel processing should be studied and used for multiprocessor architecture evaluations. The image of future cell phone applications are shown in Fig.1. When you find out beautiful flowers and interesting insects, you will probably take a picture with HDTV quality by a camera on a cell-phone. These photos are sent to the home PC which has a large DB. Then you can understand what it is. In case of now object in a photo, you should store it into your DB, when you come back. A future cell phone will surely overrun the function of conventional PDA (Personal Digital Assistance) which support us like a notes, and it will become a new PDA, abbreviated form of Personal Digital Advisor which tell us what we do not know, such as automatic translation of foreign language and person's name through face recognition. Friendly interface to/from such PDA is another important technology factor to study. Therefore, this project has been carried out in the following 4 different subprojects.

Subproject-1:
Global/Local Multimedia Signal Processing and ASIC processor.
Subproject-2:
Data Flow processor and its applications
Subproject-3:
Media Conversions
Subproject-4
Non-professional User Interface

Although this project has started this year(2004), daily communications and discussions on these subproject status, enable publishing quite a lot papers. The followings are the report of subprojects in more detail. 2. Subproject-1

Global/Local Multimedia Signal Processing and ASIC processor

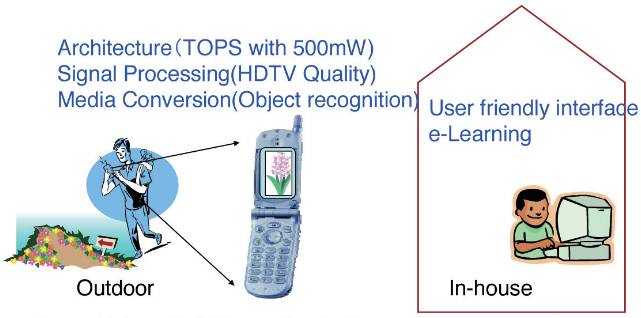
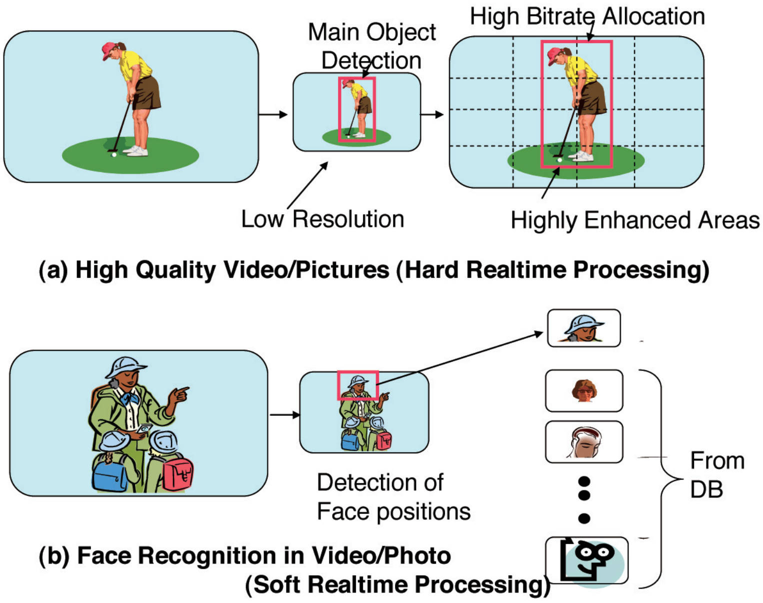

Architecture (TOPS with 500mW)
Signal Processing(HDTV Quality)
Media Conversion(Object recognition)
User friendly interface
e-Learning
Outdoor
In-house

Fig.1. Future Cell Phone Applications and key technologies. Photos in the fields can be stored into your Data Base. In addition, a future cell phone tells us what we do not know, such as foreign language translation, names of people in a photo and navigation to the destination.

2.1. Multi Resolution Processing for Cell Phone Applications

One of the growing hardware functions on a cell phone is a high resolution camera, and its resolution, a number of pixels in other words, is now reaching 3M, and is expanding to more pixels. Picture processing on such high resolution video/photos becomes the heaviest task in the cell phone applications. However, such high resolution video/photos are not for cell-phone to cell-phone communication purpose, because of a small display on a phone. Applications might be for live transmission to home TV or photos for memory, just like a digital camera. Other important applications are object recognition for making annotation on the video/photos for rich media application, or for remembering the name of person.



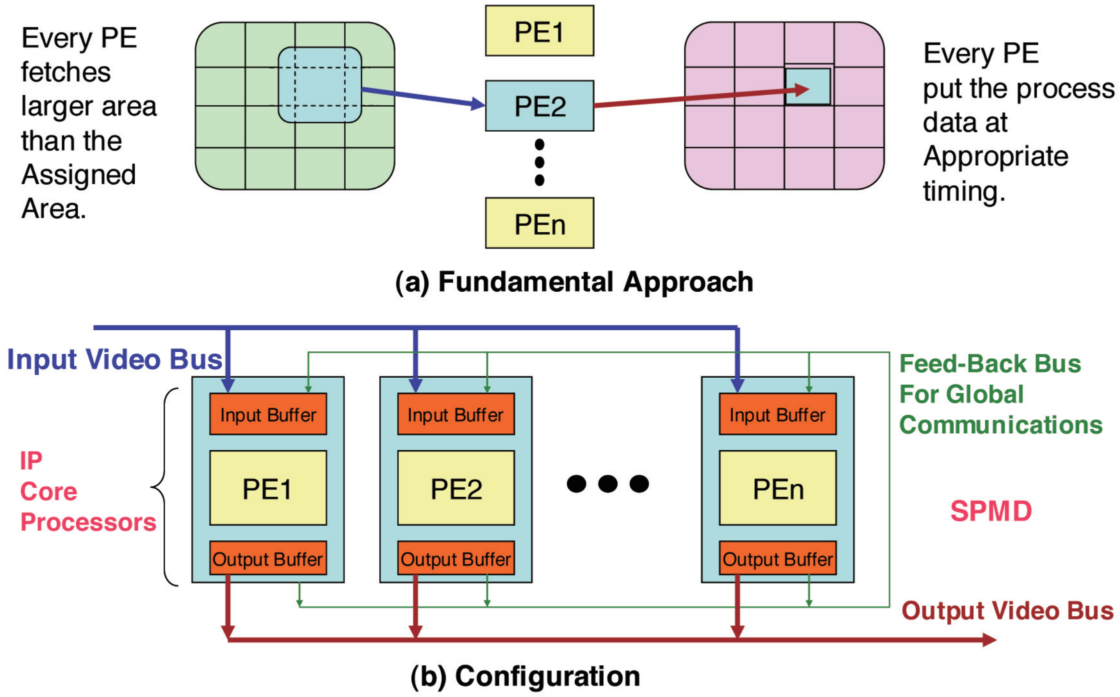
(a) High Quality Video/Pictures (Hard Realtime Processing)

(b) Face Recognition in Video/Photo (Soft Realtime Processing)

Fig.2. Mega-pixel video/photo applications on a cell phone.
(a) Live video transmission to home.
(b) Object recognition for person identification or annotation for rich media.

Figure 2 shows such applications and multi-resolution approaches in two different classes. In case of live applications, high quality encoding or picture enhancement should be processed within a frame period; that is hard real-time processing. Plural number of processors should process one picture with collaboration at a time. However, adaptive spatial enhancement or adaptive bit allocation on a spatial area of importance gives better performance as shown in Fig. 2(a). This requires global processing. On the contrary, soft real-time applications are for object recognition. In a low resolution picture, an object to be recognized is detected and then a segment of a high resolution picture, corresponding to the object, is compared with a lot of objects stored in recognition data base as shown in Fig. 2(b). As the full resolution processing area is limited to that containing the object, processing burden becomes light. In addition, recognition during several frame periods is acceptable; time requirement is relaxed. In such a case, whole matching process to a picture from DB can be completed in the same processing element. Other processing element executes matching between the detected sub-picture and other pictures from the DB.

2.2 VSP Review



(a) Fundamental Approach

(b) Configuration

Figure 3. VSP Multiprocessor. (a) Fundamental Approach with overlap-save technique. Processing is carried out independently during one frame period. (b) Multiprocessor configuration. The same programs except index addressing data runs in every PE.

The architecture of VSP is based on the overlap-save technique on a FIR filter processing, shown in Fig. 3 (a). First, one frame picture is divided into a number of processing elements (PE) and every PE is assigned to every sub-picture, but the input area of every PE is set to be larger than the processing area. Thanks to the input data redundancy, every PE can carry out processing, such as FIR filter and motion compensation, without communicating with other PE. In addition, every program for PE are the same; a kind of SPMD (Single Program, Multiple Data) machine classes. VSP configuration is also simple, shown in Fig 3(b), where video samples are fed on an input bus, and every PE fetches necessary data from the bus. Therefore, the overlap-save condition is easily realized. This processor had been developed in commercial use as a video codec. However, the big drawback is a redundant memory capacity. When the processing area is set to NxN, one pixel wider input area in every direction causes 4N. Actual memory capacity required is easily exceeds twice or third times of the processing area.

2.3 IMAP Review

IMAP, shown in Fig. 4, follows VSP's strong points as much as possible, but the target is to realize a single chip multiprocessor for automobile cruising. In order to eliminate the redundant memory, IMAP employs direct communication between adjacent PEs with SIMD control. Video I/O is carried out through shift registers, which come from a pipelined video bus approach for VSP. The big difference between IMAP and other SIMD processors exists in the employment of index addressing. This function enable flexible processing of global operations such as labeling or boundary tracing by using autonomous addressing mode, where boundary search is started from the initial point to every directions at the same time.

Thanks to the simple architecture, IMAP has 128 PEs, operating at 100MHz. As every PE has a 4 way VLIW structure, totally 50GOPs processing capability is realized with 2.4 to 5 W of power. As the IMAP is developed by a very conservative LSI technology of 0.18 um, 1 TOPS operation will be expected to be possible if 0.06 um technology is applied. In this case, 1024 PEs will be on-chip and every PE operates at 300MHz with 0.5 V power supply. The power dissipation will become around 600mW, reasonable to cell phone.

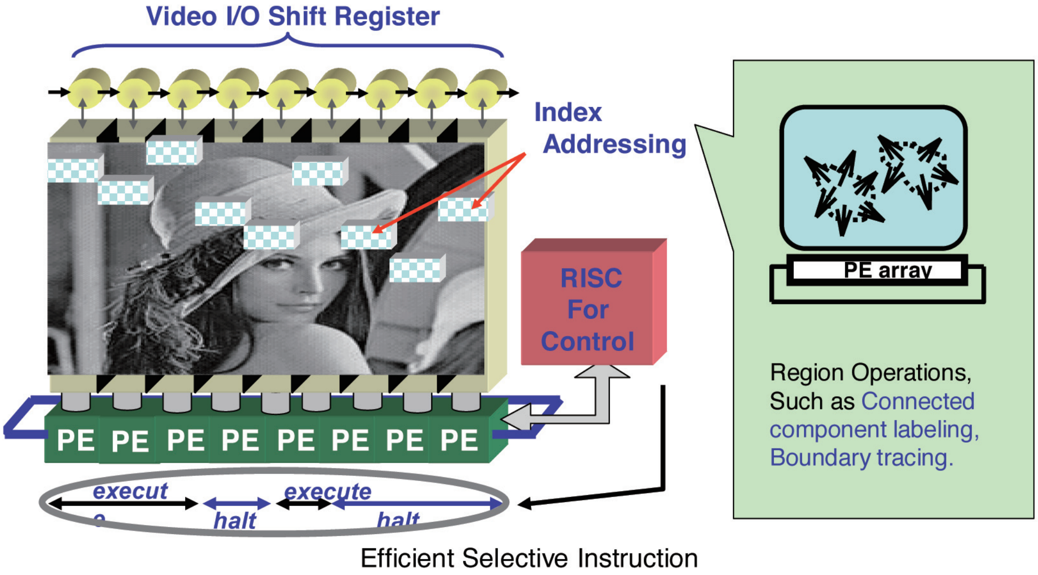


Figure 4. IMAP is a SIMD processor with index addressing. Every PE is assigned to a column area of a picture. Due to index addressing functions, global operations such as labeling becomes possible.

2.4 Candidate ASIC Multiprocessor Architecture

Figure 5 shows a candidate for future multiprocessor approach, where IMAP, followed by VSP with non-overlap processing for multi-resolution processing is used for both hard real-time and soft real-time processing. The reason of the selection is as follows.

VSP approach in Section 2.2 is suitable for both hard real-time applications, collaboration of PEs, and soft real-time applications, whole processing in every PE. Also, software compatibility to an existing cell-phone processor will be easily realized, when every PE is selected from one of industry standard embedded processors, such as ARM, MIPS or SH. Some of such processors have already been available as an IP core, for giving simple implementation. In addition, power management is simple enough, due to the linear array multiprocessor nature. However, redundant memory reduction has to be mandatory for cell phone applications. Global operations in low level signal processing are for computationally extensive functions, such as boundary tracing, labeling. Also, high order FIR filtering and motion compensations are classified into global functions. In this area, IMAP is suitable, due to the simple, but powerful architecture of SIMD. However, due to the column based processing nature and the SIMD nature of all processing among PE, which are carried out by single instruction at a time, it seems not to be suitable for several different pattern matching processes with different picture sizes at a time.

The above matching or recognition processing should be transferred to VSP with a non-overlap memory structure. A large grain processing can be easily realized in this approach. Further study is required for comparison to data flow multiprocessors such as Data Driven Multimedia Processor (DDMP) [4] in the area of multi-resolution decomposition and boundary tracking.

2.5. Conclusion of Subproject-1

Future cell-phone applications and possible architecture have been studied.

In terms of applications, a class of hard real time applications and a class of soft real time ones have been shown to have different requirements on architecture design. However, almost all applications, classified into soft real time, require some global operations for their preprocessing. In addition, global processing has a similar nature of hard real time processing. Therefore, the structure of IMAP followed by VSP seems to be a suitable way at the moment, but further study is required for multi-resolution decomposition.

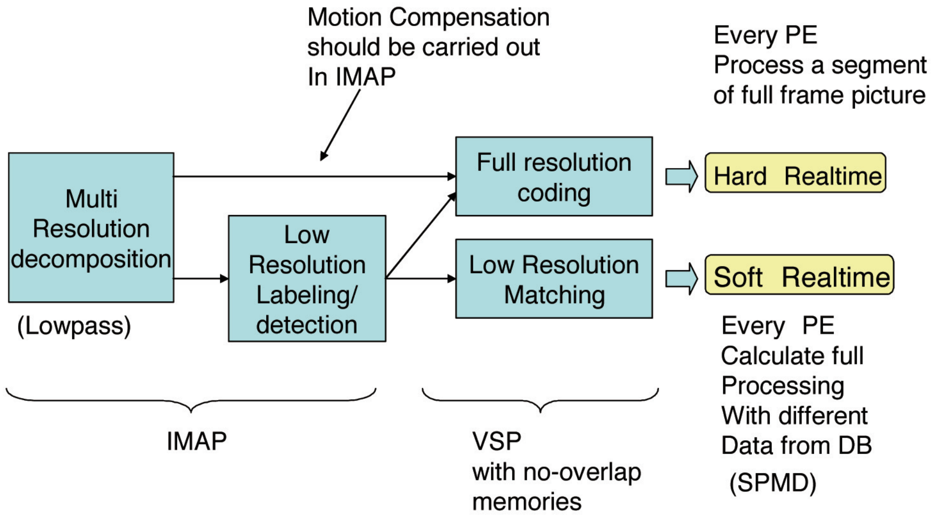


Fig. 5. Architecture of IMAP followed by VSP with non-overlap memories. This is a reasonable candidate of multi-resolution multiprocessor for future cell phones.

3. Subproject-2 Self-Timed Data-Driven Multiprocessor

Pipeline structure is considered to be the best solution to overcome LSI design limitation constraints by allowing divide and conquer design principle. In addition, it also helps us diminish wiring lengths across and thus minimizing extrinsic degradations. However, with increase in clocking rate, the structure also suffers from excessive power consumption and skew problems associated with synchronous clock distribution. A self-timed pipeline structure has been proposed to solve these problems simultaneously and applied to the commercial self-timed superpipelined multimedia processors [4].

3.1. Subproject2-1: Fully Self-Timed Priority Queue

A folded pipeline scheme employed in a folded queue (FQ) demonstrates another functional advantage of the self-timed pipeline (STP) scheme. An FQ capable of differentiating 100M packets/s streams on Diffserv basis [5] was successfully fabricated by 0.18um CMOS process.

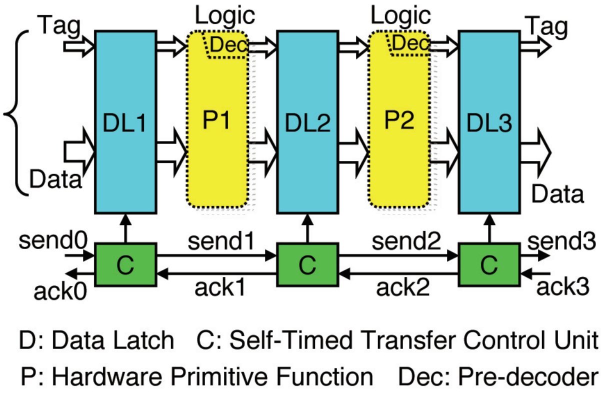

Tag
Logic
Dec
Logic
Dec
Tag
DL1
P1
DL2
P2
DL3
Data
Data
send0
send1
send2
send3
C
C
C
ack0
ack1
ack2
ack3
D: Data Latch C: Self-Timed Transfer Control Unit
P: Hardware Primitive Function Dec: Pre-decoder

Figure3.1: Schematic diagram of self-timed pipeline.

Figure 3.1 shows the basic structure of an STP scheme where data transfer between the stages of a pipeline is controlled by a chain of self-timing transfer control units. Every control unit generates a clock signal to the data latches when send and ack signals are both active. That is, the send signal indicates that the processed data in the preceding stage is ready to be fed to the inputs of the latches and the ack signal shows that the succeeding stage is empty. A piece of input data traverses pipeline stages until the data arrives at an occupied stage, i.e., one in which active data are present. If a piece of data at the end of a pipeline is removed, the remaining data in each of the pipeline stages step successively to succeeding stages in a bucket relay fashion. Therefore, the asynchronous FIFO exhibits an elastic nature by adjusting the effective length of the pipeline to the amount of data stream residing in the pipeline. The STP scheme provides good design and signal integrity by virtue of localized control and wiring, even in deep submicron chips. These features were utilized in the development of self-timed super-pipelined data-driven chip-multiprocessors (DDMPs) [4].

The mutual interactions among two or more STP's potentially provide various functionalities for developing SoC's. The FQ module shown in Figure 3.2 is proposed as one of these extensions of STP to achieve the queueing and scheduling speed required for network processors working at over 10Gb/s. This figure shows a folded pipelined queue FQ constructed by folding a linear STP in half and attaching a shortcut path at each stage of the pipeline. The bypass stage allows a piece of data flowing at the up-stream pipeline to bypass the pipeline when a corresponding stage of the opposite down-stream pipeline is not occupied, thanks to the elastic mode of operation. In other word, the data are automatically queued in the FQ if its egress is congested under certain external conditions. Therefore, the FQ behaves flexibly along with the egress traffic condition as if it were a variable length FIFO queue.

Data branching and merging transfer in each stage of the FQ are locally controlled by the TC circuits, as shown in Figure 3.3. The data branching off to the shortcut pass is controlled by an extended data transfer control unit Cb, shown in Figure 3.4. The ARB unit detects which send signal in up-stream or down-stream stages arrives earlier. Then, if a send signal sent from the preceding stage of the up-stream arrives early, the Cb unit generates a send signal and a local clock signal to the data latch in the bypass direction. If not, the Cb unit generates those to a latch in the up-stream detour stage. On the other hand, a sort of merging function with first-come-first-service is carried out at every stage in the down-stream pipeline.

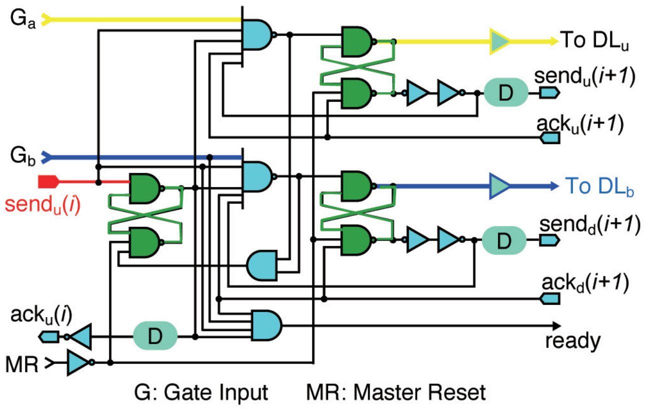


Figure 3.4: A self-timing transfer control circuit for the branch module.

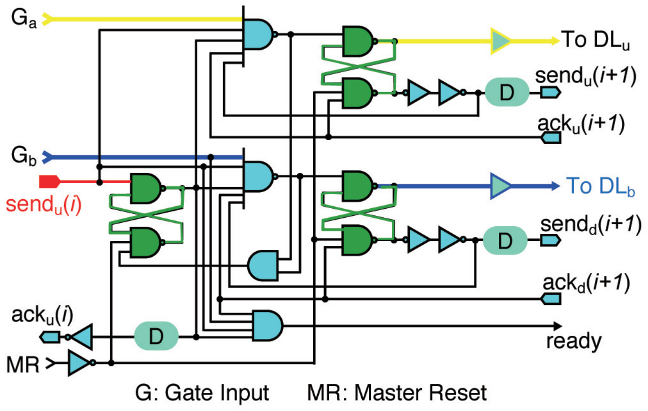


Figure 3.4: A self-timing transfer control circuit for the branch module.

If the send signal is delayed by a certain delay element, the detection of the signal in the ARB unit is latent. Thus, the bypassing probability of data packets would be lower. This can be applied to the priority queueing function. Therefore, we introduce the insertion of a variable delay module (VD) on each send signal line. The delay time of the VD varies according to the priority value included in the data packet. As a result, lower priority class data packets traverse for a longer time within the FQ chip because the probability of bypassing is decreased by the greater latency of the send signal.

In Internet QoS control protocols like Diffserv, it is also required to differentiate packet loss ratio as well as queueing delay. Usually, application traffic requiring short delay like VoIP allows packet loss, while ftp-like traffic requires no packet loss in place of allowing long delay. In order to realize such a priority queueing function in a single FQ module, each stage of the up-stream pipeline may discard a packet based on its priority. By presetting the specific discarding stage for each priority class, we can implement any priority queueing function on the FQ module.

Thus, the FQ module also allows us to deal with a class of long delay and low packet loss. It is noted that in order to realize those kinds of elastic function in synchronous pipeline circuits, there is no alternative except to emulate this folded STP circuit, incorporating autonomous queueing and scheduling functions.

To verify the automatic differentiation capability of an FQ module under various egress conditions, we have simulated the FQ module, incorporating a packet discarding function at each stage. In this simulation, input data packets have one of three priorities. The highest priority in those requires the shortest queueing delay but permits the highest probability of packet loss. The data packets with the highest priority are discarded for the FQ module when they arrive at the 30th stage of the pipeline. The middle ones and the lowest ones are discarded at the 60th and 100th stages respectively. Figure 3.5 show simulation results on the equivalent volume of traffic in each priority class when altering the egress blocking ratio from 10% to 90%. The results indicate that the FQ module can definitely differentiate prioritized packets in terms of both queueing delay and packet loss probability under various egress traffic conditions.

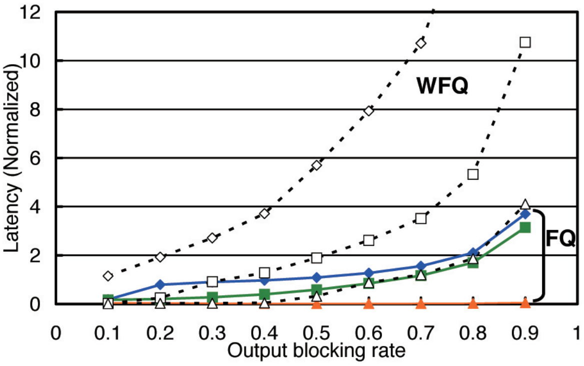


Figure3.5: Latency characteristics of the FQ module.

The proposed FQ module with 100x128bit word packet queueing capacity is implemented in a 1.5V, 0.18um CMOS six-metal layer process. The test chip interfaces with the existing DDMP chip and allows us the utilization of a coprocessor for expanding DDMP performance. The test chip layout, with a total core area of 1.42mmx1.42mm The FQ module in the chip accepts 128bit packets categorized in 8 flow classes at around 100M packets/s.

3.2. Subproject2-2: SSS on Data Driven Processor

Secret Sharing Scheme (SSS) is used to store data securely, and the data to be stored is distributed and encrypted. The original data is distributed and encrypted to multiple shares. The security is enhanced by the feature that the original data is never restored from the single share. However, the encryption process takes a lot of time. In the past, the calculation technique based on 2's extension field have been used to reduce the time, but the effect is limited.

The purpose of the research is reduction the time to encrypt the data by SSS. Our approach adopts data driven processor such as Data Driven Multimedia Processor (DDMP) for encryption processor. In this research, we show the efficiency of the data driven processor for big number calculation used to k, n threshold SSS by the basic implementation. Furthermore, we describe about the application of (k, n) threshold SSS. The application is written by dataflow graph (DFG) where the DFG is corresponding to the program in the conventional von Neumann type processor, and it is evaluated by the data driven processor simulator or the real processor DDMP. Our goal is to implement a fast and secure distributed backup program.

3.2.1. Introduction of Subproject2-2

SSS is the technique of the data to be stored, distributed and encrypted. However, the encryption process takes a lot of time. In the past, the calculation technique based on 2's extension field[6,10] have been used to reduce the time, but the effect is limited.

The purpose of this research is reduction the time to encrypt the data by SSS. We think that the limitation of the time reduction is caused by the processing scheme of the processor because of the data dependencies among the words (ex. 32bits for 32bit processor) in the big number calculation.

Our approach adopts data driven processor such as DDMP for encryption process instead of a conventional von Neumann type processor. It is natural to adopt the data driven processor for the big number calculation because of the data dependencies are no problems. The first is (k, n) threshold SSS [6, 7, 9] encryption/decryption module written in DFG.

The calculation technique based on 2's extension field, and we aim at to reduce the calculation time. The second is a user command using SSS module. The command divide, encrypt and distribute the data into physically distant site through the network, and then it gather, concatenate and decrypt the data from physically distant site through the network.

The original data is divided into n-pieces of share in distribution, while restoration of the original data requires at least k-pieces (where k is less than n) of share.

3.2.2 Former SSS

The secret sharing scheme is the technique of the data to be stored, distributed and encrypted. The distributed data is called share, the original data is distributed and encrypted to multiple shares. There are several kinds of secret sharing scheme [6, 7]. In this research, the (k, n) threshold SSS that used a polynomial complement is taken up. The (k, n) threshold SSS is distribute and encrypt original data to n shares and it need more than k share for decryption to original data. If the share is less than k then original data is not decrypt. Example of the (k, n) threshold SSS is shown by Figure 3.6.

In the case of this example, it say that the (3, 4) threshold SSS. If we keep having only one share, we can't decrypt original data. But if we have 3 or 4 shares, we can decrypt the original data.

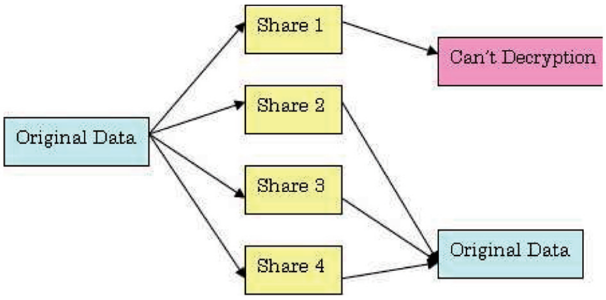


Figure 3.6: Example of the (k, n) threshold SSS.

Therefore the (k, n) threshold SSS is better for concealment and disasters. However, there is a problem that is calculation time is very long in this (k, n) threshold SSS. The reason is a calculation of prime number and primitive number when the data is distributed and encrypted. A conventional technique to solve the problem is a calculation using 2's extension field. All calculation inside a conventional computer is performed with the binary number. Therefore, it is desirable to express calculation with the binary number. The conventional technique effectively reduces the calculation time because of the binary number corresponds to 2's extension field. Comparison of the calculation time of encryption and decryption is listed in the table 3.1.

In the case of using the 2's extension field, calculation time is less than another [8]. However, there is a limitation using the 2's extension field.

Consequently, we adopt the data driven processor such as DDMP instead of Neumann type processor, and we aim at fundamental resolution in this research.

Table 3.1: Comparison of Calculation Time of Encryption and Decryption.

Encryption		
Block length [Byte]	Do not using 2's ext. field [sec]	Using 2's ext. field [sec]
1	29	12.8
2	55	14.3
Decryption		
Block length [Byte]	Do not using 2's ext. field [sec]	Using 2's ext. field [sec]
1	15	7.5
2	8	10.8

3.2.3 Improvement of Former SSS

Past SSS have the problem that is calculation time is very long. Consequently we used the 2's extension field as a measure for reduce the time.

However, there is a limitation to reduce the calculation time yet. The limitation is due to the processing scheme of the conventional processor (i.e. von Neumann type processor). In the conventional processor, the calculation is sequential by predetermined order in the program.

A big number used in SSS scheme is divided into machine's natural size (i.e. word), data dependencies among the words cause severe pipeline stall. Consequently, we adopt the data driven processor instead of Neumann type processor, and we aim at fundamental resolution in this research. The data dependency in the data driven processor calculation is no problem, and it is suitable for calculate a big number.

In this research, we implement the (k, n) threshold SSS used the 2's extension field on the DDMP and we aim at more reduction the calculation time. This program is written by DFG. We make the (k, n) threshold SSS's encryption and decryption module by DFG. Figure 3.7 shows example of encryption module by DFG.

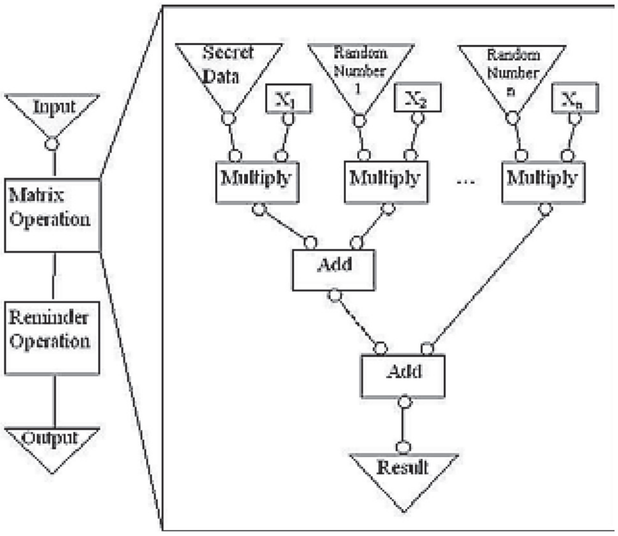


Figure 3.7: Example of encryption module by DFG. It is the simplified example of encryption module

It is the simplified example of encryption module by DFG (Figure 3.7). DFG is possible to write a calculation intuitive. Therefore it is thought easier than popular programming language to write. The goal is to make the practicality application written by DFG.

3.2.4 Conclusion of Subproject 2-2

There is a technique of safety keep of data. It is called SSS. SSS is better for concealment and disasters but it need a long calculation time when calculate a distribution and encrypt. Until now, the researcher used the 2's extension field in calculation on the conventional processor but it was limited yet. Consequently we use the DDMP that is using the 2's extension field in calculation. And we aim at fundamental solution to reduce the calculation time.

3.2.5 Future Works of Subproject 2-2

The purpose of this research is to implement a practicality application. The present stage is only to implement the (k, n) threshold SSS that is not using the 2's extension field in calculation. It is a primary stage for our purpose and there are problems to be solved. Future subjects are enumerated below.

✓Learn a technique of how to draw DFG. (How to express a table, simultaneous equations and how to use built in memory etc.)

✓A more nearly mathematical understanding.

✓Implement the the (k, n) threshold SSS using the 2's extension field in calculation.

✓Compare the calculation time of the (k, n) threshold SSS using the 2's extension field with not using it.

✓Consideration to practical use or not.

4. Subproject-3 Media Conversions

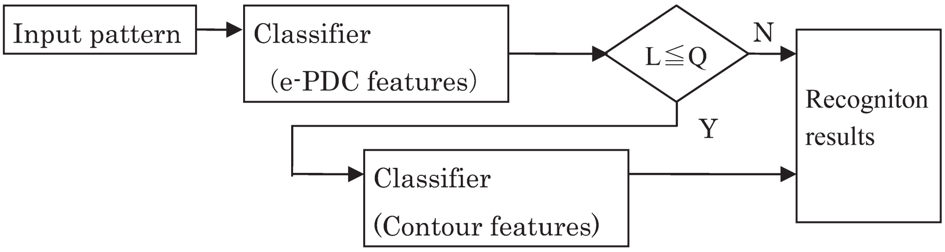
Media conversion means the operation that converts a certain media into another media such as conversion from character pattern to voice. Media conversions become key technology on automatic translation of foreign language which is one of target in Parallel Multimedia Signal Processing. This section deals with Kanji character recognition as media conversion and describes analysis conclusions of Kanji character recognition system that we developed.

4.1 Kanji character recognition

Various features and recognition methods in handwritten Kanji character recognition has been investigated [11], [12]. As a result, it has been clarified direction of stroke is effective for Kanji character recognition. This depends on that Kanji character pattern possesses many straight line components. However, since non-Kanji (Kana (Japanese syllabary) characters, symbols and alphanumerics) has many curve component, high recognition rate cannot be achieved by using the feature for Kanji character recognition. We proposed hybrid recognition system [13] that the extended peripheral direction contributivity (e-PDC) features which contains straight line component and contour features which contains curve component are used selectively according to Kanji and non-Kanji. It was confirmed that the hybrid method improve recognition rate when e-PDC features is used alone. However, reason why the recognition rate improved had not been clarified. This paper investigates the cause using relation of correct recognition and misrecognition on both features.

4.2 Hybrid recognition system

The processing flow of hybrid recognition system is shown in Fig. 4-1. First, the system performs classification using e-PDC features then obtains candidates. Next, this system judges whether the input pattern belongs to Kanji or non-Kanji. Denote non-Kanji character set as S_0, the number of candidate which belongs to S_0 among top-K candidates obtained by classifier using e-PDC features as Q and L as a threshold. If L ≦ Q, the system judges that the input pattern belongs to non-Kanji then performs classification using contour features and outputs the classification results as a final results; otherwise, the system judges that the input pattern belongs to Kanji then outputs the results obtained by classifier using e-PDC feathers as a final results.



L: Threshhold

Q: The number of candisate belonging to S_0

Figure 4-1: Hybrid recognition system.

However, this mechanism has the fault that the final result is sure to become misrecognition when Kanji character pattern is misjudged to non-Kanji. To relieve the misjudgment from Kanji to non-Kanji the dictionary covers not only non-Kanji but also Kanji whose shape is simple. Concretely, Kanji character that the probability satisfying L ≦ Q exceeds the threshold α is registered in the dictionary. By this strategy, the system performs classification that uses properly features among two kinds of features selectively according to complexity of the input character pattern's shape.

4.3 Experimental results

4.3.1 Configuration of hybrid recognition system

The classifier using e-PDC features deals with 3,201 characters consisting of 2,965 Kanji characters, 166 Kana characters, 34 symbols and 36 alphanumerics. The classifier using contour features covers 256 characters including 200 non-Kanji (166 Kana characters, 34 symbols and alphanumerics). The system used K=10, L=4 and α =0.0074. The test data (1,124 samples) were written in the free-style, so contains distorted samples.

4.3.2 Analysis of recognition results

Let Ψ be a pattern set which is judged as non-Kanji and recognized by contour features. We analyze which of features is effective. Table 4-1 shows recognition rate and misrecognition rate when e-PDC features and contour features are used.

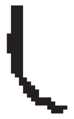
As the Table 4-1 indicates, adding the classifier using contour features reduced the error rate of the classifier using e-PDC features by 1.4% for test data. The rate of samples that passed over the classifier using contour features was 53.6% of all test data. Define positive action as the rate of samples that are misrecognized using e-PDC features and correctly recognized using contour features. Define negative action as the rate of samples that are correctly recognized using e-PDC features and misrecognized using contour features. The positive action and the negative action are 5.3% and 3.9%, respectively.

The difference of both is the effects, which is 1.4% previously described. This shows that there exists not the positive action alone but the positive/negative action, and the positive action exceeds negative action, and this excess produces the effect. These analyses clarified that why is the effect caused by the hybrid recognition system and how is the structure of the effect composed.

Figure 4-2 and Fig. 4-3 show example of the input pattern where positive action and negative action are caused, respectively. As shown in Fig. 4-2, positive action was chiefly observed for character pattern whose shape is simple such as " し ", ",", etc. On the other hand, negative action was observed for distorted character pattern or similar-shaped character pattern. Figure 4-3 (a) shows example of the distorted input pattern " グ ", which is misrecognized to " づ " because of large deformation. Figure 4-3 (b) shows example of similar-shaped character pattern " 才 ", which is misrecognized to " オ ".

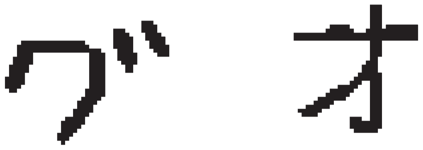
Table 4-1: The relation of correctly recognition and misrecognition for each features.

Contour feature e-PDC feature	correctly recognition	mis- recognition
correctly recognition	39.7%	3.9%
misrecognition	5.3%	4.7%



(→ し

Figure 4-2: Example of positive action.



グ → づ　　オ → 才

(a) Distorted pattern.　(b) Similar-shaped character pattern.

Figure 4-3 Example of negative action.

4.4 Conclusion of Subproject-3

We have clarified relation of recognition and misrecognition concerning e-PDC features and contour features, and confirmed the effect that both features are selectively used. As a result, it is clarified that positive action introducing contour features and the negative action are 5.3% and 3.9%, respectively, and 1.4% of difference of both is the effects. Namely, it is clarified that recognition rate increases because of not positive action alone, but positive action over the negative action. This analysis method can be used besides the handwritten Kanji character recognition because of its universality.

5. Subproject-4 Non-professional User Interface

In recent years, computerization has been progressing quickly in schools. In Japan, the Ministry of Education, Culture, Sports, Science and Technology and the Ministry of Public Management, Home, Affairs, Posts and Telecommunications pushing forward the introduction of computers and network environments to schools in order to enrich information education [14][15].

The computers and network environments in Japanese schools are being improved. However, the present environment is not adequate for children. The main reason is that it is not an established individual environment. User authentication is required in order to establish an individual environment. When a student logs on to the networks, she/he types her/his account and encrypted password on a keyboard. However, not all primary children know the alphabet. This was the focus of this study.

This paper describes the new password input interface suitable for primary school children. First, we conducted an icon discernment study with the schoolchildren in the lower grades. Next, we designed an interface using the icons obtained from the results of the discernment study. Additionally, the evaluation of the use of the designed interface is described. Moreover, the interface was improved and it was evaluated. Finally, the example of the application system using improved the interface is described.

5.1 Design of Password Input Interface

5.1.1 Investigation of Icon Discernment

First, we investigated the discernment of icons by primary school children. The subjects were 31 Japanese first graders. We prepared 10 categories of icons, fruits, flowers, colors, carriages, insects, animals, symbols, vegetables and necessary goods. A total number of 129 icons were prepared. The subjects looked at these icons on the computer screen. Then, they had to describe the icons on paper. Consequently, 65 kinds of icons that they can discriminate were extracted. Icons with a discernment of 100% were strawberry, mandarin orange, banana, melon, watermelon, Japanese persimmon, apple, patrol car, airplane, bike, bicycle, red, aqua, yellow, rabbit, cattle, giraffe, cat, carrot, frog, turtle, cicada, ant, desk, chair, triangle, rectangle, heart, daystar and rain [16][17].

5.1.2 Design of Password Input Interface

Most primary school children could operate a mouse, so we designed a mouse based password input interface. Figure 5-1 shows the designed interface. The icons are 32 pixels square and each interval was half size the size of an icon. The icons were arranged at random. Whenever an icon is chosen, it is arranged at random. Thereby, a password cannot be distinguished by others from the position of an icon. The interface has three buttons. A push on the determination button means password input is complete. A push on the clear button means clearing an old input. If the back button is pushed, input in the previous icon can be repeated. A user name registered beforehand can be chosen from the pulldown login name list. The message indicator shows the user the success or failure of the login. The state indicator shows the input situation of an icon used in the present password.

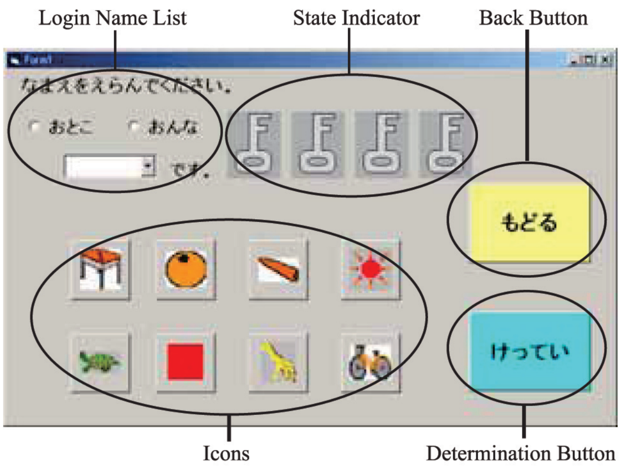


Figure 5-1 Overview of Designed Interface.

5.2 Evaluation

5.2.1 Outline of Evaluation

Evaluation was conducted using the improved interface. Figure 5-2, 5-3, 5-4 shows the arrangement of icons. They are investigation of the questionnaire by primary school children. All the numbers of inputs of a password were fixed to 4 times. Three types of interfaces with different numbers of icons and its arrangement were used for evaluation.

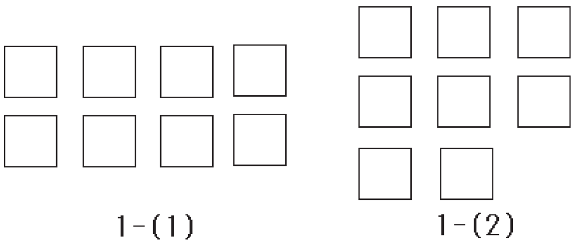


Figure 5-2: 8 Buttons.

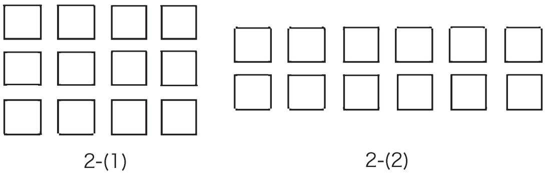


Figure 5-3: 12 Buttons.

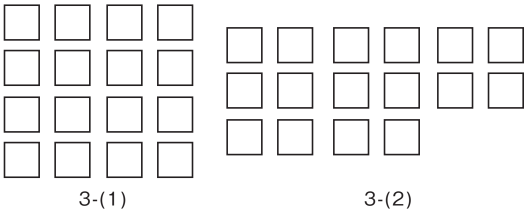
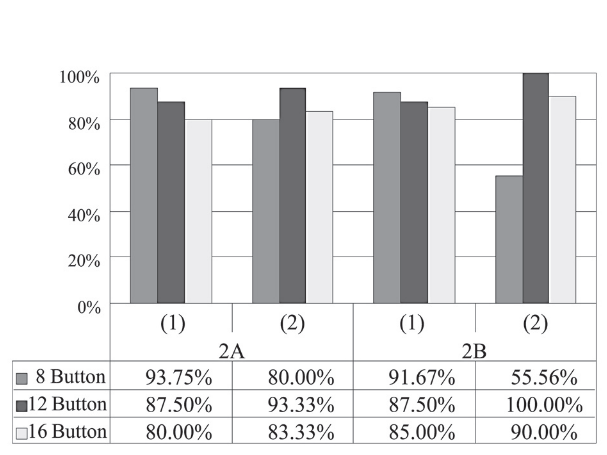


Figure 5-4: 16 Buttons.

Subjects are two classes (2A and 2B) of the second grader. The children of each class were divided into three groups. They are using 8 button interface group, 12 button interface group and 16 button interface group. 2A class children used the interface of (1), after using the interface of (2). 2B class children used the interface of (2), after using the interface of (1). The input time and correctness of each interface were compared.

5.2.2 Results of Correctness

Figure 5-5 shows the results of correctness. There was a significant difference between 8 button (1) of 2B to 8 button (2) of 2B and each button (2) of 2B according to analysis of variance. Additionally, 12 button interface is stable as a result of comparing the average value. This result means that the interface with the arrangement of an icon near two lines has a good rate of a correct answer.



	2A (1)	2A (2)	2B (1)	2B (2)
▨ 8 Button	93.75%	80.00%	91.67%	55.56%
■ 12 Button	87.50%	93.33%	87.50%	100.00%
□ 16 Button	80.00%	83.33%	85.00%	90.00%

Figure 5-5: Correctness.

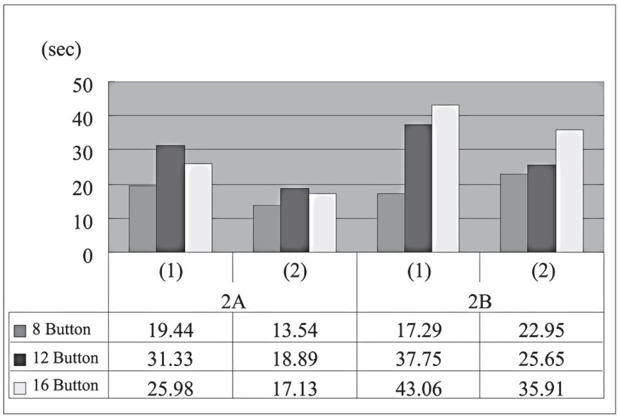
5.2.3 Results of Selection Time

Figure 5-6 shows the results of selection time.

There was a significant difference between 12 button (1) of 2A/2B to 12 button (2) of 2A/2B and 16 button (1) of 2A to 16 button (2) of 2B according to analysis of variance. Additionally, there was a significant difference between 8 button (1) of 2A to 8 button (2) of 2A according to analysis of variance. Moreover, there was a significant difference between each button (1) to (2) according to analysis of variance. This result means that the interface with the arrangement of an icon near two lines has a quickly input.

5.3 Conclusion of Subproject-4

This section describes a new password input interface using icons familiar to primary school children, and its evaluation by varying parameters such as numbers of icons and selection time for each icon. In future work, the number of icon displays and the input times of icons will be evaluated in more detail.



	2A (1)	2A (2)	2B (1)	2B (2)
▨ 8 Button	19.44	13.54	17.29	22.95
■ 12 Button	31.33	18.89	37.75	25.65
□ 16 Button	25.98	17.13	43.06	35.91

Figure 5-7: Average of Input Time.

Acknowledgements

These works were supported in part by the Research Grant-in-Aid for Private University of MEXT.

References

[1] Takao Nishitani, "TOPS DSP Applications for Future Cellular Phones", IEEE Proc. MWSCAS04, July 2004.

[2] T. Nishitani, et al., "Parallel Video Signal Processor Configuration based on Overlap-Save Technique and Its VLSI Element: VISP", Kluwer Academic, J. VLSI Signal Processing, Vol. 1, No. 1, 1988.

[3] Kyo, et al, "A 51.2GOPS Scalable Video Recognition Processor for Intelligent Cruise Control based on a Linear Array of 128 4-Way VLIW Processing Elements", IEEE J.SSC, Vol.38, Nov. 2003.

[4] H.Terada, S. Miyata and M. Iwata, "DDMP's: Self-Timed Super-Pipelined Data Driven Multimedia Processors", Proc. IEEE, Vol.87, No.2. Feb. 1999.

[5] S. Blake, D. Black, M. Carlson, et al., "An Architecture for Differentiated Services," RFC 2475, Dec. 1998.

[6] Aki SHODA, "Efficient Algorithm for the Secret Sharing Scheme", The graduation thesis of Kochi University of Technology, 2001. (in Japanese)

[7] Sekiji FUNAHASHI, "Implementation of an archive command using Secret Sharing Scheme", The graduation thesis of Kochi University of Technology, 2001. (in Japanese)

[8] Nao YAMAMOTO, "Implement of Archive Command That is Used SSS with 2's Extension Field (Implement Version.)", Especially Research of Kochi University of Technology, 2003. (in Japanese)

[9] Eizi OKAMOTO, "Introduction to Dryptography the 2nd Edition", pp127-149, Kyoritsu Publication Corporation, 2002. (in Japanese)

[10] "About Extension Field",

http://www.ccad.sccs.chukyo-u.ac.jp/˜mito/syllabi/daisu/fext/#TOP. (in Japanese)

[11] M. Umeda, "Advances in recognition methods for handwritten Kanji characters," IEICE Trans. Inf. & Syst., Vol. E 79-D, No. 5, pp. 401-410, 1996.

[12] J. Tsukumo, "Handprinted Kanji OCR development — What was solved in handprinted Kanji character recognition? —," IEICE Trans. Inf. & Syst., Vol. E 79-D, No. 5, pp. 411-416, 1996.

[13] Y. Kimura, T. Akiyama, M. Mori, N. Miyamoto, T. Wakahara and K. Ogura, "Hybrid recognition method for handwritten Kanji/non-Kanji characters using extended peripheral direction contributivity features and contour features," IEICE Trans. D-II, Vol. J82-D-II, No. 12, pp. 2271-2279, 1999.

[14] Ministry of Education, Culture, Sports, Science and Technology, "Computerization of school education' which greeted the turning point from the Millennium Project," http://www.saip.ne.jp/ogura/monbusho/ (in Japanese)

[15] Ministry of Education, Culture, Sports, Science and Technology, "Results of an investigation about the actual condition of the information education in a school etc., " http://www.mext.go.jp/a_menu/shotou/houdou/ (in Japanese)

[16] Takahiko Mendori, Miki Kubouchi, Minoru Okada, Akihiro Shimizu, "Password Input Interface Suitable for Primary School Children," Proc. of International Conference on Computer Education 2002, pp.765--766, New Zealand, 2002.

[17] Takahiko Mendori, Miki Kubouchi, Natsuko Ikenoue, Akihiro Shimizu, "A Study of Password Input Method Using Icons Suitable for Primary School Children," Journal of Japanese Society of Information and Systems in Education, Vol. 20 No. 2, pp.160--169, 2003. (in Japanese)