TDES CODER USING SSE2 TECHNOLOGY

In-Hoi Koo[1], Tae-Hoon Kim[2], Sang-Il Ahn[1]

Ground System Development Department, Korea Aerospace Research Institute[1]
freewill@kari.re.kr[1], siahn@kari.re.kr[1]
SOLETOP Inc. Satellite Image Dept.[2]
freekid99@soletop.com[2]

ABSTRACT: DES is an improvement of the algorithm Lucifer developed by IBM in the 1977. IBM, the National Security Agency (NSA) and the National Bureau of Standards (NBS now National Institute of Standards and Technology NIST) developed the DES algorithm. The DES has been extensively studied since its publication and is the most widely used symmetric algorithm in the world. But nowadays, Triple DES (TDES) is more widely used than DES especially in the application in case high level of data security is required. Even though TDES can be implemented based on standard algorithm, very high speed TDES codec performance is required to process when encrypted high resolution satellite image data is down-linked at high speed.
In this paper, Intel SSE2 (Streaming SIMD (Single-Instruction Multiple-Data) Extensions 2 of Intel) is applied to TDES Decryption algorithm and proved its effectiveness in the processing time reduction by comparing the time consumed for two cases; original TDES Decryption and TDES Decryption with SSE2

KEY WORDS: DES, TDES, SIMD, SSE2,

1. INTRODUCTION

The acquired image data via satellite can be encrypted for transmission to ground or space for data security according to its data characteristics like commercial or military and so on. For encryption in satellite image data, Triple DES [2] scheme based on DES [1] is used.

In case of both low rate and small volume of data, the generic TDES can meet the speed performance requirement as well as functional requirement.

But as high resolution earth observation satellite is more common, the very high speed performance for TDES decryption is required when TDES encryption is used for high speed downlink transmission.

In this paper, the Streaming SIMD (Single-Instruction Multiple-Data) Extensions 2(hereafter Intel SSE2) Technology was applied for TDES algorithm. SSE2 uses the SIMD technology in which single instruction applied to multiple data. Input data was re-arranged to be in parallel and then SSE2 was used for parallel data processing for increasing the processing performance in TDES decryption.

2. TDES ALGORITHM

This section provides short description of TDES covered in this paper to help reader's understanding.

TDES adopts the concept of 3-times of serial DES.

DES is an improvement of the algorithm Lucifer developed by IBM in the 1977. IBM, the National Security Agency (NSA) and the National Bureau of Standards (NBS now National Institute of Standards and Technology NIST) developed the DES algorithm. The DES has been extensively studied since its publication and is the most widely used symmetric algorithm in the world. But nowadays, Triple DES (TDES) is more widely used than DES especially in the application in case high level of data security is required.

DES encryption and decryption show symmetric structure as shown in Figure 1 using 56-bit key for 64-bit data.

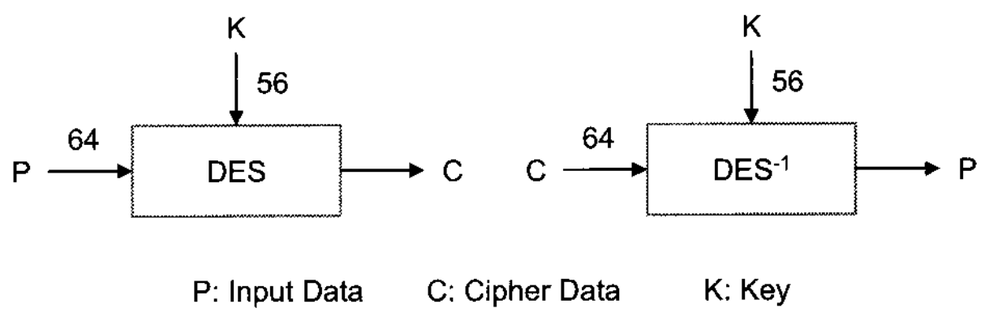

Figure 1 DES Structure

64-bit input data is separated as Left 32bits and Right 32bits in DES encryption as shown in Figure 2. 16 Times of iteration for Exclusive OR and Function (hereafter F). This F includes Extension, Exclusive OR, S-Box, and Permutation.

3. TDES PROCESSING IMPROVEMENT METHODS

For SSE2 application in TDES decryption, the encrypted input data is parallelized for better processing performance.

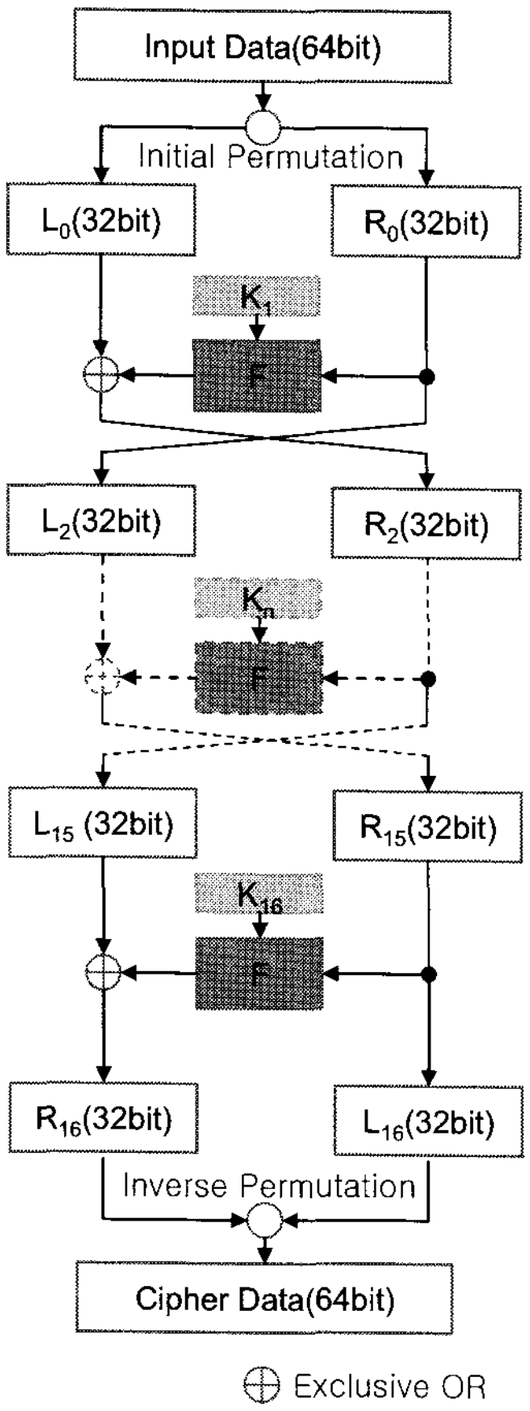

Figure 2 DES Algorithm

3.1 Description of SSE2

SIMD [4] is the one of three performance enhancement factor in MMX technology. With the help of this, just single instruction can be used for iterative loop with multiple instructions.

For example, the 8 byte data can be processed by 8 times of 1 byte data operation but 8 byte data can be processed by 1 time instruction with SIMD as shown in Figure 4.

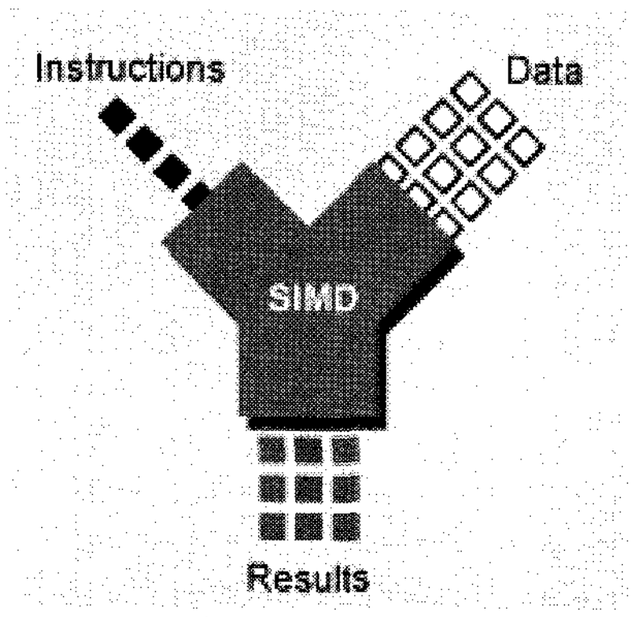

Figure 3 SIMD

SSE2 is extended technology for SIMD and Intel applied this technology into P-4 since Nov, 2000. SSE2 includes new 144 instruction commands using SIMD technology and both 128-bit length integer and float instruction command were added.

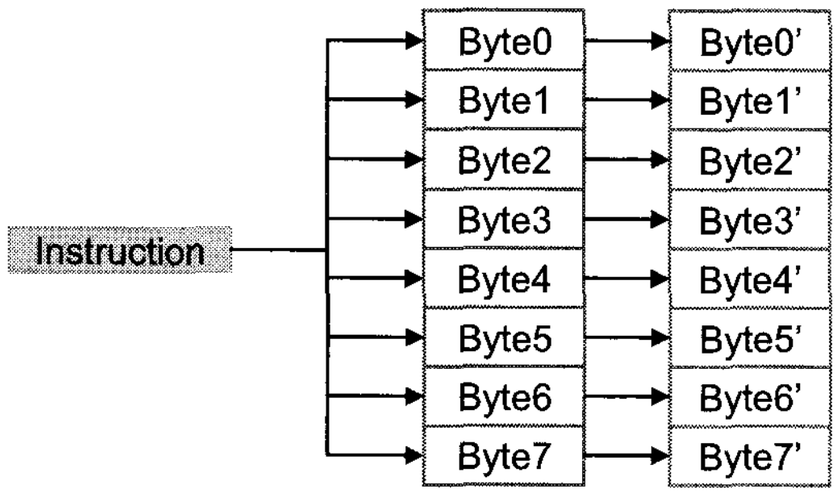

Figure 4 SIMD Processing

3.2 Parallel Composition of Input Data

DES performs encryption and decryption independently for 64-bit block regardless of operation mode like Electronic Codebook (ECB) mode, the Cipher Block Chaining (CBC) mode, the Cipher Feedback (CFB) mode, and the Output Feedback (OFB)

DES divides 64-bit block into Left32bits and Right32bits and process independently and performs Exclusive OR at the last round.

Considering this, 4 of 64-bit block data can be arranged to be input for parallel processing as shown in Figure 5. That means 4 of Left32bits can be input to one XMM register and 4 of Right32bits into other XMM register.

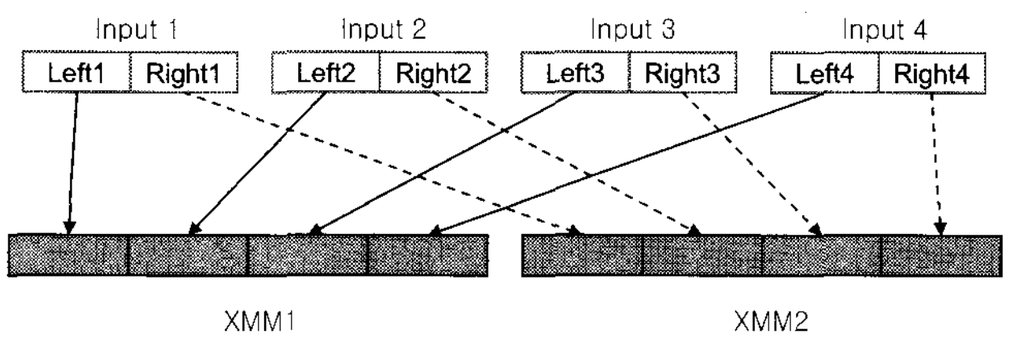

Figure 5 Input data re-arrangement

Parallelized input data of 4 x Left32bits or 4 x Right32bits can be processed at a time using SSE2 instruction. Therefore, 4 of 64-bit block can be processed using 128-bit XMM register in SSE2.

3.3 Application of SSE2 Instruction

DES algorithm includes 16 times of iteration and most frequently used operation includes Exclusive OR, Logical Shift Left, Logical Shift Right. Dedicated 32-bit instruction command for Exclusive OR, Logical Shift Left, Logical Shift Right operation is available and data arranged in parallel can be processed at a time. Therefore, the processing performance was enhanced by optimizing the number of operation/instruction command in iterative 16 times of round operations.

3.3.1 Use of PXOR Instruction

PXOR[5] instruction performs Exclusive OR for 32-bit in XMM in Figure 6.

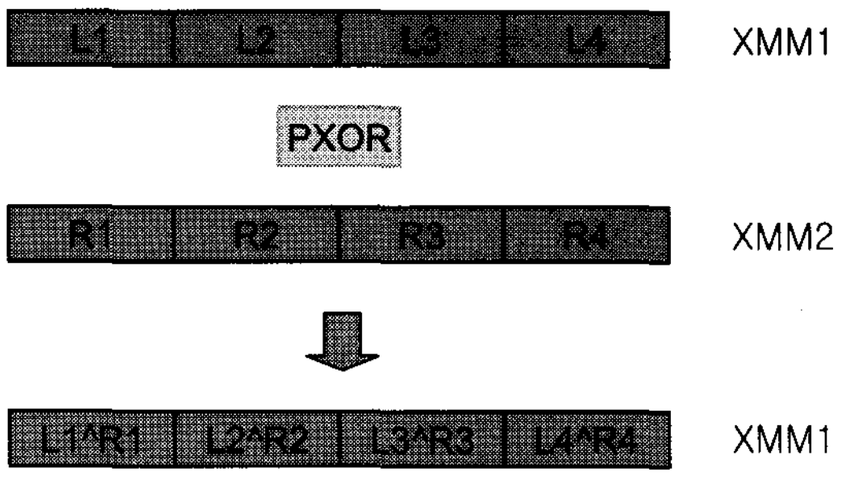

Figure 6 PXOR

Normally for this operation, 4 times of individual iteration is required for 32-bit data but in SSE2 128-bit data can be processed at a time.

3.3.2 Use of PSRLD and PSLLD Instruction

The PSRL[5] (Packed Shift Right Logical) instructions shift the bits of the first operand to the right by the amount of bits specified in the count operand. The result of the shift operation is written to the destination register. The empty high-order bits are set to zero.

The PSRLD 2 instructions shift the 2bits of the first operand to the right for 32-bit data as shown in Figure 7.

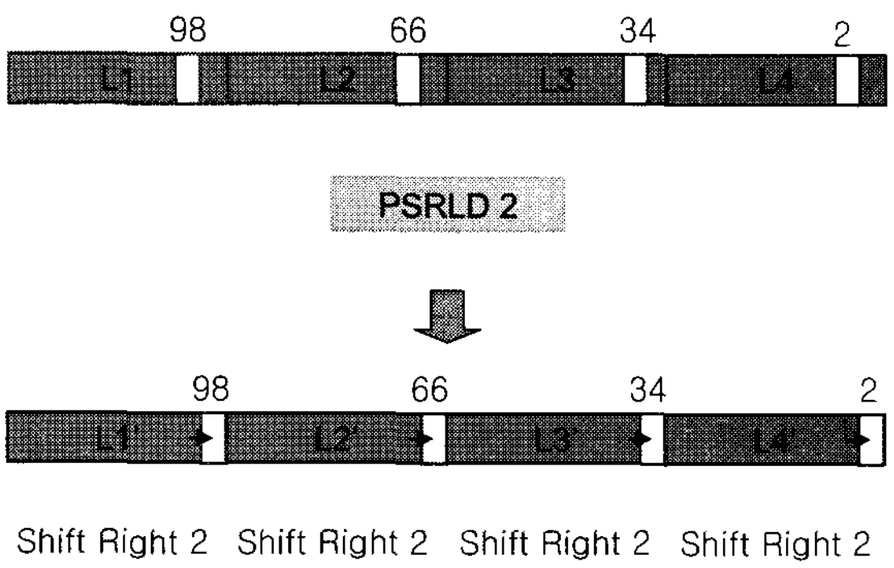

Figure 7 PSRLD

The PSLL[5] (Packed Shift Left Logical) instructions shift the bits of the first operand to the left by the amount of bits specified in the source operand. The result of the shift operation is written to the destination register. The empty low-order bits are set to zero. The PSLLD 2 instructions shift the 2bits of the first operand to the left for 32-bit data as shown in Figure 8.

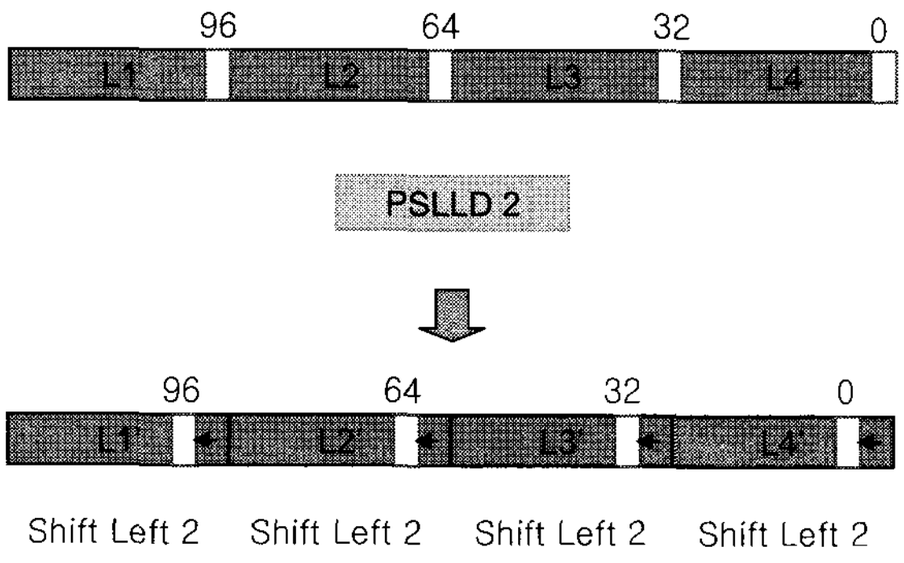

Figure 8 PSLLD

Using PSLRD and PSLLD with PXOR Instruction, 128bits data (4*32bit) can be processed simultaneously.

4. RESULTS

The processing time consumed for TDES decryption of 100,000 to 490,000 times for normal algorithm and for SSE2 application and its results was summarized in Table 1. As shown in Table 1, the SSE2 case shows 2.5 times higher speed than normal scheme even though we can expect 4 times higher speed at best in SSE2 case due to its feature, 1 instruction for 4 of 64-bit data block, This came from the characteristic of S-Box processing algorithm in F.

Count	Not-applied SSE2 (msec)	Applied SSE2 (msec)
100,000	498.498016	192.807373
150,000	747.31842	290.708466
200,000	994.699951	385.319244
250,000	1239.686401	484.420807
300,000	1488.406982	578.009888
350,000	1735.293701	683.428223
400,000	1994.971802	779.131287
450,000	2241.342285	877.369263

Table 1 Processing Time

The PC specification used for test is as follows;

- CPU: Intel(R) Pentium(R)4 3.2GHz
- Memory: 1.5GB
- OS: Windows XP

Figure 9 shows the processing time obtained for two test cases.

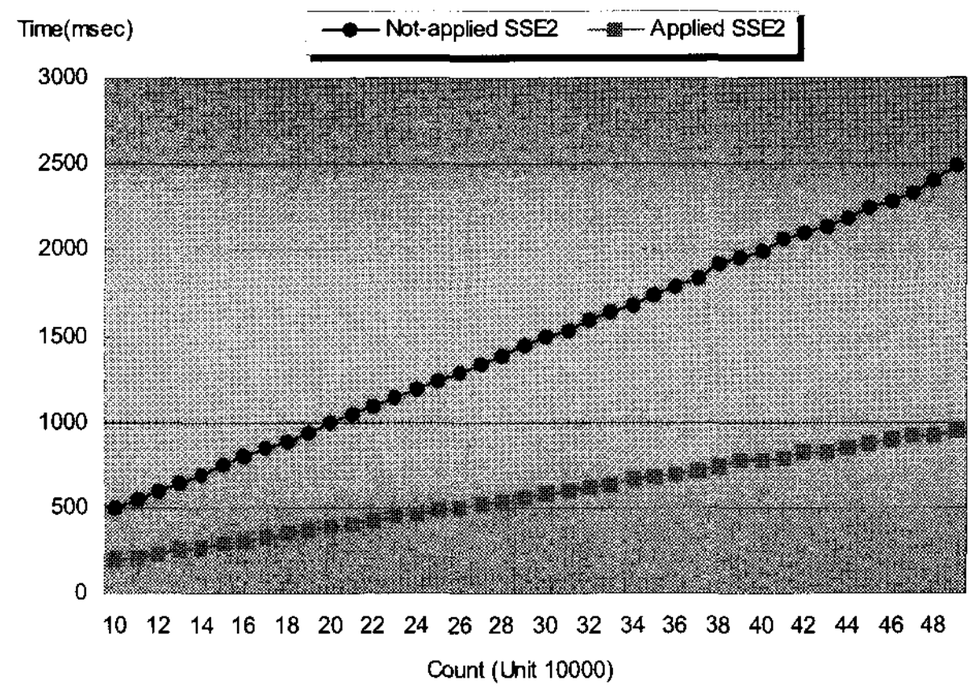

Figure 9 Processing Time

5. CONCLUTION

High resolution satellite image data usually requires high speed downlink and adopts encryption like TDES for data security. For quick processing, the dedicated hardware for TDES decryption can be used with high performance computing hardware but it is normally expensive. But, by adopting the new technology like

SSE2 in processing algorithm routine, both cost effective and powerful performance can be met. In this paper, SSE2 shows 2.5 times better performance.

SSE2 technology continuously evolves into more powerful function for SSE3 and SSE4. When we apply this kind of latest technology, the TDES decryption performance may be evolved.

The SSE2 scheme in this paper can be also applied to recent block encryption technology like AES and IDEA.

6. REFERENCES

[1] FIPS Publication 46-3, "Data Encryption Standard (DES)." U.S. DoC/NIST, October 25,1999.

[2] NIST, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Special Publication 800-67.

[3] DES algorithm, fast and compact, written by Richard Outerbridge in 1991

[4] The Software Vectorization Handbook, Aart J.C.Bik

[5] IA-32 Intel® Architecture Software Developer's Manual Volume 2A: Instruction Set Reference, N-Z