2011년 2월
석사학위논문

디지털 홀로그램을 이용한 DES 알고리즘의 암호성능 개선

조선대학교 대학원

컴퓨터공학과

노 창 오

디지털 홀로그램을 이용한 DES 알고리즘의 암호성능 개선

Improvement of Cipher Performance in DES Algorithm using Digital Hologram

2011년 2월 25일

조선대학교 대학원

컴퓨터공학과

노 창 오

디지털 홀로그램을 이용한 DES 알고리즘의 암호성능 개선

지도교수 조 범 준
공동지도교수 문 인 규

이 논문을 공학 석사학위신청 논문으로 제출함.

2010년 10월

조선대학교 대학원

컴퓨터공학과

노 창 오

노창오의 석사학위논문을 인준함.

위원장 조선대학교 교수 李 俊 (인)

위 원 조선대학교 교수 金忠源 (인)

위 원 조선대학교 교수 趙範峻 (인)

2010년 11월

조선대학교 대학원

목 차

표 목 차

그 림 목 차

ABSTRACT

Improvement of Cipher Performance in DES Algorithm using Digital Hologram

Chang-Oh Noh
Advisor : Prof. Beom-Joon Cho, Ph. D.
Co-advisor : Prof. Inkyu Moon, Ph. D.
Department of computer Engineering
Graduate School of Chosun University

Electrical, electronic and computer industries by developing personal and business use of electronic devices is increasing rapidly. National administration, finance, healthcare, education, welfare and community throughout the computerized systems were introduced.

But the computer H/W due to the development of information security concerns have increased. Accordingly, various encryption algorithms have appeared. But with the development of the computer attempts to cracking was frequent, which the DES algorithm, the algorithm is vulnerable to brute-force attack has become. The length of the secret key is limited to 56Bits the system is vulnerable to brute-force attack is abandoned. To resolve this problem, increase the length of the secret key of DES should be considered measures.

In this paper, 2 DES, 3 DES, unlike in the other algorithms can be used to mix and arrange a way to investigate. So, by applying the private key of the digital holograms is proposed to increase the length. For digital holographic images or holograms to create three-dimensional object out of the data in the form of white noise is produced. Use this information for the three-dimensional

objects can be extracted, and the hologram itself is composed in the form of white noise represents the effect of encryption. 64bits of data for each pixel of a hologram that is composed of complex data. DES process before applying the hologram length of the secret key is used to increase to 184bits.

Thus, due to the convergence of the hologram and the DES D (H (p, k1), k2) to create structure out of the way encryption is proposed.

I. 서 론

1. 연구배경 및 목적

전기/전자 및 컴퓨터 산업의 발달로 개인과 기업의 전자기기의 사용이 비약적으로 늘어났고, 초고속/광대역 통신망 및 인터넷의 발달로 인해 대용량의 정보를 매우 빠른 시간에 전송 및 수신이 가능하게 되었다. 이러한 이유로 국가의 행정업무, 금융, 의료, 교육, 복지 등 사회 전반에 걸쳐서 전산시스템이 도입되었다. 하지만 컴퓨터 성능의 발달로 인해 업무에 사용되는 정보에 대한 불법 복제 및 악용이 그 어느 때보다 손쉽게 이루어지고 있다. 따라서 개인과 기업의 정보보안에 대한 관심도 증가하게 되었다. 즉, 전산시스템에 대한 전산/정보보안은 필수 요건이 되었다. 이러한 보안 문제로 인해 다양한 암호학 이론- DES, RSA, RSH, AES 등 - 이 개발 되었다.

일상생활 속에 쓰이는 암호화 알고리즘 중에서 DES 알고리즘은 대칭 암호화 방식이다. 암호화를 할 때의 키와 복호화를 할 때의 키가 같은 암호화 알고리즘이다. 컴퓨터 산업이 발전되기 이전의 대칭형 이라고 할 수 있는 암호화 방법들은 단순한 방법으로 암호화를 하였다. 예를 들어 시저 암호방식은 암호화 할 때와 복호화 할 때의 몇 글자를 밀려 썼는지가 암호화키가 되고, 비즈네르 알고리즘은 키워드로 사용한 secret is beautiful이 암호화키가 된다.

현재 사용되고 대칭암호화 방식들은 암호화 성능을 측정하기 위해서는 혼돈과 확산이라는 개념을 알아야한다. 혼돈은 암호문의 통계적 성질과 평문의 통계적 성질의 관계를 난해하게 만드는 성질로써 입력 데이터의 비트가 암호문에 영향을 미치는지 알아보는 단계이다. 단일 대칭 암호화 방식은 이러한 혼돈이 부족했기 때문에 통계적 분석을 통해서 쉽게 복호화가 가능했다. 확산은 각각의 평문 비트와 각 비트가 암호문의 모든 비트에 영향을 주는 성질이다. 단일 대칭 암호화방식은 키워드를 사용할 때 일부 문자에만 키가 영향을 미침으로 확산 기능도 약하다. 현대 암호화 알고리즘은 이 혼돈과 확산 기능이 필수적으로 강하게 나타난다.

혼돈과 확산이 표현된 암호화 알고리즘이 강력한 암호화 알고리즘이며, 두가

지를 측정하는 방법으로 쇄도효과(Avalanche Effect)를 이용할 수 있다. DES 알고리즘은 강력한 쇄도효과가 나타나는 알고리즘으로써 인정받았고, 단순한 비트 연산만을 이용하여 처리되기 때문에 속도 면에서도 빠르다고 인정받고 있다.

이와 같은 DES 알고리즘은 컴퓨터 성능이 발전하면서 비밀키의 길이가 짧다는 문제점이 발생하였다. 그래서 비밀키의 길이를 확장하는 방법이 필요하여 2중 DES, 3중 DES 방법이 사용되었다.

본 논문에서는 광학분야에서 사용하는 디지털 홀로그램을 이용하여 DES의 비밀키를 확장하려고 한다. 디지털 홀로그램은 2차원 혹은 3차원 정보에 대한 기록이 가능하며, 컴퓨터상에서 가상광학 기법을 통해 구현이 가능하다. 따라서 대칭형 암호화 알고리즘에서의 DES에 대하여 알아보고 DES의 취약점을 찾아서 이를 디지털 홀로그램을 이용하여 보완하는 알고리즘을 제안한다.

2. 연구내용 및 방법

블록암호화 기법인 DES의 알고리즘은 1971년 미국 NIST(Nat- ional Bureau of Standards)에 의해 표준으로 제정 되었다. 하지만 일부 취약키(Weak Key)들의 생성과 무차별 대입공격(Brute force attack) 때문에 보안 강도가 높았던 DES알고리즘이 전수키 공격에 취약함이 발견되었다. 전수키 공격에 대한 취약점을 보강하기 위해 2중DES, 3중DES와 같은 방법론이 나왔지만 여전히 DES의 원천적인 전수키 공격에 대한 해결책은 만들어지지 않고 있다.

전수키 공격(Brute force attack)은 암호화 알고리즘의 비밀키 길이에 따라 취약성 정도가 달라진다. 암호문을 만들기 위한 비밀키의 길이가 작아지면 작아질수록 전수키 공격에 약한 성격을 보인다. 따라서 전수키 공격에 강인한 상태의 암호화 알고리즘을 만들려면 비밀키의 길이를 길게 하여야 한다.

따라서 전수키 공격에 취약한 DES의 성능을 늘리기 위해 디지털 홀로그램을 적용한다. 3차원 영상획득 기술인 디지털 홀로그램(Digital Hologram)은 영상보안 부분에서 응용될 수 있는 기술로서 최근 많은 연구가 이루어지고 있다. 디지털 홀로그램 기술은 원 영상에 랜덤 한 위상 값을 곱한 후 가상광학을 이용하여 컴퓨터상에서 프레넬 전파시켜 원 영상을 백색 잡음(White Noise) 형태로 변환시켜 암호화하는 방법으로 전파거리와 빛의 파장에 따라 다양한 패턴이 생성된다.

제안하는 방법에서는 평문의 행렬을 프레넬 전파 시켜 생성된 디지털 홀로그램으로부터 각 원소에 대한 64개의 위상 값을 사용하여 64bits DES 라운드키를 생성한다. 생성된 라운드키는 디지털 홀로그램의 고유 위상정보이기 때문에 DES 키가 노출된 경우에도 평문의 복호화가 매우 어렵게 된다. 즉, 디지털 홀로그램 패턴 생성과정 사용한 정확한 광학적 파라미터(전파거리, 빛의 파장)를 알지 못하면 정확하지 않는 디지털 홀로그램 패턴이 나타나게 되며, 평문으로의 복원이 되지 않는다.

DES 블록대칭암호화 알고리즘은 단순한 함수를 반복적으로 적용하여 암호학적으로 강한 함수를 만드는 과정을 통해 개발이 된다. 즉, 반복되는 라운드 함수와 라운드 키를 이용하여 단순 반복 연산을 하게 된다. 또한 수학적 계산이 없어서 수행속도가 빠르고 H/W와 S/W로 구현이 가능하다. 그리고 디지털 홀

로그램과 DES는 공통적으로 역변환이 가능한 대칭성 알고리즘이기 때문에 두 알고리즘의 결합이 가능하며, DES 비밀키가 노출되어도 디지털 홀로그램 패턴 생성 과정에서 사용한 광학 파라미터를 알지 못하면 평문 복원이 어렵게 된다.

본 논문의 구성은 1장의 서론에 이어 2장에서 기존에 사용되어진 DES와 디지털 홀로그램의 이론을 정리하여 암호학적 특징을 살펴보고, 디지털 홀로그램을 통한 3차원 영상 보안의 암호화 기법을 정리하여 보고 3장에서 디지털 홀로그램과 DES 암호화 알고리즘의 결합을 통해 기존과 차이점이 발생하는지 알아보고 전수키 공격에 강인한 이유를 알아보고 4장에서 실험결과를 통해 실제 이루어지는 결과들을 비교한다. 마지막으로 5장에서 결론을 맺는다.

II. 관련연구

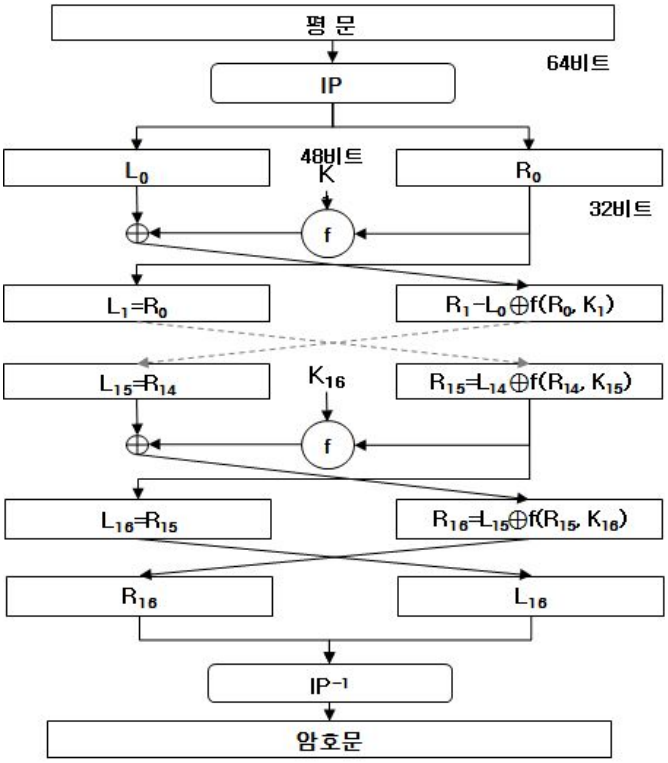
1. DES(Data Encrypted Standard)

DES는 1972년에 미국 NBS(National bureau of Standard)에서 정보보안을 위한 암호기술이 필요함에 따라 미국정부 규모의 표준적인 암호 알고리즘을 개발하기로 하여 개발하기 시작한 암호화 알고리즘이다. 그래서 1974년 8월 27일 IBM에서 루시퍼(Lucifer) 암호알고리즘을 제안하였다. 루시퍼는 민간에서 개발한 최초의 블록 암호들에 붙는 이름으로 IBM사의 호르스트 파이스텔에 의해 제작된 암호화 알고리즘이다. 최종적으로 NBS는 1975년 IBM사의 파이스텔 구조를 갖는 루시퍼 알고리즘을 개량하여 DES를 완성하여 국가 표준 암호화 알고리즘으로 지정하였다.

DES 알고리즘은 한 블록이 64bits로 구성이 되고 64bits의 비밀키로 동작하는 대칭형 블록 암호화 알고리즘이다. 반대로 복호화 하는 과정 또한 암호화 과정과 동일한 64bits의 비밀키로 복호화 되도록 구성되어 있다.

1) DES의 암호화 과정

DES는 입력 데이터의 초기 순열을 재배치 시키는 IP(Initial Permutation) 테이블, IP 테이블에 의해 재배치된 순열을 최초의 입력배열의 상태로 재배치하는 IP^{-1} 테이블, DES의 암호화 함수 역할을 하는 라운드 f(Function) 함수, 64Bits의 비밀키를 입력 받아 각 라운드에서 사용할 라운드 키를 생성하는 KS(Key Schedule) 과정, 라운드(Round)키 생성 시 키 스케줄링 과정에서 필요한 P(Permutation) 테이블과 S_i(Sbox) 테이블들을 이용하여 암호화 전체 과정을 처리한다.



[그림 2-1] DES의 암호화 과정

[그림 2-1]에서 입력 평문이 암호화 16라운드를 거치며 암호문이 생성되는 과정 이다. 최초의 입력 평문은 *IP* 테이블을 통하여 64bits로 구성된 평문 블록의 비트들을 전치시킨다.

IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

[그림 2-2] *IP* 테이블

IP 테이블을 통과한 비트들은 전치 과정을 통해서 새로운 입력 비트로 재 생성되고, 입력 평문의 블록과 다른 비트 조합이 만들어진다. 비트변환이 이루어진 입력 블록은 각각 32bits씩 나뉘어서 L(Left)과 R(Right)블록으로 분리된다. 이때 L은 입력 블록의 최초 32bits를 갖게 되고 R은 33번째 bit부터 마지막 64번째 bit를 갖게 된다.

분리된 R 블록은 f 함수라는 처리 과정을 거치게 되는데, 이 함수에서 48bits의 라운드 키 K_i와 결합이 이루어져 32bits의 결과 값을 갖게 된다. f 함수를 통해 만들어진 32bits의 결과와 L값이 서로 모듈러 연산이 이루어져 다음 라운드의 R값으로 저장이 이루어지며, 연산 전의 R값은 다음 라운드의 L값으로 저장이 된다. 이 과정을 통하여 DES 알고리즘의 한 라운드가 이루어진다. 식(2-1)이 한 라운드의 과정을 설명한 것이다.

$$\begin{aligned} L_{i+1} &= R_i \\ R_{i+1} &= L \oplus f(R, K_i) \end{aligned} \qquad (2\text{-}1)$$

DES는 동일한 라운드 과정을 총 16번을 수행하게 되며 가장 마지막 라운드에서는 L과 R블록을 한 번 교차시킨다.

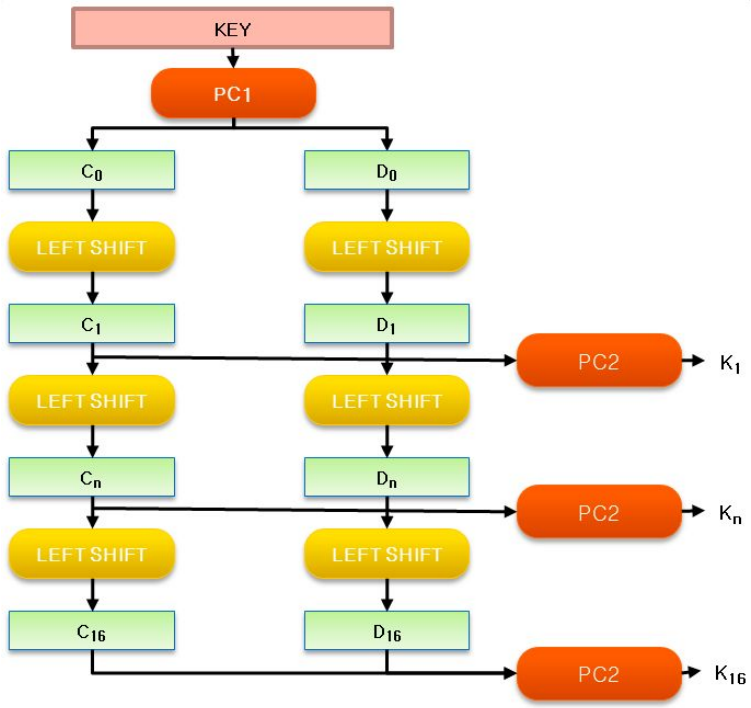
IP^1

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

[그림 2-3] IP^{-1} 테이블

최종 라운드를 통과한 데이터는 IP^{-1} 테이블을 지나며 입력 평문의 배치구조로 전치가 이루어진다. 라운드 과정을 모두 마친 평문은 DES 암호문 블록으로 구성이 되어 입력 평문 블록에 대한 암호 블럭이 완성이 된다. 즉, 64bits의 평문 바이너리 블록이 DES의 처리과정을 통과하면서 새로운 64bits의 암호문 블록으로 생성된다.

DES 암호문을 생성할 때 사용하는 라운드 키는 암호문 생성 시 부여받은 비밀키 K가 아니고 DES의 키 스케줄링 KS 과정을 통해서 만들어진 16개의 라운드 키 K_i 이다.



[그림 2-4] 라운드키 스케줄링 KS

[그림 2-4]에서 라운드키 스케줄링은 입력받은 비밀키 64bits를 48bits로 구성된 16개의 라운드 키 K_i 를 생성한다.

***PC*-1**

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

[그림 2-5] *PC*1 테이블

입력받은 비밀키 *K*는 *PC*1 테이블을 거쳐 56bits로 치환되어 진다. 이렇게 줄어든 비밀키 데이터는 *C*(Left)와 *D*(Right)로 분리된다. 분리된 *C*와 *D*는 각각 28bits로 구성되며, 각각의 *C*와 *D*는 *Left Shift* 테이블을 통해 비트 쉬프트 연산을 거치게 된다.

Iteration Number	Number of Left Shifts
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

[그림 2-6] Left Shift 테이블

[그림 2-6]의 *Left Shift* 테이블을 통해 각 라운드 별로 비트 쉬프트 연산을 거치며 비트의 위치가 변경이 된다. 변경된 각 C와 D는 다시 56bits로 결합이 이루어지며, 이 값은 $PC2$ 테이블을 통해 48Bits로 치환된다. 이 과정에서 쇄도 효과를 발생할 수 있도록 라운드키의 비트들의 입력 값을 바꾸게 된다.

PC-2

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

[그림 2-7] $PC2$ 테이블

[그림 2-7] 과정을 지나서 최종적으로 한 라운드 키 K_i 가 생성되며, 총 16번의 동일한 과정을 거쳐 16개의 라운드 키 $K_1 \sim K_{16}$ 이 생성된다.

따라서 키 생성과정은 식(2-2)와 같다

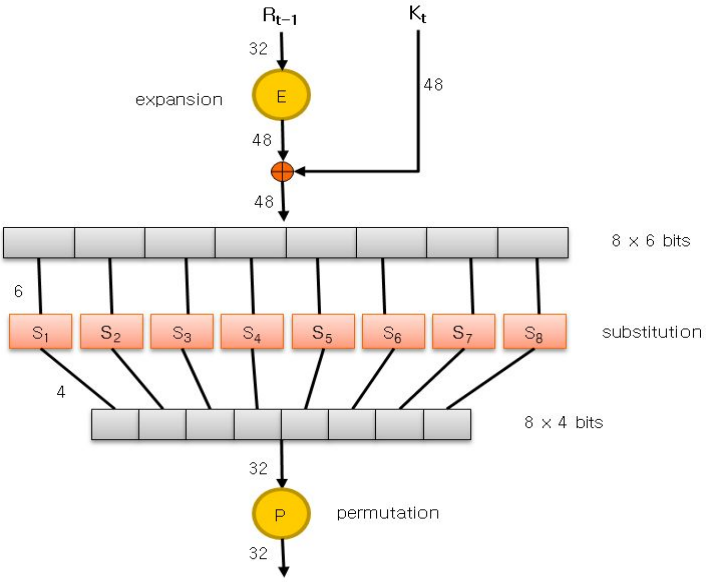
$$K_n = KS(n, K) \tag{2-2}$$

라운드 키 K_n은 키 스케줄링 KS를 통해 1~16의 n으로 처리되며 비밀키 K에 의해 생성됨을 알 수 있다.

키 스케줄링 과정을 통해 생성된 라운드 키 K_i 를 적용한 DES 알고리즘의 각 라운드 과정은 식(2-3)과 같다.

$$L_n = R_{n-1}$$
$$R_n = L_{n-1} \oplus f(R_{n-1}, K_n) \quad (2\text{-}3)$$

DES 암호화의 가장 중요한 부분을 차지하고 있는 부분이 f 함수이다. f 함수의 처리과정에서는 32bit의 키 데이터를 혼돈과 확산에 대한 방법을 이용하여 새로운 32bit의 결과를 만든다. 즉, 쇄도효과(Avalanche Effect)가 발생되는 부분이다. [그림 2-8]은 f 함수의 처리 과정이다.



[그림 2-8] f 함수 과정

f 함수는 [그림 2-8]과 같이 동작하며 E와 P 테이블, S Box 처리과정을 통과한다. 확산(E와 P 테이블)과 혼돈(S Box)을 보여주는 과정이다.

E BIT-SELECTION TABLE

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

[그림 2-9] E 테이블

f 함수로 입력받은 R 데이터는 E 테이블을 통하여 32bits에서 48bits로 치환이 되어 해당 라운드의 라운드 키 K_i 와 모듈러 연산을 거치게 된다.

S1

Column Number

Row No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

[그림 2-10] S Box의 인덱스 예시

이 과정에서 생성된 48bits의 데이터는 6bits씩 총 8개의 세부 블록으로 나뉘게 되는데, 각 6bits의 1번째와 6번째의 비트를 결합하고, 나머지 2번째부터 5번째까지의 4비트를 결합하여 2개의 정수 값을 만든다. 2개의 정수 값들은 각 S Box의 Row, Column 인덱스로 처리되어 4bits의 정수 값으로 변환이 된다.

P

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

[그림 2-11] P 테이블

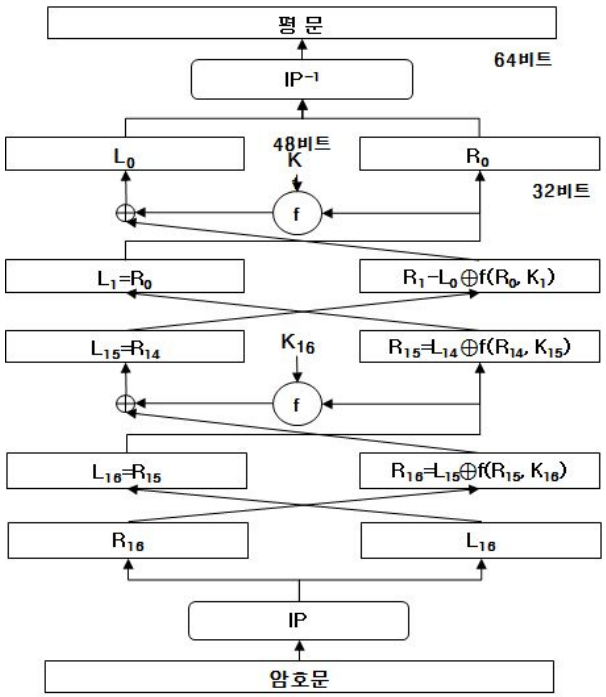
변환된 4bits로 구성된 정수의 비트들을 서로 연결하여 총 32 bits를 만들어 P 테이블을 통해 32bits를 전치시켜 f 함수를 종료한다.

$$f(R_{n-1},K_n) = P(S(E(R_{n-1})\oplus K_{n)}) \qquad (2\text{-}4)$$

결과적으로, f 함수를 통하여 각 라운드를 암호화하는 과정을 거치면 하나의 암호문이 나오는데 이는 보안상의 문제로 인해 16라운드라는 과정을 모두 거쳐 한다. DES 표준 문서에서는 16번의 라운드 과정을 거치는 것이 가장 안정적이라고 주장한다. 이유는 페이스텔 구조에서 규명되었다. 16라운드를 통하면서 평문의 비트가 최적으로 혼돈의 과정을 거친다. 이 전체 라운드를 거치고 나서 최종적으로 64bits로 결합을 하면 입력 평문 P에 대한 DES 암호문인 E 암호문이 생성된다.

2) DES의 복호화 과정

DES의 복호화 과정은 암호화 과정의 정 반대로 구성된다. 이는 대칭형 알고리즘의 특징으로 암호화 과정과 정반대로 복호화 과정이 이루어지는 성질을 이용하는 것이며, [그림 2-12]의 과정이다..



[그림 2-12] DES의 복호화 과정

$$R_{n-1} = L_n$$
$$L_{n-1} = R_n \oplus f(L_n, K_n) \qquad (2-5)$$

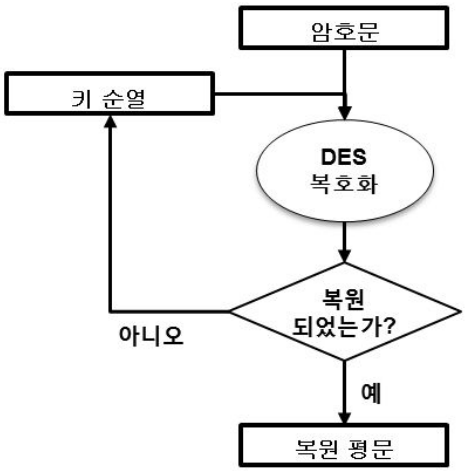
복호화 과정은 암호화 과정에 사용된 모든 16개의 라운드 키 $K_1 \sim K_{16}$가 사용되어 복호 과정이 이루어지는 것을 볼 수 있으며, 처리과정 또한 역변환 방법으로 암호문에서 평문으로 올라가는 것을 확인 할 수 있다. 이것이 대칭형 암호화 알고리즘의 특징인 대칭성이다. 즉, 암호화 과정의 역순이 복호화 과정이다.

3) DES의 전수키 공격에의 취약성

DES 암호화 알고리즘은 H/W의 성능의 향상으로 인해 전수키 공격(Brute force attack)에 취약한 특성을 나타낸다.

전수키 공격이란 암호화 알고리즘을 풀어내는 암호해독 기법으로 무차별 대입공격이라고도 일컫는다. 공격의 방법은 비밀키 길이의 한도 내에서 생성가능한 모든 비밀키 순열을 암호와 알고리즘에 일일이 적용하여 보는 기법이다.

전수키 공격은 두 가지 방법으로 나눌 수 있다. 먼저 하나의 암호문이 있을 때 모든 가능한 키를 대입하여 암호문이 평문으로 복호화 되는지 검사하는 방법과 한 평문과 그에 해당하는 암호문이 있을 때 모든 가능한 키를 대입하여 검사하는 방법이 있다. 이 방법의 단점은 이론적으로는 키를 찾을 수 있으나 실제적으로 계산복잡도, 즉 암호화 및 복호화 과정을 계속적으로 실행하여야 되기 때문에 시간상의 제약이 있고, 주어진 데이터가 암호문이라는 것만을 알고 있는 경우에는 키들을 대입하여 복호화 된 출력문이 실제로 찾으려는 평문인지 확인할 방법이 없다는 것이다. 또한 전수키 공격은 분석을 수행하는 컴퓨터의 계산능력과 비용대비 비밀키 탐색의 효율성도 고려해야 한다. S/W 구현은 가능하지만 키를 찾는 시간 제약 조건에 따라서 가능성을 구분할 수 있다.



[그림 2-13] DES의 전수키 공격

[그림 2-13]에서 DES 알고리즘에 대한 전수키 공격은 무차별적인 키 순열 대입을 통해 이루어지는 것을 확인할 수 있다. 이와 같이 모든 키 순열을 대입하여 암호를 해독하는 기법은 생성 가능한 키 순열의 양에 따라 해독 시간이 결정 된다. 즉, 생성 가능한 키 순열은 비밀키의 비트 수에 따라 다르게 나타난다. 키 순열의 선택은 바이너리 데이터이므로 2의 진수로 표현이 되며, 이는 키의 길이에 대한 지수의 형태로 순열이 만들어진다.

비밀키 비트 크기	가능한 비밀키 순열 갯수
8	2^8
56	$\mathbf{2^{56}}$
64	2^{64}
128	2^{128}
256	2^{256}

[표 2-1] 비밀키 크기와 키 순열의 관계

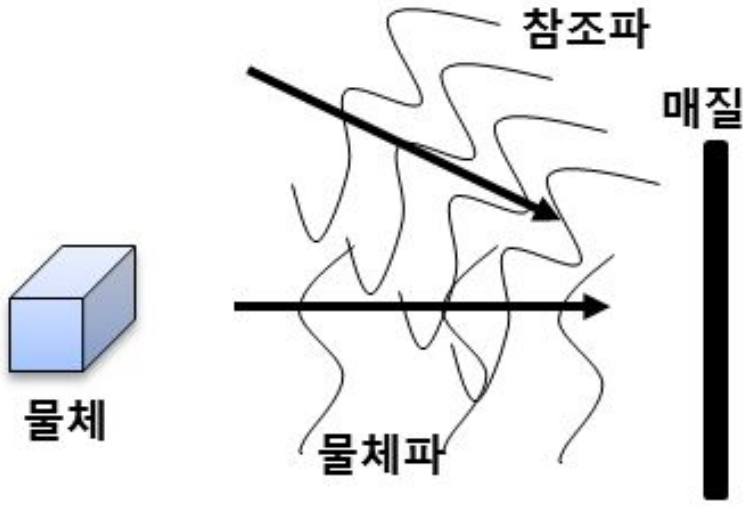
DES의 경우는 64bits의 키를 사용하지만 실제로 사용하는 비밀키 크기는 56bits이므로 [표 2-1]에서 나타내듯이 2^{56} 개의 비밀키 순열을 만들어 낼 수 있다. 따라서 상대적으로 작은 크기의 비밀키 순열이 나타난다.

이미 1977년에 Diffie와 Hellman이 하루 반 정도면 DES 키를 해독할 수 있는 전수키 공격 H/W를 개발 및 공개하였으며, 1993년에는 Weiner가 23시간이면 DES 키를 해독할 수 있는 H/W를 개발 및 공개하였다. 즉, H/W적으로 DES의 키를 해독하는데 하루가 채 걸리지 않는다. 성능이 발전된 현대의 컴퓨터를 이용하면 1900년대 보다 빠른 속도로 전수키 공격이 가능하다.

따라서 DES 암호화 알고리즘은 키 길이가 56bits로 매우 작기 때문에 전수키 공격에 매우 취약한 상태이다. 이를 보완하기 위해 디지털 홀로그램을 이용하여 비밀키의 길이를 늘리는 방법을 제안하였다.

2. 디지털 홀로그램(Digital Holography)

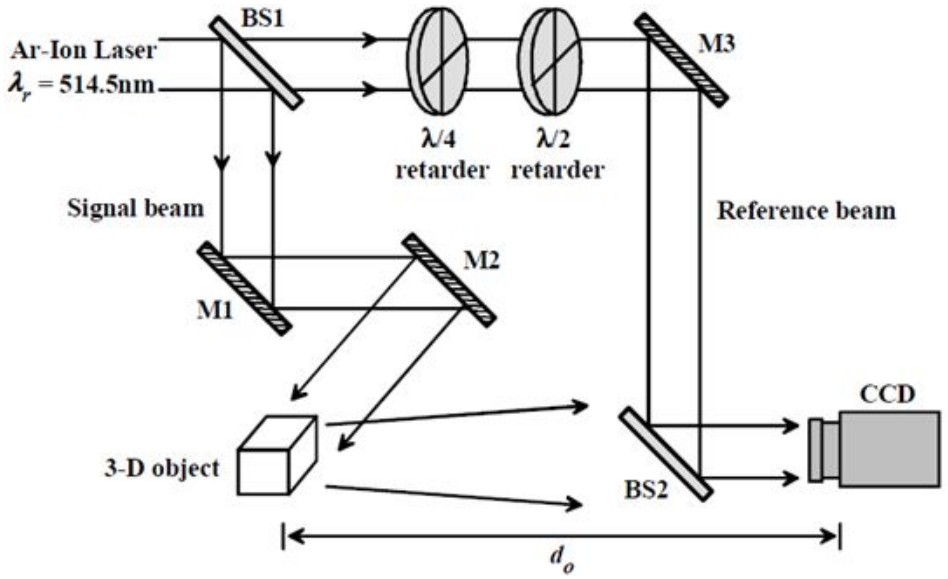
홀로그램이란 광학매질에 맺히는 특정 물체에 대한 파형에 또 다른 간섭 파형을 결합하여 만들어지는 일종의 일그러진 영상이다. 본 영상은 매질에 맺히는 일반적인 영상과 다른 형상을 하고 있으며 이 형태의 영상에서 3차원 영상데이터를 만들어내는 전반적인 과정을 디지털 홀로그램이라고 한다. 또한 매질에 맺힌 홀로그램은 물체에 대한 3차원 정보가 포함되어 있다.



[그림 2-14] 홀로그램의 획득 예

[그림 2-14]에서 홀로그램 데이터를 획득하는 간단한 예시를 나타내고 있다. [그림 2-14]에서 3차원 물체가 일정 거리에서 위치하고 있고 이 영상을 기록할 수 있는 매질이 존재한다. 여기에 물체의 파형이 아닌 또 다른 파형이 나타나게 되면 둘 사이에 간섭이 생겨 관찰하는 물체에 대한 화면이 기존의 이미지와는 다르게 일그러져 보이는 영상 데이터를 얻을 수 있는데 이것이 홀로그램 영상이다. 이 영상은 새로운 참조파에 대하여 이미지의 파장이 변형된 영상데이터로 표현이 된다.

이와 같은 홀로그램 데이터를 얻는 방법으로는 광학(Optics)기법과 가상광학(Virtual Optics) 기법 두 가지가 존재한다.



[그림 2-15] 광학을 이용한 홀로그램의 획득

첫째, 광학 기법으로 홀로그램 영상데이터를 추출하는 방법은 [그림 2-15]의 기구를 이용하며, 간섭계와 파장을 조절할 수 있는 레이저광선, 반사경 그리고 획득할 영상과 매질간의 전파거리를 설정하여 CCD에 맺히게 한다.

광학 장치에서 홀로그램 영상을 획득하는 기법은 CCD 카메라의 평면에 지연계(retarder) 2개를 부착시켜 0, $-\pi/2$, $-\pi$ 그리고 $-3\pi/2$의 4개의 영상을 통해 홀로그램데이터를 입력받는다. 이 과정을 통하여 3차원 영상 객체의 3차원 데이터를 획득 할 수 있다. 또한 3차원 영상 객체를 $U_O(x_0, y_0 : z)$라고 하면 CCD 카메라의 렌즈에 맺히는 영상은 식(2-6)과 같다.

$$U_H(x,y)=\iiint_{d_0-\triangle/2}^{d_0+\triangle/2}\exp[j2\pi z/\lambda_r]/(j\lambda_r z)\exp[j\pi(x^2+y^2)/\lambda_r z]\times U_O(x_0,y_0;z)\exp[j\pi(x_0^2+y_0^2)/\lambda_r z]\exp[-j2\pi(xx_0+yy_0)/\lambda_r z]dzdx_0dy \quad (2\text{-}6)$$

식(2-6)은 프레넬 전파를 통하여 홀로그램 영상을 획득하는 방법으로써 d_0는 물체와 CCD사이의 전파 거리, △는 z 축의 값에 해당한다.

입력 영상의 위상 정보는 :

$$A_H(x,y)\exp[j\Phi_H(x,y)] \quad (2\text{-}7)$$

로 표현이 가능하다.

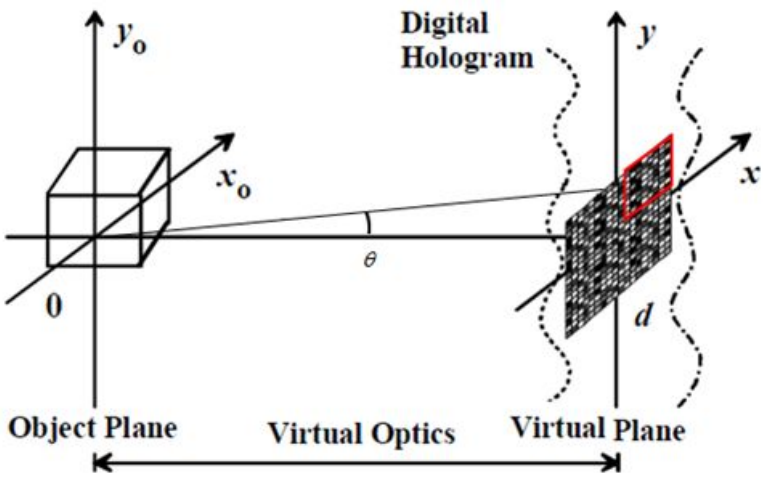
$A_H(x,y)$는 광선에 해당하며 $\exp[j\Phi_H(x,y)]$는 [0, 2π]의 간섭데이터이다. 본 과정을 통하여 가우시안 백색 잡음(white noise)이 생성되어 본래의 영상은 위상이 변형된 홀로그램으로 구성된다.

CCD 평면상에 표시되는 참조파는 :

$$R(x,y;\alpha)=A_R\exp[j(\phi_R+\alpha)] \quad (2\text{-}8)$$

의 형태를 갖으며, A_R과 ϕ_R은 위상의 참조파 값이 된다.

[그림 2-15] 과정을 거쳐 홀로그램 영상을 얻을 수 있으며, 이렇게 얻어진 홀로그램 영상을 가공하여 전산 시스템에 처리 과정을 나타낸 것을 가상광학(Virtual Optics)라고 한다.



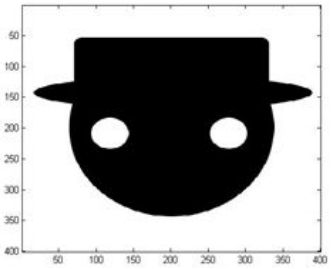
[그림 2-16] 가상광학을 이용한 디지털 홀로그램 획득

가상광학은 [그림 2-16]처럼 컴퓨터상에서 가상으로 물체의 이미지가 있다고 가정하고 가상의 CCD 평면(가상 평면)에 맺히는 물체의 홀로그램 데이터를 획득하는 기법이다. 즉, 원본의 이미지에 참조파(Reference Wave)와 임의의 위상키 값을 이용하여 원본이미지의 위상을 변형하고 이를 컴퓨터상에서 처리하기 위해 FFT(Fast Fourier Transform)를 이용하여 2차원 DFT(discrete Fourier Transform)을 함으로써 계산된다. 가상광학 방법으로 얻은 디지털 홀로그램은 부착된 랜덤 위상키로 인해 전파 거리에 상관없이 백색잡음 형태로 변환된다.

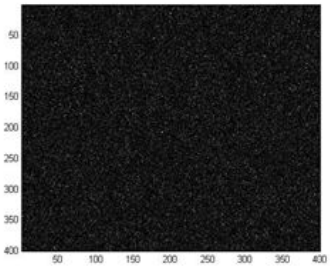
$$U_H(x_h, y_h) = \frac{\exp(j2\pi d_h/\lambda)}{j\lambda d_h}\exp\{j\frac{\pi}{\lambda d_h}(x_h^2+y_h^2)\}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}U_O(x,y)\exp\{j\phi_O(x,y)\}\times \exp\{j\frac{\pi}{\lambda d_h}(x^2+y^2)\}\exp\{-j\frac{2\pi}{\lambda d_h}(xx_h+yy_h)\}dxdy \quad (2\text{-}9)$$

식(2-9)의 λ는 참조되는 파장을 나타내며, d_e는 전파거리에 해당한다. 참조되는 파장과 전파거리를 이용하여 디지털 홀로그램의 참조파에 대한 가상의 데이터를 만들고, 이를 원본의 영상과 결합하는 처리과정을 통해 가상광학을 이용한 디지털 홀로그램이 만들어진다.

그 결과 [그림 2-17] 영상이 나오게 된다.



(a) 원본 이미지



(b) 생성된 백색잡음 형태의 홀로그램 영상

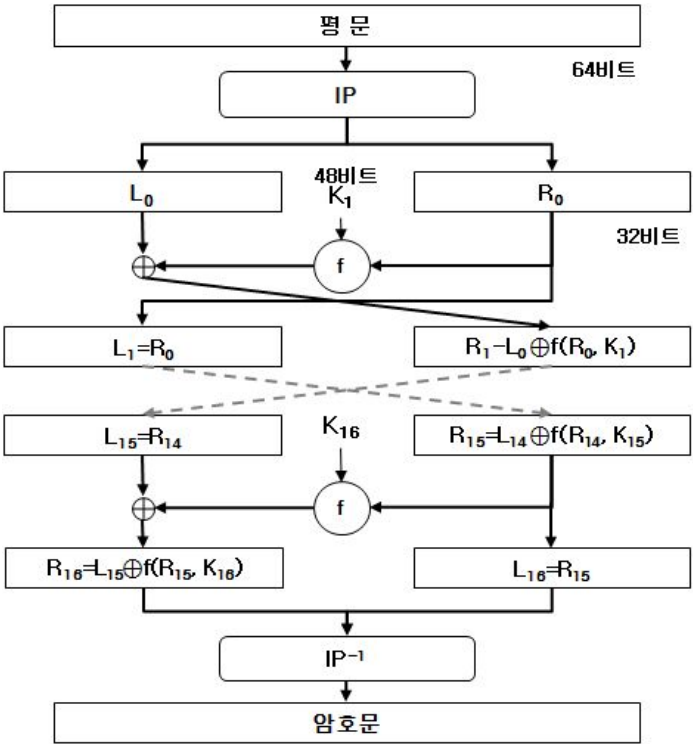
[그림 2-17] 원본 영상과 디지털 홀로그램 영상

(b) 형태로 디지털 홀로그램이 생성이 되고, 홀로그램 영상을 원래의 영상으로 복원을 하면 (a)와 같이 본래의 이미지와 깊이가 저장된 이미지가 된다.

III. 디지털 홀로그램을 이용한 DES의 성능개선

1. DES 알고리즘의 취약성

DES는 블록대칭암호화기법의 암호화 알고리즘이다. 한 블록당 크기는 64bits이며, 블록을 반복 사용한다. 이는 64bits(실 56bits)의 보안키를 이용해 만들어진 16개의 라운드 키를 사용하여 16라운드의 과정을 거치며 비트 치환, 전치 과정을 통하여 본래의 비트의 손실 없이 암호화 가능한 알고리즘이다. [그림 3-1]에서의 16라운드의 과정을 통해 암/복호화가 이루어진다.



[그림 3-1] DES의 암호화 과정

DES는 1개의 암호화 키를 이용하여 16개의 각 라운드 키를 생성하고, 각각 라운드마다 적용하여 비트 치환, 전치 처리를 하며 암호화 한다.

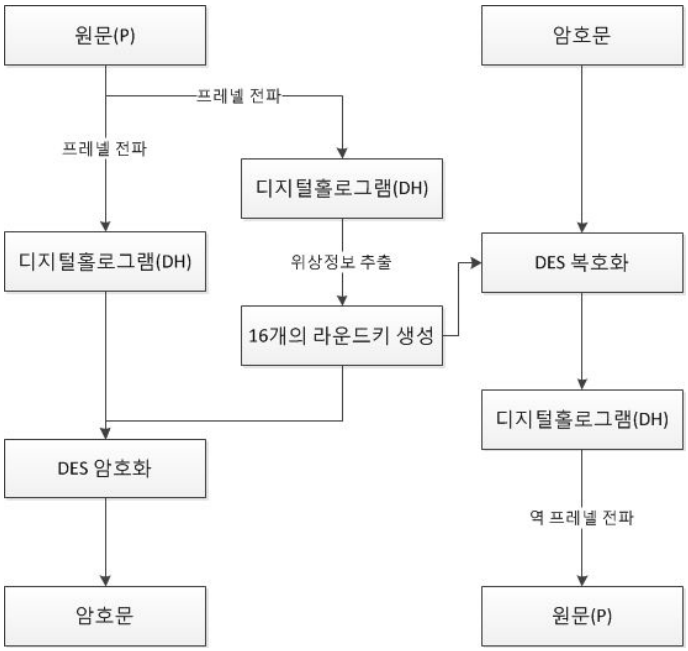
이러한 DES 암호화 알고리즘은 총 길이 56bits의 비밀키를 사용한다. 짧은 길이의 비밀키 사용으로 인하여 DES는 속도면에서 처리량 면에서 성능이 우수하지만, 전수키 공격(Brute force attack)에 취약한 암호화 알고리즘이 되어버렸다. 이를 보안하기 위해 기존의 DES 알고리즘을 두 번 반복하는 2중 DES 알고리즘이 나왔고, 다음으로 3중 DES 알고리즘이 사용되어 왔다. 이들 알고리즘은 원천적인 DES의 취약성인 비밀키의 길이를 늘리는 것이 아닌 다른 동일한 과정을 2배, 3배 처리하는 과정을 취한 것이기 때문에 전수키 공격에는 원천적인 해결 방법이 아니다.

이런 원천적인 취약점인 비밀키의 길이에 변화를 주어 그 결과를 실험해 보고, DES암호화 알고리즘에 디지털 홀로그램 기법을 결합하여 키 순열의 무한대성을 측정하여 전수키 공격에 강인한 암호화 알고리즘을 제안하고, 그 결과를 측정 한다.

또한 제안한 알고리즘에서 디지털 홀로그램은 DES의 56bits의 비밀키 길이를 늘이기 위하여 무한대의 홀로그램 패턴을 이용하여 비밀키 길이를 184bits로 확장하는 용도로 사용된다.

2. 제안 알고리즘

[그림 3-2]에서 제안하는 알고리즘은 평문 데이터를 가상광학을 이용하는 디지털 홀로그램을 사용하여 암호화 과정을 거치고, 그 결과에 기존에 존재하는 DES암호화 알고리즘을 결합하는 형태이다. 이때 사용하는 암호화 정보로는 디지털 홀로그램에 사용되는 홀로그램 파라미터 전파거리(d)와 빛의 파장(λ)이다.

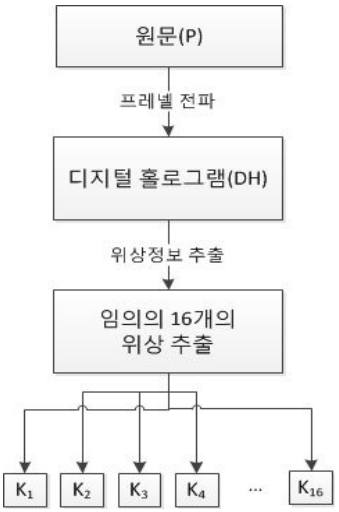


[그림 3-2] 제안하는 암/복호화 구조도

사용되는 평문데이터는 64bits로 표현 가능한 문자열 데이터(8자 단위)와 $N \times N$으로 표현이 가능한 2차원 이미지이다. 두 가지의 입력데이터를 이용하여 디지털 홀로그램을 구하며, 이때 프레넬 전파를 통과하게 되는데 이는 FFT를 거침으로써 전파가 가능하고, 만들어진 홀로그램 데이터는 하나의 요소($DH(i,j)$)가 $a+bi$ 형태의 구조의 64bits 값으로 변환이 된다.

또한 DES를 처리하기 위해 사용되는 DES의 라운드키는 기존에 또 다른 파라미터 정보를 통해 생성되는 디지털 홀로그램의 위상 정보로 부터 임의의 16개의 요소($DH(i,j)$)를 랜덤하게 추출하여 이를 48bits의 라운드키 그룹(K_i)를

구성한다. 이 라운드키는 디지털 홀로그램의 위상정보로부터 값을 추출해 내기 때문에 값들에 대한 서로의 연관성이 줄어든다. 이는 디지털 홀로그램의 각 요소간의 정보는 서로 관계가 없다는 이유에서 가능하다[27].



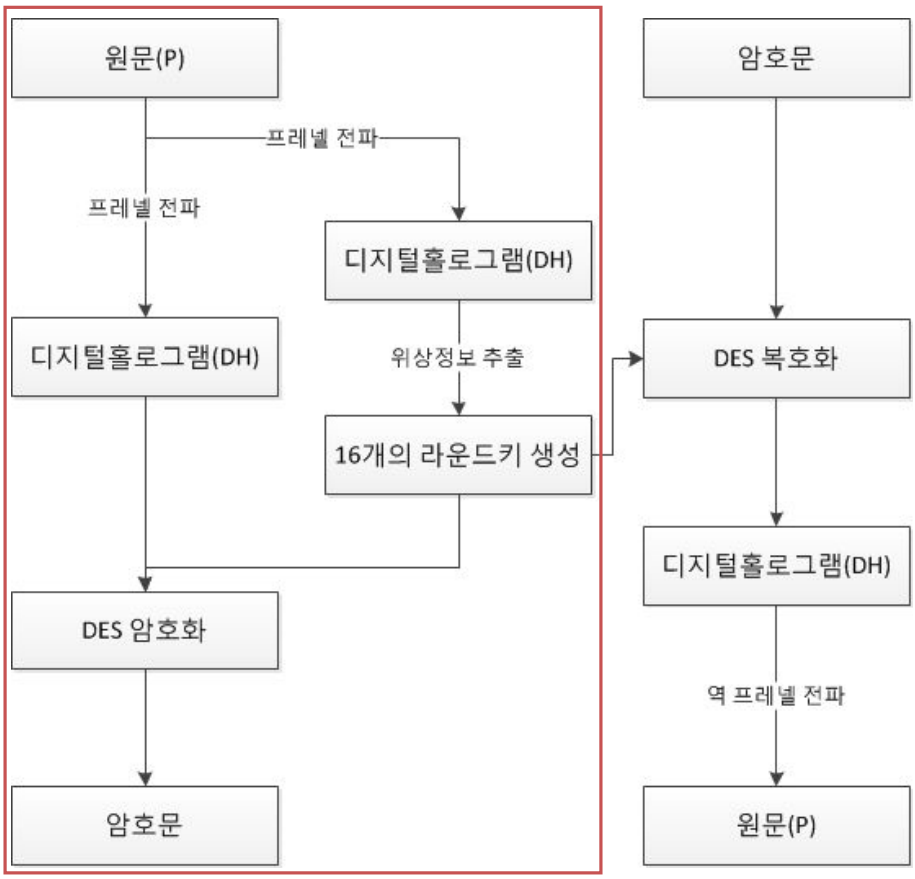
[그림 3-3] 키 생성 알고리즘

```
DH_DES()
{
   P ← LoadInput();                          // 평문을 준비
   DHK ← GetDH(P, dK, ramdaK);               // 라운드키용 홀로그램
   DHP ← GetDH(P, dP, ramdaP);               // 암호용 홀로그램
   DES_K ← CreateDHRound(DHK);               // DES용 라운드 키 생성
   DH_E ← GetDHDES_Encrypt(DHP, DES_K);      // DES 암호화 과정
   Result ← GetAvalancheInfo();              // 쇄도효과 및 기타 프로세싱
   DH_D ← GetDHDES_Decrypt(DH_E, DES_K);     // DES 복호화 과정
   DHO ← GetIDH(DH_D, dP, ramdaP);           // 홀로그램 복호화 과정
}
```

[표 3-1] 제안 Pseudo Code

3. 홀로그램을 이용한 DES 암호화 기법

본 알고리즘에서는 8×8 행렬을 이용하여 64bits의 블록을 설정하고, 입력 평문을 컴퓨터상에서 프레넬 전파시켜 입력 평문에 대한 디지털 홀로그램 패턴을 생성한다. 이렇게 생성된 홀로그램 패턴은 광학적 파라미터 값(파장, 전파거리)에 의존하는 복소수 값이 된다. [그림 3-4]의 선택된 부분을 통하여 암호화 과정을 거치게 된다.



[그림 3-4] 홀로그램을 이용한 새로운 DES 암호화 알고리즘의 과정

[표 3-1]은 암호화를 위한 한 블록의 8×8 행렬을 나타낸 것이며 평문의 비트를 구하여 행렬에 채워 넣는다. 행렬구조가 되는 이유는 입력 평문이 64bits의 블록단위로 처리되기 때문에 입력 값의 구조는 64bits의 구조가 되어야 하기 때문이다.

평문 : Morning!
비트
0100110101101111011100100110111 0
0110100101101110011001110010000 1

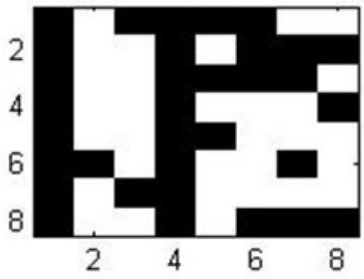
0	1	0	0	1	1	0	1
0	1	1	0	1	1	1	1
0	1	1	1	0	0	1	0
0	1	1	0	1	1	1	0
0	1	1	0	1	0	0	1
0	1	1	0	1	1	1	0
0	1	1	0	0	1	1	1
0	0	1	0	0	0	0	1

[표 3-2] 입력 평문 예시

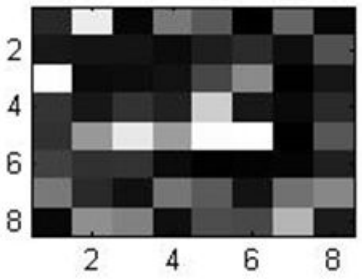
평문의 행렬을 프레넬 전파 시켜 생성된 디지털 홀로그램으로부터 각 원소에 대한 64개의 위상 값을 사용하여 64bits DES 라운드키를 생성한다. 생성된 라운드키는 디지털 홀로그램의 고유 위상정보이기 때문에 DES 키가 노출된 경우에도 원 평문의 복호화가 매우 어렵게 된다. 즉, 디지털 홀로그램 패턴 생성과정에서의 정확한 광학적 파라미터를 알지 못하면 디지털 홀로그램 패턴으로 원 평문 복원이 어렵다[27].

$$U_H(x_h,y_h)=\frac{\exp(j2\pi d_h/\lambda)}{j\lambda d_h}\exp\{j\frac{\pi}{\lambda d_h}(x_h^2+y_h^2)\}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}U_O(x,y)\exp\{j\phi_O(x,y)\}\times \exp\{j\frac{\pi}{\lambda d_h}(x^2+y^2)\}\exp\{-j\frac{2\pi}{\lambda d_h}(xx_h+yy_h)\}dxdy \quad (3\text{-}1)$$

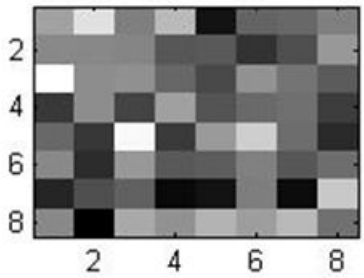
식(4-1)의 d_0 는 전파거리, 파장 λ를 이용하여 입력 평문을 프레넬 전파 시켜 홀로그램 데이터를 획득한다.



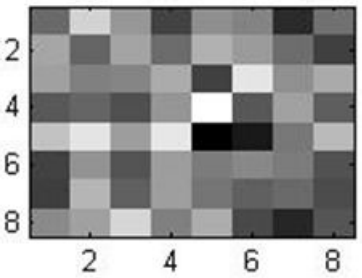
(a)입력 평문의 바이너리 값



(b)디지털 홀로그램으로 변환된 평문



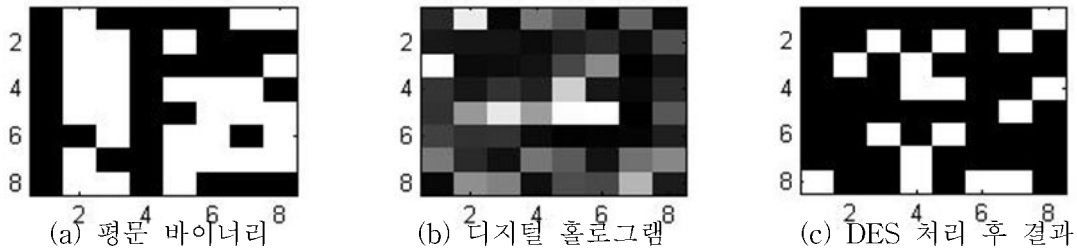
(c)홀로그램의 Real 영역



(d)홀로그램의 Img 영역

[그림 3-5] 평문에 대한 홀로그램

[그림 3-5]에서 얻어진 디지털 홀로그램(b)는 입력된 평문(a)의 바이너리 데이터가 각 필드가 복소수의 형태를 띄는 홀로그램으로 변환된 것이다. 본 과정을 통해 홀로그램을 암호화 할 수 있으며, 각 필드의 복소수의 값을 Real(c), Img(d) 로 분리하여 각각의 필드를 모두 DES 암호화 알고리즘을 적용하여 암호화 할 수 있다.



(a) 평문 바이너리 (b) 디지털 홀로그램 (c) DES 처리 후 결과

[그림 3-6] 홀로그램의 DES 처리 결과

[그림 3-6]에서 DES를 이용하여 암호화 알고리즘을 구성하게 되면 (c)처럼 홀로그램의 각 필드는 더 이상 백색잡음 형태의 구성을 띄지 않게 된다. 즉, DES에 의해서 각 필드의 비트들은 서로 얽혀 있어서 홀로그램 데이터를 평문으로 인식하여 암호화 과정을 거친 결과이기 때문에 각 필드마다 DES 암호화가 이루어져 있게 된다.

DES 과정을 거친 암호문은 더 이상 전수키 공격에 취약하지 않은 상태가 된다. 여기서 취합 가능한 전수키 공격 가능한 키 순열의 수는

$$K_n = 2^{56} \times (\nabla z \in R^3 \text{ or } \nabla \lambda \in R^3) \tag{3-2}$$

이 성립한다.

암호화 키는 기존 DES 알고리즘에 사용한 키 조합이 2^{56}에 해당하고. 홀로그램을 만들 때 사용한 광학적 파라미터(전파거리 d, 파장 λ)에 의한 3차원 공간상의 z 축의 실수 값이 첨가되어 파라미터의 범위는 R^3으로 확장된다.

즉 파라미터는

$$2^{56} \times (\nabla z \in R^3 \text{ or } \nabla \lambda \in R^3) \fallingdotseq \infty, \quad K_n \fallingdotseq \infty \tag{3-3}$$

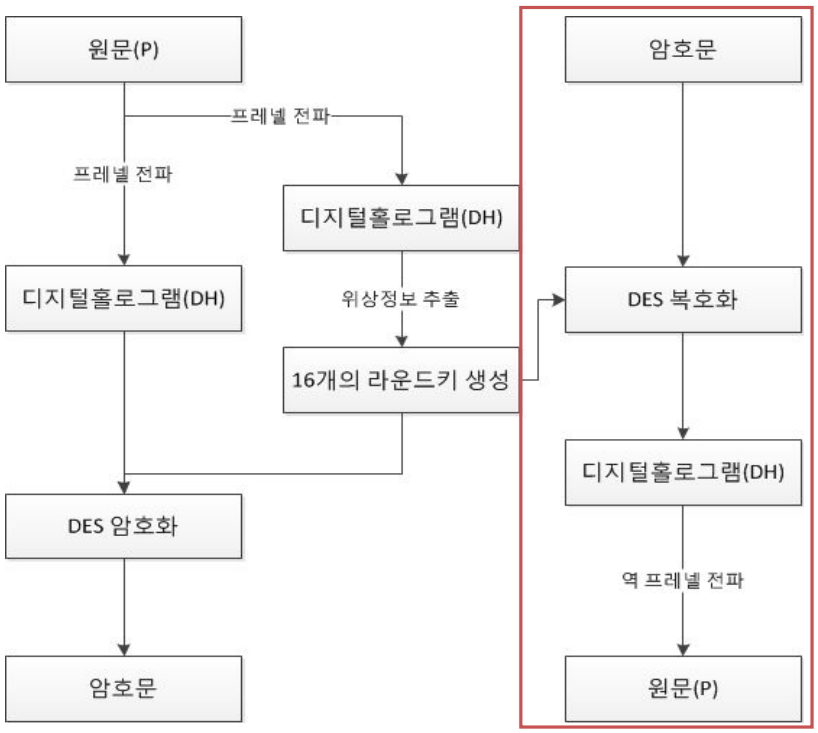
에 해당하는 키 순열을 포함한다.

따라서 제안하는 알고리즘은 거의 무한대에 가까운 키 순열이 생성될 수 있으므로 전수키 공격에 강인한 알고리즘이 된다.

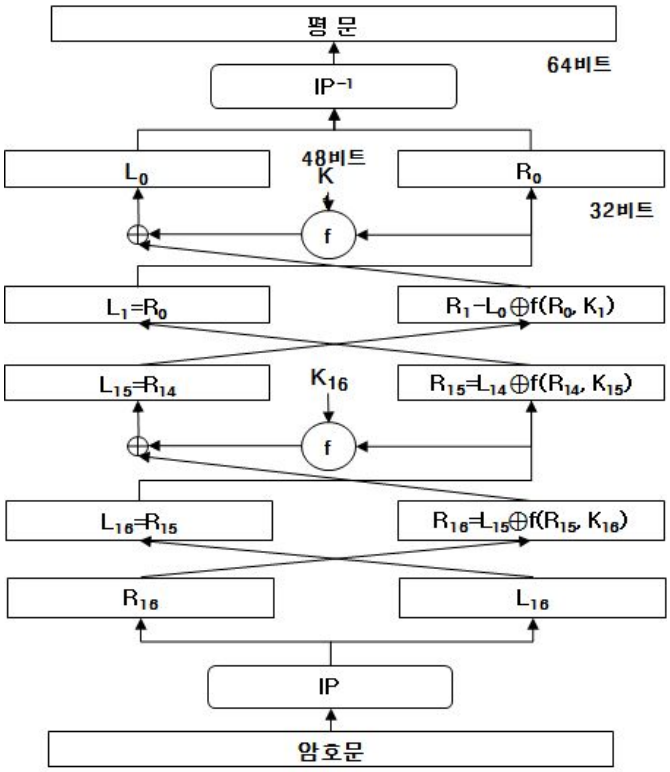
4. 홀로그램을 이용한 DES 복호화 기법

본 알고리즘에서는 8×8 행렬을 이용하여 64bits의 블록을 설정하고 입력 평문을 컴퓨터상에서 프레넬 전파시켜 입력 평문에 대한 홀로그램을 생성하였고, 64bits 블록 단위로 DES 암호화 알고리즘을 적용하였다. 생성된 암호문 데이터를 사용하기 위해서는 복호화 과정을 거쳐서 평문데이터를 복원해 내야한다.

복원을 하기 위해서는 [그림 3-7]의 과정을 통해 복원 과정을 거친다. 복호화 과정들은 대칭형 암호화 방법에 정의대로 암호화 과정의 반대로 이루어지게 되며 DES에 사용하였던 비밀키를 이용하여 복호화 과정을 거치게 된다.



[그림 3-7] 홀로그램을 이용한 새로운 DES 복호화 알고리즘의 과정



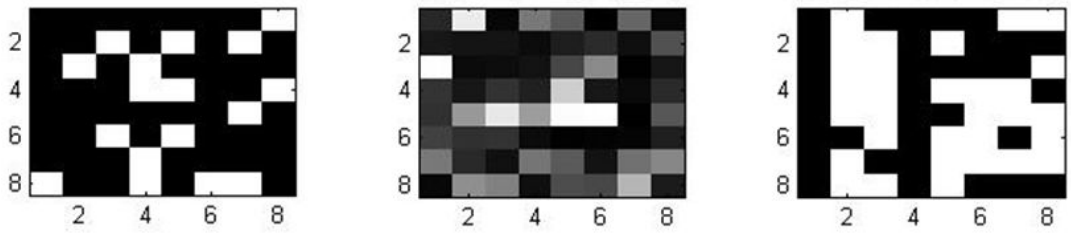
[그림 3-8] DES의 복호화 과정

제안한 암호화 과정에서 생성된 암호문과 DES 암호화 과정에 사용한 비밀키를 이용하여 [그림 3-8]처럼 DES 복호화 과정을 통해 64bits 블록 단위로 복원을 한다. 본 DES 복호화 과정을 통해서 만들어진 복원문은 디지털 홀로그램을 암호화하는 방법은 역 프레넬 전파를 시키는데,

이때 (3-2)의 식과 같이 FFT를 이용한 홀로그램 암호화과정을 거쳤으므로

$$U_H(x_h, y_h) = \frac{\exp(j2\pi d_h/\lambda)}{j\lambda d_h}\exp\{j\frac{\pi}{\lambda d_h}(x_h^2+y_h^2)\}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}U_O(x,y)\exp\{j\phi_O(x,y)\}\times \exp\{j\frac{\pi}{\lambda d_h}(x^2+y^2)\}\exp\{-j\frac{2\pi}{\lambda d_h}(xx_h+yy_h)\}dxdy \quad (3\text{-}4)$$

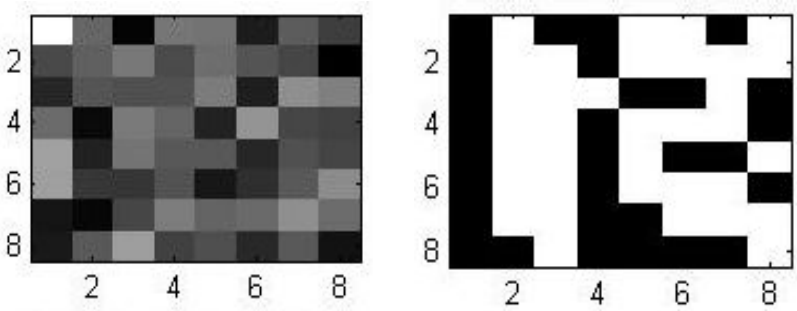
복원 과정에서는 IFFT(Inverse Fast Fourier Transform)과정을 거쳐서 홀로그램을 복원한다. 이 d와 λ는 각각 전파거리와 파장이 된다.



(a) 암호문 (b) 디지털 홀로그램으로 변환된 암호문 (c) 복원된 평문

[그림 3-9] 암호문의 복원된 결과

[그림 3-9]에서 암호문을 역 DES(DES 복호화)를 취하고, 이를 다시 디지털 홀로그램으로 역변환 시킴으로써 본 알고리즘의 복호화 과정을 구하게 된다. 이 때 사용한 파라미터 d와 λ는 각각 전파거리와 파장이 되며 두 파라미터의 정보를 알지 못한다면 본래의 평문 데이터가 복원되지 않는다.



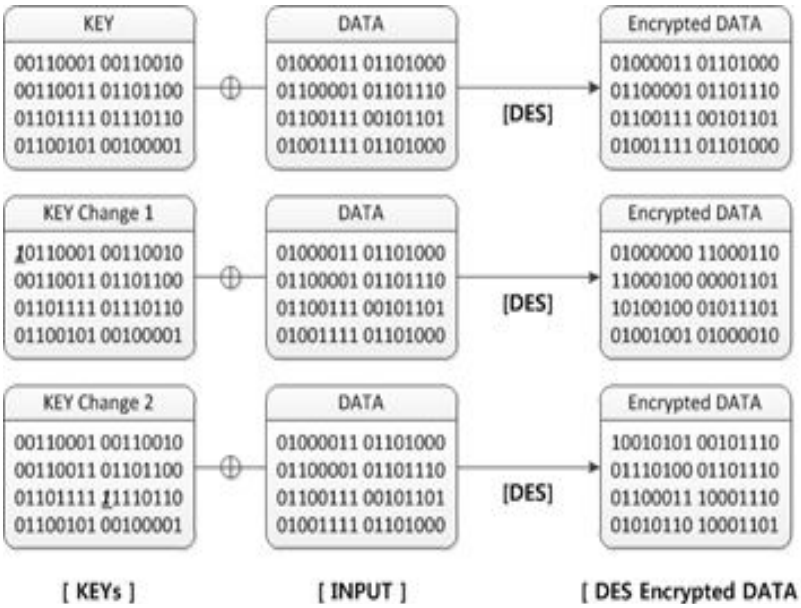
(a) 홀로그램 (b) 평문

[그림 3-10] 잘못된 파라미터로 복원

5. 성능 개선 평가를 위한 쇄도효과 측정

제안한 디지털 홀로그램을 이용한 DES 알고리즘을 이용하면 전수키 공격에 강인한 암호문을 만들 수 있다. 전수키 공격에 강인한 성격을 갖는 특성을 만들어 냈지만, 실질적으로 디지털 홀로그램이 암호로 사용할 수 있는지 판별을 하기 위해서는 쇄도 효과를 측정해야 한다.

쇄도 효과(Avalanche Effect)란 평문이나 비밀키의 작은 변화에도 암호문에는 커다란 영향을 미쳐 결과적으로 암호문에 중요한 변화를 일으키게 하는 효과를 말한다.



[그림 3-11] 쇄도효과 예(DES)

[그림 3-11]에서 DES 알고리즘의 입력데이터의 일부를 변경하면 암호문의 결과가 급격히 변화된 것을 확인 할 수 있다.

또한, 쇄도 효과는 변경전의 결과와 50%의 수치적인 차이가 발생하여야 한다. 입력데이터는 0, 1의 바이너리 데이터이기 때문에 50% 이상/이하의 수치는 허용되지 않으며 50%의 이상적인 수치가 나와야 성능을 인정받는다.

블록암호화 알고리즘에서 쇄도효과를 측정하기 위해서는 전체 요소의 개수가 n인 입력 평문의 P에 대한 암호화 데이터가 $E(P)$라 하고, 입력 평문 P의 비밀키의 일부를 변경한 것을 P'라고 할 때 생성된 암호화 데이터가 $E(P')$라 하면

$$E(P) \oplus E(P') = D \text{ (단, } D = \frac{n}{2} \text{)} \tag{3-5}$$

가 만족하는 D가 존재하여야 한다.

디지털 홀로그램이 쇄도효과를 만족하는지 알아보기 위해 파라미터인 전파거리(d)와 파장(λ)이 변화하는 양에 따라 어떻게 나타나는지를 알아야 한다. 따라서 쇄도효과를 측정하기 위해 홀로그램의 두 파라미터의 값을 순차적으로 변화시켜 가면서 어느 정도의 양에서 D가 발생하는지 측정한다.

IV. 실험 및 성능평가

본 연구에서는 디지털 홀로그램의 쇄도효과의 측정과 디지털 홀로그램을 이용한 DES 알고리즘의 성능을 측정하였다.

1. 실험 환경

본 연구에서는 디지털 홀로그램을 가상광학을 이용하여 측정하고자 Windows XP운영체제에서 Intel Core I5 2.67 GHz, 3GB RAM으로, Matlab 7.x 를 사용하였다. 분석에 사용되는 데이터는 8x8 크기의 64bits 바이너리 데이터이며, 이는 영상 또는 텍스트 정보를 이용하여 생성된 이미지이다.

실행에 필요한 소스 코드는 DES 알고리즘과 가상광학을 이용한 디지털 홀로그램 구현코드를 기반으로 하였으며 프로그램의 성능 측정을 위하여 저자가 직접 구현한 구현코드를 사용하였다.

2. 실험 결과

1) 입력 평문 데이터

입력에 사용된 데이터는 [표 4-1]에 해당하는 텍스트 정보 데이터와 [그림 4-1]에 해당하는 이미지 데이터를 사용하였다.

평문 : Morning!
비트
01001101011011110111001001101110
01101001011011100110011100100001

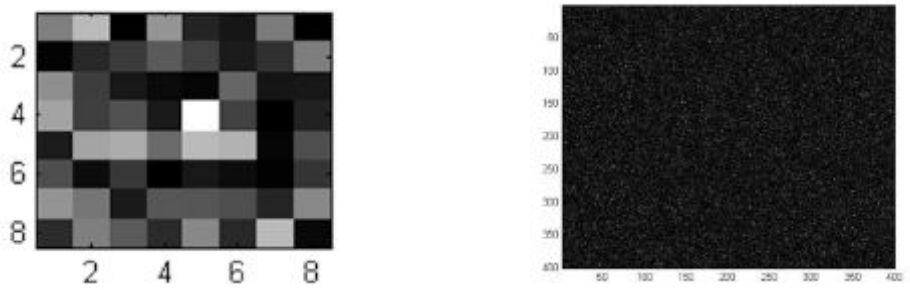
0	1	0	0	1	1	0	1
0	1	1	0	1	1	1	1
0	1	1	1	0	0	1	0
0	1	1	0	1	1	1	0
0	1	1	0	1	0	0	1
0	1	1	0	1	1	1	0
0	1	1	0	0	1	1	1
0	0	1	0	0	0	0	1

[표 4-1] 입력 평문 : 텍스트

[그림 4-1] 입력 평문 : 이미지

2) 홀로그램으로의 변환

입력데이터의 홀로그램을 확인하기 위하여 전파거리 d와 파장 λ를 이용하여 홀로그램을 생성하였다. 전파거리 d=8000와 파장 λ=0.5145를 파라미터로 사용하였다.



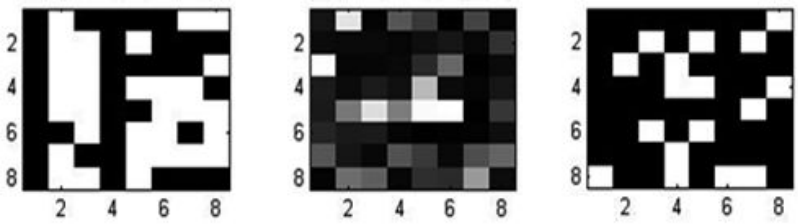
(a) 텍스트의 디지털 홀로그램 (b) 이미지의 디지털 홀로그램

[그림 4-2] 디지털 홀로그램의 예

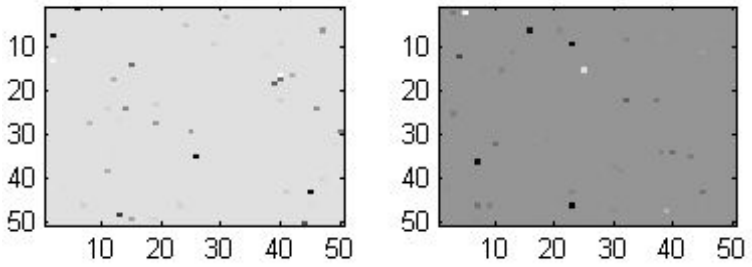
측정된 홀로그램은 단순히 FFT를 이용하여 프레넬 전파된 홀로그램으로 백색잡음 형태의 성격을 갖고 있다. 텍스트에 대한 홀로그램 역시 백색잡음의 형태로 표현이 된다.

3) 홀로그램에 DES를 적용한 암호화

생성된 디지털 홀로그램의 각 필드에 DES 알고리즘을 적용하면 백색 잡음 형태의 홀로그램은 내부 비트가 바뀌어 버린 상태로 된다. 전파거리 d=8000와 파장 λ=0.5145를 파라미터로 사용하였다.



[그림 4-3] 텍스트에 대한 홀로그램의 DES



(a) real 영역의 DES 결과 (b) img 영역의 DES 결과

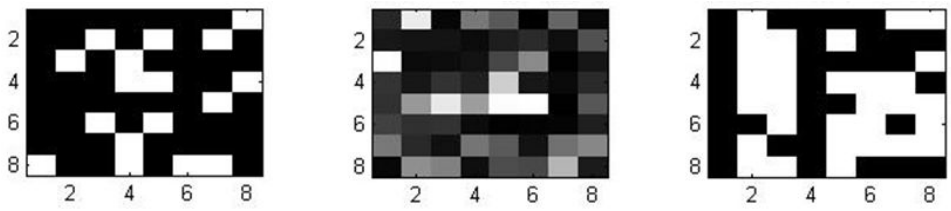
[그림 4-4] 이미지에 대한 홀로그램의 DES

홀로그램의 각각의 필드에 DES를 적용한 결과 [그림 4-3], [그림 4-4]와 같이 가우시안 백색잡음 형태의 구조는 사라지고 비트가 변환되어 임의의 값으로 나타난다.

4) 암호문에 역DES를 취한 복호화

생성된 암호문에 암호화 과정에서 사용한 비밀키를 적용하여 역DES를 취하면 [그림 4-5] (b)처럼 백색잡음 형태의 디지털 홀로그램 데이터가 나타난다

.

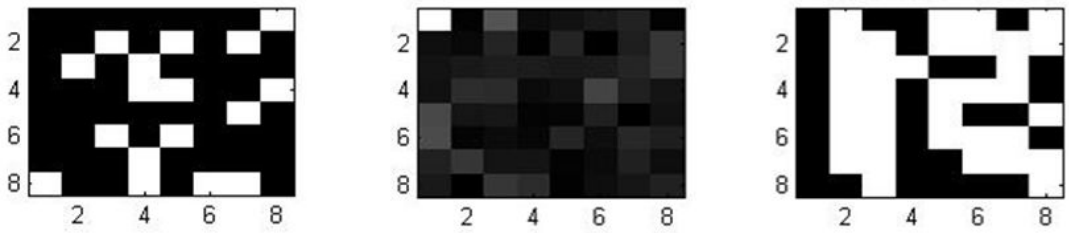


(a) 암호문 (b) 디지털 홀로그램으로 변환된 암호문 (c) 복원된 평문

[그림 4-5] 암호문의 복원된 결과

재생된 디지털 홀로그램에 전파거리 d=8000와 파장 λ=0.5145를 파라미터로 사용하여 IFFT를 취하게 되면 디지털 홀로그램이 평문으로 복원된다. 하지만 생성된 암호문에 전파거리 d=8000와 파장 λ=0.5145를 파라미터와 같이 초기 사

용한 파라미터 값이 아닌 값을 입력하여 복호화 과정을 거치면 비정상적인 홀로그램은 물론이고 복원된 결과 데이터 또한 원본과 다른 데이터가 발생한다.



(a) 암호문 (b) 디지털 홀로그램으로 변환된 암호문 (c) 복원된 평문

[그림 4-6] 암호문이 틀린 파라미터를 적용하여 복원된 결과

5) 홀로그램에 대한 쇄도 효과 측정

홀로그램 패턴에 대한 쇄도 효과를 측정하기 위하여 디지털 홀로그램의 광학적 파라미터(파장, 전파거리)의 변화를 주며 변경전의 결과와 50%의 수치적 차이가 발생하는지 여부를 판단한다.

(단위 : ㎛)

전파거리 (d)	8000	8001	8010	8070	**8100**	8123	8150	8600	8800	8900	9000	9010
차이 bits	0	4	19	26	**32**	33	26	26	33	36	36	37

[표 4-2] 전파거리(d)에 따른 암호문의 변화

[표 4-2]는 전파거리(d)를 이용하여 측정한 데이터로써 64bits의 1/2인 32개의 비트가 차이가 발생하여야 쇄도 효과가 있다고 평가 할 수 있다. [표 4-2]는 전파거리를 8000㎛로 시작하여 증가 변화를 주어 측정 결과 전파거리가 8100㎛ 범위에서 32개의 비트가 달라지는 것이 측정되었다. 따라서 전파거리는 100㎛ 범위에서 쇄도 효과가 발생한다.

(단위 : ㎛)

파장 (λ)	0.5145	0.5148	0.518	0.519	0.52	**0.5224**	0.53	0.5315
차이 bits	0	2	17	19	22	**32**	38	38

[표 4-3] 파장(λ)에 따른 암호문의 변화

[표 4-3]은 파장(λ)을 0.5145㎛으로 시작하여 측정한 데이터이다. 파장이 0.5224㎛에서 32개의 비트의 변화가 측정된다. 따라서 파장에서의 변화는 79㎛의 범위에서 쇄도 효과가 발생하는 것을 확인 할 수 있다.

V. 결 론

본 논문에서는 비밀키의 길이에 대한 문제점으로 DES 블록대칭암호화 알고리즘에서 발생할 수 있는 전수키 공격에 대한 방어의 목적으로 시작되었다.
그래서 DES 블록대칭암호화 알고리즘의 단순한 반복적 비트연산을 이용하고 디지털 홀로그램 암호화 기법을 이용하여 전수키 공격에 강인한 암호화 알고리즘을 구성하는 것을 제안하였다. 제안된 알고리즘은 기존에 존재하는 DES 암호화 알고리즘에 디지털 홀로그램 암호화 과정(DH)을 결합하고, 디지털 홀로그램의 위상 정보로부터 랜덤하게 DES의 라운드키를 생성하여 사용하는 이중적인 암호화 알고리즘의 구조를 갖는다. 이렇게 생성된 라운드키를 사용하면 DES의 비밀키의 노출이 발생하더라도 디지털 홀로그램의 과정을 알지 못하면 바로 DES에 대한 전수키 공격은 소용이 없게 된다. 반대로 디지털 홀로그램에서 다룰 수 있는 파라미터 정보(전파거리 d, 빛의 파장 λ)의 정보를 알지 못하면 또는 100㎛의 범위의 차이를 모르면 디지털 홀로그램의 쇄도효과로 인해 비정상적인 홀로그램의 평문이 복원이 되어 결과는 다르게 나타난다.

실험결과 알고리즘의 안전성을 논하는 대표적인 방법으로 이용되는 쇄도효과를 디지털 홀로그램에 대하여 측정하였다. 디지털 홀로그램의 파라미터 정보인 전파거리 d, 빛의 파장 λ에서 쇄도효과가 발생 가능한 증감 범위가 약 100㎛의 작은 값으로 측정되었다. 따라서 파라미터들의 입력 가능한 범위를 ∞라고 가정한다면 디지털 홀로그램은 $\fallingdotseq \infty$의 범위 내에서 쇄도효과가 발생한다. 또한 수치적으로 표현이 가능한 비트수는 2^{128}에 해당하므로 디지털 홀로그램의 생성 가능한 비밀키 순열은 2^{128}개이다.

DES의 후속 보안알고리즘으로 제안되어 표준화된 AES(Advanceed Encrypti-on Standard) 암호화 알고리즘과 비교하면, AES는 128bits의 비밀키 길이를 사용하여 사용함으로써 56bits를 사용하는 DES에 비하여 전수키 공격에는 강인하지만 수학적인 수식의 도입으로 인해 DES와 비교하여 속도에서는 상대적으로 느리다. 이런 DES에 2^{128}에 해당하는 비밀키 길이를 갖는 디지털 홀로그램의 추가적인 결합은 속도에서는 AES 보다는 느리지만 전수키 공격의 취약에서

$2^{56}*2^{128}=2^{184}$에 해당하는 키 길이를 가지므로 AES와 비교하여 볼 때 더욱 전수 키 공격에 대하여 강인한 성질를 갖는다. 제안한 알고리즘의 단점인 디지털 홀로그램으로의 변환과정에서 발생하는 속도면의 문제는 암호화과정의 대부분의 처리과정이 반복 작업의 특성을 가지므로 GPU 프로세싱이나 병렬프로세싱을 사용하면 빠른 처리가 가능하다.

제안한 알고리즘은 전수키 공격에서 DES의 후속인 AES에 비하여 높은 성능을 보이면서 속도에서는 느리다. 속도문제는 앞서 제시한데로 병렬 프로세싱을 통하여 해결 가능한 문제이다. 새로운 알고리즘을 일반적인 시스템에서 사용하는 것 보다는 국방시스템이나 기업의 서버시스템에서 보안이 강화되어야할 자료를 암호화 할 때 비로써 성능을 발휘 할 수 있다. 추후 발전방향으로 단일 프로세스에서도 성능을 발휘 할 수 있도록 불필요한 작업을 제외하고 복합적인 반복 작업을 빠르게 수행할 수 있는 방법이 필요하다.

참고문헌

[1]. P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. 20, 767-769 (1995).

[2]. G. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain," Opt. Lett. 29, 1584-1586 (2004).

[3]. S. Kishk and B. Javidi, "Information hiding technique with double phase encoding," Appl. Opt. 41, 5462-5470 (2002).

[4]. S. Kishk and B. Javidi, "Watermarking of three-dimensional objects by digital holography," Opt. Lett. 28,167-169 (2003).

[5]. L. Cai, M. He, Q. Liu, and X. Yang, "Digital image encryption and watermarking by phase-shifting interferometry," Appl. Opt. 43, 3078-3084 (2004).

[6]. B. Javidi and T. Nomura, "Securing information by use of digital holography," Opt. Lett. 25, 28-30 (2000).

[7]. O. Matoba and B. Javidi, "Optical retrieval of encrypted digital holograms for secure real-time display," Opt. Lett. 27, 321-323 (2002).

[8]. L. Yu, X. Peng, and L. Cai, "Parameterized multi-dimensional data encryption by digital optics," Opt. Commun. 203, 67-77 (2002).

[9]. X. Peng, Z. Cui, and T. Tan, "Information encryption with virtual-optics imaging system," Opt. Commun. 212, 235-245 (2002).

[10]. L. Yu and L. Cai, "Multidimensional data encryption with digital holography," Opt. Commun. 215, 271-284 (2003).

[11]. X. Peng, L. Yu, and L. Cai, "Digital watermarking in three-dimensional space with a virtual-optics imaging modality," Opt. Commun. 226, 155-165 (2003).

[12]. S. Lai and M. A. Neifeld, "Digital wavefront reconstruction and its application to image encryption," Opt. Commun. 178, 283-289 (2000).

[13]. E. Tajahuerce, O. Matoba, S. C. Verrall, and B. Javidi, "Optoelectronic information encryption with phaseshifting interferometry," Appl. Opt. 39,

2313-2320 (2000).
[14]. E. Tajahuerce and B. Javidi, “Encrypting three-dimensional information with digital holography,” Appl. Opt. 39, 6595-6601 (2000).
[15]. B. Zhu, H. Zhao, and S. Liu, “Image encryption based on pure intensity random coding and digital holography technique,” Optik 114, 95-99 (2003).
[16]. H.-Y. Li, Y. Qiao, and D. Psaltis, “Optical network for real-time face recognition,” Appl. Opt. 32, 5026 - 5035 ~1993!.
[17]. B. Javidi and J. L. Horner, “Optical pattern recognition for validation and security verification,” Opt. Eng. 33, 1752 - 1756 ~1994!.
[18]. Ph. Re´fre´gier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” Opt. Lett. 20, 767 - 769 ~1995!.
[19]. C. L. Wilson, C. I. Watson, and E. G. Paek, “Combined optical and neural network fingerprint matching,” in Optical Pattern Recognition VIII, D. P. Casasent and T. Chao, eds., Proc. SPIE 3073, 373 - 382 ~1997!.
[20]. N. Yoshikawa, M. Itoh, and T. Yatagai, “Binary computergenerated holograms for security applications from a synthetic double-exposure method by electron-beam lithography,” Opt. Lett. 23, 1483 - 1485 ~1998!.
[21]. O. Matoba and B. Javidi, “Encrypted optical memory system using three-dimensional keys in the Fresnel domain,” Opt. Lett. 24, 762 - 764 ~1999!.
[22]. J. E. Ford, Y. Fainman, and S. H. Lee, “Array interconnection by phase-coded optical correlation,” Opt. Lett. 15, 1088 - 1090 ~1990!.
[23]. C. Denz, G. Pauliat, G. Roosen, and T. Tschudi, “Volume hologram multiplexing using a deterministic phase encoding method,” Opt. Commun. 85, 171 - 176 ~1991!.
[24]. H. Lee and S. K. Jin, “Experimental study of volume holographic interconnects using random patterns,” Appl. Phys. Lett. 62, 2191 - 2193 ~1993!.
[25]. J. F. Heanue, M. C. Bashaw, and L. Hesselink, “Encrypted holographic data storage based on orthogonal-phase-code multiplexing,” Appl. Opt. 34, 6012 - 6015 ~1995!.

[26]. C. Denz, K. O. Mueller, F. Visinka, and T. T. Tschudi, “Digital volume holographic data storage using phase-coded multiplexing,” Proc. SPIE. 3802, 142 - 147 ~1999!.
[27]. C. C. Sun, W. C. Su, B. Wang, and Y. Ouyang, “Diffraction selectivity of holograms with random phase encoding,” Opt. Commun. 175, 67 - 74 ~2000!.
[28]. J. W. Goodman, Introduction to Fourier Optics ~McGraw-Hill, New York, 1996!. 14. U. Schnars and W. P. O. Ju¨ ptner, “Direct recording of holograms by a CCD target and numerical reconstruction,” Appl. Opt. [29]. 179 - 181 ~1994!.
[30]. Y. Takaki, H. Kawai, and H. Ohzu, “Hybrid holographic microscopy free of conjugate and zero-order images,” Appl. Opt. 38, 4990 - 4996 ~1999!.

저작물 이용 허락서

학 과	컴퓨터공학과	학 번	20097087	과 정	석사
성 명	한글: 노창오	한문 : 盧昌吾	영문 : CHANGOH NOH		
주 소	광주광역시 동구 서석동 375번지				
연락처	E-MAIL : shckddh@gmail.com				
논문제목	한글 : 디지털 홀로그램을 이용한 DES 알고리즘의 암호성능 개선 영어 : Improvement of Cipher Performance in DES Algorithm using Digital Hologram				

본인이 저작한 위의 저작물에 대하여 다음과 같은 조건아래 조선대학교가 저작물을 이용할 수 있도록 허락하고 동의합니다.

- 다 음 -

1. 저작물의 DB구축 및 인터넷을 포함한 정보통신망에의 공개를 위한 저작물의 복제, 기억장치에의 저장, 전송 등을 허락함
2. 위의 목적을 위하여 필요한 범위 내에서의 편집·형식상의 변경을 허락함. 다만, 저작물의 내용변경은 금지함.
3. 배포·전송된 저작물의 영리적 목적을 위한 복제, 저장, 전송 등은 금지함.
4. 저작물에 대한 이용기간은 5년으로 하고, 기간종료 3개월 이내에 별도의 의사 표시가 없을 경우에는 저작물의 이용기간을 계속 연장함.
5. 해당 저작물의 저작권을 타인에게 양도하거나 또는 출판을 허락을 하였을 경우에는 1개월 이내에 대학에 이를 통보함.
6. 조선대학교는 저작물의 이용허락 이후 해당 저작물로 인하여 발생하는 타인에 의한 권리 침해에 대하여 일체의 법적 책임을 지지 않음
7. 소속대학의 협정기관에 저작물의 제공 및 인터넷 등 정보통신망을 이용한 저작물의 전송·출력을 허락함.

동의여부 : 동의(○) 반대( )

2010년 12월

저작자 : 노 창 오 (인)

조선대학교 총장 귀하