『난수발생장치분야』 특허동향보고서

조사분석4팀
정 문 영

서 론

IT산업의 발전에 따른 일상생활의 컴퓨터/인터넷 이용에 있어서 중요시 되는 것이 보안이다. 가장 흔히 볼 수 있는 예로, 특정 사이트를 자유롭게 이용하기 위해서 일반 클라이언트들은 해당 사이트에 회원가입을 하고 이때, 자신의 ID를 발급받고 이를 서버측에 인증하기 위한 패스워드를 설정하게 된다. 클라이언트는 추후 해당 사이트를 이용시 자신의 ID와 패스워드를 입력하여 로그인 과정을 거친 후 사이트에서 제공하는 컨텐츠를 이용하게 되는데, 이러한 패스워드와 같은 개인의 비밀정보는 철저하게 그 보안을 유지해야 한다.

최근 들어 인터넷을 통한 개인 또는 기업을 상대로 한 해킹 사례가 빈번한 것은 일일이 그 사례를 언급하지 않아도 누구나 인지하고 있는 바이고, IT 산업의 규모가 성장하고 그 가치가 증대함에 따라 해킹을 이용한 범죄의 빈도와 규모 또한 증가하고 있다.

이러한 상황에서 통신회선을 통한 각종 행위에 대한 보안의 중요성은 개인적인 차원에서는 물론이거니와, 기업 및 국가적인 차원에 있어서 때로는 해당 기업 및 국가의 흥망을 좌우할 정도의 중요성을 갖는 경우도 존재한다.

본 기술 동향 보고서에서는 이러한 통신회선 상의 보안을 위한 데이터의 암호화시에 사용되는 난수(Random Number) 및 난수를 발생시키기 위한 여러 방법에 대해서 고찰하여 보고 나아가 난수발생장치의 국가별 출원량과 다양한 난수발생방법의 세부방법(물리적 난수, 디지털 난수)별 출원량을 비교/분석해 보고자 한다.

본 론

제 1 절 난수발생장치 기술의 정의(배경)

1. 난수(random number)의 정의

기수가 n인 수에서 연속된 각 자릿수가 N개의 숫자 중에서 각각 같은 확률로 어느 하나를 선택하는 무작위 숫자. 예를 들면, 10진수 236에서 첫 번째 자릿수인 2는 0/9의 10개 숫자 중에서 10분의 1 확률로 2를 취하게 된 것이고, 3과 6도 마찬가지로 각각 10분의 1 확률로 얻어진 것이다.

2. 난수발생방법

2.1. 선형합동발생기 (Linear Congruential Generator)

1차원적인 선형합동발생기(LCG)는 아래와 같은 수식으로 이루어지며, 이전값을 이용하여 현재값을 도출한다.

$X_n = (aX_{n-1} + b) \bmod m$

2.2. 다중재귀발생기 (Multiple Reculsive Generator)

다중재귀발생기(MRG)는 다음과 같은 수식을 사용한다.

$X_n = (aX_{n-1} + \cdots + aKX_{n-K}) \bmod m$

그러나 LCG나 MRG의 경우 그 랜덤성을 예측가능하기 때문에 이 둘을 조합한 조합선형발생기를 주로 사용하고 있다.

2.3. 비선형 발생기(Nonlinear Generator)

X_{n-1}에서 X_n으로 전이하는 전이함수를 비선형 함수를 사용하는 것이다.

대표적으로 역합동 발생기(Inversive Congruetial Generator)가 있으며, 이것은 LCG에 비선형적인 왜곡을 추가한 것으로 아래와 같은 수식을 사용한다.

$U_n = ((X_{n-1} \times X_n^{-1}) \bmod m) / m$

2.4. 선형피드백쉬프트레지스터 (Linear Feedback Shift Register)

컴퓨터 내에서 모든 산술연산이 2진으로 이루어진다는 것을 이용하여, 선형 혹은 비선형적으로 각 비트들을 선발해 시프트와 비트 연산을 거쳐 새로운 난수를 발생시키는 방법이다.

그러나 진정한 의미에서의 난수는 상기와 같은 알고리즘의 복잡성과 비예측성도 중요하지만, 실제적으로 난수의 랜덤성을 결정하는 주요한 요소는 난수발생장치에 공급되는 시드(seed)값에 따라 좌우된다. 난수에 공급되는 시드값은 그 종류에 따라 크게 아날로그 시드와 디지털 시드로 나누어질 수 있다.

3. 난수를 발생시키기 위한 시드(seed)의 종류

3.1. 아날로그(물리) 시드

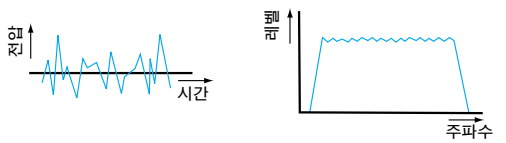
3.1.1. 백색잡음(White Noise)

: 열잡음(Thermal Noise), 플리커잡음(Flicker Noise), 전자회로잡음(Circuit Noise)

아래 왼쪽 그림에서 보면 화이트 노이즈의 시간에 따른 전압의 주파수 파형이 랜덤하게 진행됨을 알 수 있고, 이를 난수 발생에 이용 가능하다는 것을 인지할 수 있다. 오른쪽 그림에서 보면 화이트 노이즈의 주파수 대역별 레벨이 거의 일정하다는 것은 각 주파수가 거의 대등하게 발생한다는 것으로 이 또한 난수의 기본 요건인 예측불가능성에 만족하는 것임을 알 수 있다.

3.1.2. 생체정보(Bio Information)

〈그림 1〉

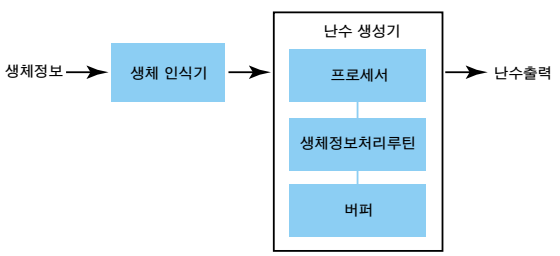


●화이트노이즈의파형 ●화이트노이즈의스펙트럼

생체정보를 이용하는 방법에 있어서도 디지털 생체정보를 잡음원으로 사용하여 난수 생성률과 구현의 용이성 등을 포함한 효율성 평가척도와 예측불가능성, 난수성을 포함한 안전성 평가척도를 모두 만족할 수 있다.

생체정보를 이용한 잡음생성 방법을 간단한 예를 들어 설명하면, 먼저 사람의 얼굴영상을 카메라와 같은 촬상장치로 촬영한다. 촬영된 화상 이미지의 특정 픽셀 영역에 대한 픽셀값을 추출하고 이를 난수로서 이용한다. 카메라에 의해 촬상되는 사람의 이미지는 시간과 장소에 따라 항상 차이가 발생하고 이러한 랜덤성은 난수 발생의 잡음원으로써 그 요건을 충족시킨다.

〈그림 2〉

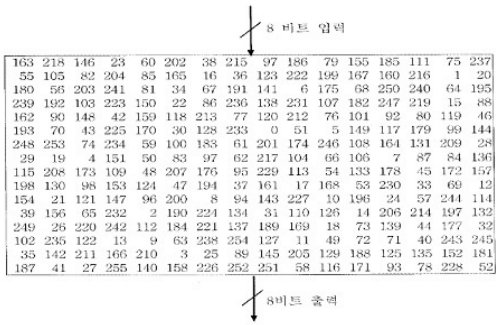


상기와 같은 노이즈는 완전히 불규칙한 신호이며, 신호의 전압크기(Amplitude)와 신호위상(Phase)은 불규칙한 주파수 성분을 갖게 된다. 이런 신호에서 긴 시간 동안의 RMS(Root Mean Square)값을 얻어낼 수는 있다 하더라도, 어느 한 순간의 정확한 신호의 크기를 예측하는 것은 불가능하기 때문에 이런 노이즈를 이용하여 완전한 난수를 얻어낼 수 있다.

3.1. 디지털 시드

디지털 시드를 이용하는 방법은 주로 임의의 숫자를 배열해 놓은 난수표를 이용하는 방법이다. 다음 그림에 난수표의 일례가 개념적으로 제시되어 있다. 입력되는 8비트의 숫자를 s-box라 불리우는 난수표의 특정 숫자와 소정의 연산(치환, 덧셈, 뺄셈 등)을 통해 암호화하여 8비트의 난수를 출력하는 방법이다. 그러나 이러한 난수표를 이용한 방식은 그 랜덤성에 있어서 완전하다고 볼 수 없으며 어느 정도의 예측 가능성을 가지는 면에서 보안상의 취약점은 가지고 있다고 볼 수 있다. 그러나 구현하기가 쉽다는 측면에서 낮은 보안 수준을 요구하는 방식에는 적당한 방법이다.

〈그림 3〉

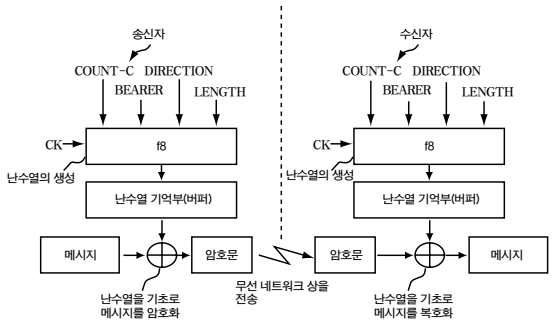


163	218	146	23	60	202	38	215	97	186	79	155	185	111	75	237
55	105	82	204	85	165	16	36	123	222	199	167	160	216	1	20
180	56	203	241	81	34	67	191	141	6	175	68	250	240	64	195
239	192	103	223	150	22	86	236	138	231	107	182	247	219	15	88
162	90	148	42	159	118	213	77	120	212	76	101	92	80	119	46
193	70	43	225	170	30	128	233	0	51	5	149	117	179	99	144
248	253	74	234	59	100	183	61	201	174	246	108	164	131	209	28
29	19	4	151	50	83	97	62	217	104	66	106	7	87	84	136
115	208	173	109	48	207	176	95	229	113	54	133	178	45	172	157
198	130	98	153	124	47	194	37	161	17	168	53	230	33	69	12
154	21	121	147	96	200	8	94	143	227	10	196	24	57	244	114
39	156	65	232	2	190	224	134	31	110	126	14	206	214	197	132
249	26	220	242	112	184	221	137	189	169	18	73	139	44	177	32
102	235	122	13	9	63	238	254	127	11	49	72	71	40	243	245
35	142	211	166	210	3	25	89	145	205	129	188	125	135	152	181
187	41	27	255	140	158	226	252	251	58	116	171	93	78	228	52

2. 난수발생기의 용도

2.1 메시지의 암호화/복호화

〈그림 4〉

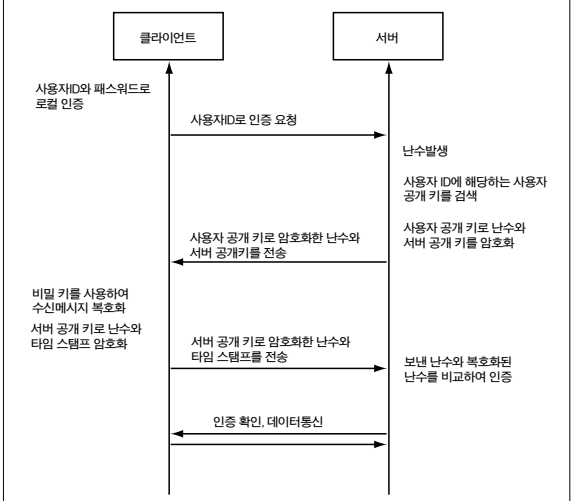


난수 발생기의 가장 기본적인 용도로서 데이터의 암호화 및 복호화를 들 수 있다. 상기 그림은 네트워크를 통한 데이터 전송에서 전송 대상 데이터의 보안을 위해 데이터를 난수를 이용하여 암호화하여 수신측에 전송하고 수신측은 이를 동일 난수를 이용하여 복호화함으로써, 네트워크 회선을 불법적으로 모니터링하는 제3자에 의한 데이터 열람을 방지할 수 있다.

2.2. 사용자 인증

아래 그림에서와 같이 서버측에서 발생시킨 난수는 사용자의 공개 키로 암호화 되어 사용자에게 전송되고 이를 자신의 비밀키로 해독한 사용자는 해당 난수를 서버 공개 키로 암호화하여 재전송하고 서버측에서는 자신이 보유한 난수와 사용자측에서 전송한 난수의 동일 여부를 판단하여 사용자의 정상 사용자 여부를 인증하는 방법이다.

〈그림 5〉



2.3. 기타

복권 발매기, 추첨기 등 랜덤성을 필요로 하는 숫자를 발생시켜야 하는 장치.

제 2 절 난수발생장치 기술의 분석기준

1. 난수발생방법 및 장치에 관한 것

1.1. 아날로그 시드를 이용한 난수의 발생방법 및 그 장치.
1.2. 디지털 시드를 이용한 난수의 발생방법 및 그 장치.
1.3. 난수발생장치를 이용한 보안 시스템 – 암호화

2. 조사범위 및 키워드

2.1 조사범위

한국과 일본의 경우, 2005년 7월 31일 이전에 출원/공개된 특허들을 사용했고, 미국의 경우 2005년 7월 31일 이전에 출원/등록된 특허들을 사용하였으며, 난수발생 자체에 관한 특허 및 난수발생기를 이용한 암호화에 관한 기술을 포함하였다. 또한 사용한 키워드는 아래와 같다

2.2. 키워드

(난수*, 랜덤넘버*, 랜덤 넘버*, 무작위 숫자*, 무작위 번호*, 무작위 넘버*, 임의 숫자*, 임의 번호*, 임의 넘버*, random number*)
(발생*, 생성*, 제너레이*, generat*)
(암호화*, 복호화*, 부호화*, 인크립*, 디크립*, encrypt*, decrypt*, cryptograph*, cipher*)

2.3. 관련 IPC분류

G06F 7/58*
G09C 1/00*
H04L 9/22, 26*
H04K 1/00*

특 허 동 향

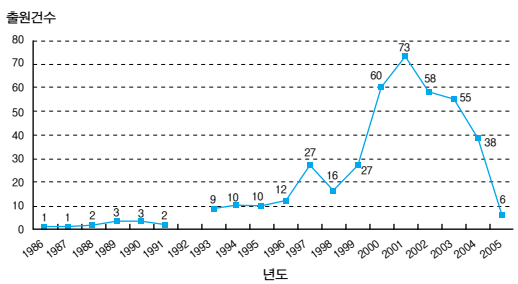
제 1 절 한국 특허동향

1 연도별 특허동향

표1 한국 내 연도별 출원동향

년도	1986	1987	1988	1989	1990	1991	1992	1993	1994	1995	계
출원건수	1	1	2	3	3	2	0	9	10	10	
년도	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	413
출원건수	12	27	16	27	60	73	58	55	38	6	

〈그림 6〉 한국 내 연도별 출원동향



한국의 난수발생 관련 특허출원은 90년대 말 무렵부터 증가하기 시작하여 2000년대에도 꾸준한 성장을 보이고 있다. [그림6]에서 2004년 이후 출원량이 감소폭을 보이는 것은 실제 출원량이 감소한 것이 아니라, 출원 후 2005년 7월 31일을 기준으로 공개되지 않은 특허가 본 보고서의 통계에 포함되지 않았기 때문이다.

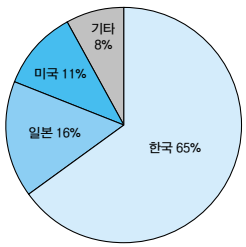
90년대 말부터 2000년대까지 이어지는 난수발생 관련 한국 특허출원의 경우, 난수발생장치 및 방법 자체에 대한 특허보다는 난수발생장치를 이용하여 데이터를 암호화하는 것에 대한 특허가 주를 이루고 있으며, 이는 90년대 말부터 급성장한 IT산업의 발전과 더불어 인터넷 상에서 중요시되는 각종 보안의 필요성의 대두에 의해 그와 관련한 특허가 다량 출원된 것으로 판단된다.

2. 국가별 특허 점유율

[표 2] 한국 내 국가별 특허 점유율

국가	한국	일본	미국	기타	계
출원건수	271	65	44	33	413

〈그림 7〉 한국 내 국가별 점유율



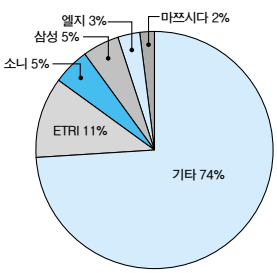
한국에서 출원된 난수발생 관련 특허의 국가별 점유율을 보면 한국 출원 특허가 65%로 가장 많은 점유율을 나타내고, 난수발생장치 및 방법 자체에 대한 특허보다는 이를 인터넷상에서의 보안과 관련한 암호화에 이용한 특허발명이 특징이며, 난수발생장치 및 방법 자체에 대한 발명은 일본 출원 특허가 주를 이루고 있음을 알 수 있다.

3. 기술분야/연구주체별 특허동향

[표 3] 한국 내 출원인별 출원동향

출원인	ETRI	SONY	삼성	엘지	마쯔시다	기타	계
출원건수	46	21	21	14	8	303	413

〈그림 8〉 한국 내 출원인별 특허동향



상위 5개 회사 외에는 기타로 분류하였음

한국 내의 출원인별 특허출원 동향을 보면 ETRI가 11%로 가장 많은 출원량을 보이며, 특이할 만한 점은 ETRI의 기관 성격상 한국의 출원이 난수발생장치를 이용한 보안에 관한 특허가 주를 이룸에 반해, ETRI의 출원은 난수발생장치 및 방법 자체에 관한 특허도 상당수를 포함하고 있다.

일본의 소니, 마쯔시다의 출원인 비율이 한국 내에서도 상당 비중을 차지하고 있는 것을 볼 수 있으며, 이들의 특허는 ETRI와 기술적으로 유사한 경향을 보이고 있다.

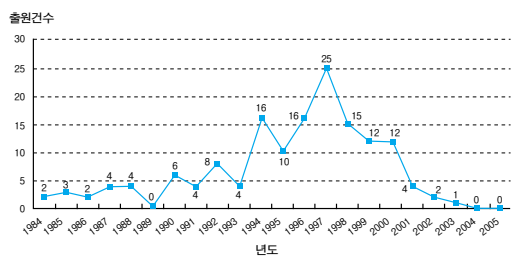
제 2 절 미국 특허동향

1. 연도별 특허동향

[표 4] 미국내 연도별 출원동향

년도	1984	1985	1986	1987	1988	1989	1990	1991	1992	1993	1994	계
출원건수	2	3	2	4	4	0	6	4	8	4	16	
년도	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	150
출원건수	10	16	25	15	12	12	4	2	1	0	0	

〈그림 9〉 미국 내 연도별 출원동향



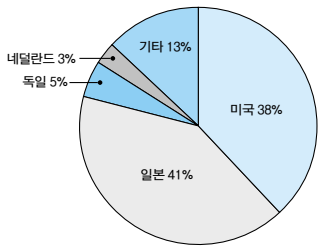
미국의 경우 난수발생관련 특허가 한국보다 조금 빠른 90년대 중반부터 증가세를 보이고 있다. 2000년 이후에는 급격한 감소세를 보이고 있으나, 이는 미국의 특허제도가 2002년 이후 등록제에서 공개제로 전환되면서 미국 등록특허만을 사용한 본 보고서의 통계상에 공개특허의 출원건수가 포함되지 않았기 때문이다.

2. 국가별 특허 점유율

[표 5] 미국 내 국가별 특허 점유율

국가	미국	일본	독일	네덜란드	기타	계
출원건수	58	62	7	4	20	150

〈그림 10〉 미국 내 국가별 점유율



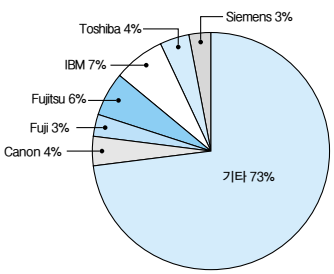
미국 내의 출원 국가별 특허 점유율을 살펴보면, 한국과는 다르게 일본이 가장 높은 점유율(41%)를 보이고 있음을 볼 수 있으며, 이는 일본에서 발명된 난수발생 장치 및 방법 자체에 관한 특허를 세계 특허 시장의 중심이라고 할 수 있는 미국 내에서 선 등록 받기 위해 다수 출원하였기 때문으로 판단된다.

3. 기술분야/연구주체별 특허동향

[표 6] 미국 내 출원인별 출원동향

출원인	Conon	Fuji	Fujitsu	IBM	Toshiba	Siemens	기타	계
출원건수	6	5	9	11	6	5	108	150

〈그림 11〉 미국내 출원인별 출원동향



미국 내의 난수발생관련 특허의 출원인별 동향을 보면, 앞서 국가별 점유율에서 볼 수 있었던 바와 같이 일본 업체의 주도가 눈에 띄게 드러난다. 다수 출원 업체 상위 6개 중, 일본 업체가 4개 업체나 포진되어 있으며 이들의 점유율을 합하면 17%로서, 미국 IBM의 7%를 2배 이상 넘어서는 수치이다. 이는 상위 6개 업체만을 선별한 결과이기 때문에 국가별 점유율에서의 일본 점유율인 41%에는 크게 못 미치지만, 다른 면에서 고찰해 보면 그 만큼 다수의 일본 업체가 미국 내에서 난수발생관련 특허를 출원했다고 판단할 수 있다.

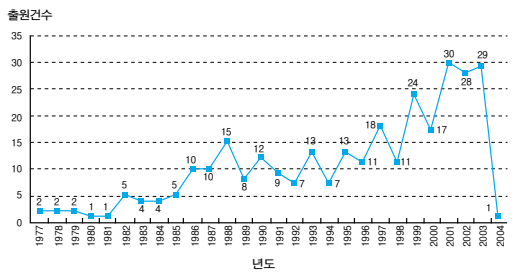
제 3 절 일본 특허동향

1. 연도별 특허동향

[표 7] 일본 내 연도별 출원동향

년도	1977	1978	1979	1980	1981	1982	1983	1984	1985	1986	1987	1988	1989	1990	계
출원건수	2	2	2	1	1	5	4	4	5	10	10	15	8	12	
년도	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	299
출원건수	9	7	13	7	13	11	18	11	24	17	30	28	29	1	

〈그림 12〉 일본 내 연도별 출원동향



일본은 앞서 한국과 미국의 난수발생 관련 특허동향에서 상당히 주도적인 위치를 보인 것과 같이 일본 내의 출원 또한 한국과 미국보다 거의 10년 정도 앞서는 1970년대 후반부터 시작되었음을 볼 수 있다. 출원량 또한 꾸준한 증가세를 보이고 있으며 2004년에 출원량이 급감한 것으로 나타나는 것은 출원 후 2005년 7월 31일을 기준으로 공개되지 않은 특허가 본 보고서의 통

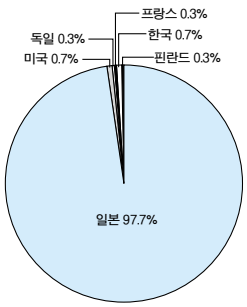
계에 포함되지 않았기 때문이다. 총 출원건수는 한국의 출원건수에 비해 다소 적으나 앞서 언급한 것처럼 일본의 경우 난수발생장치 및 방법 자체에 대한 특허가 주를 이루고 있기 때문에 출원량 대비 기술력에서는 한국에 크게 앞설 것으로 판단된다.

2. 국가별 특허 점유율

[표 8] 일본 내 국가별 특허 점유율

국가	일본	미국	독일	프랑스	한국	핀란드	계
출원건수	292	2	1	1	2	1	299

〈그림 13〉 일본내 국가별 점유율



일본 내 국가별 특허 점유율을 보면, 앞에서 언급한 한국과 미국의 현황을 통해 예측할 수 있는 것처럼, 일본 자체의 출원이 거의 대부분(98%)을 이루고 있으며, 추후 난수발생에 관련한 특허를 출원하는 업체의 경우, 필히 일본 특허에 대한 선행 기술 조사가 이루어져야 할 것임은 자명하다고 보여진다.

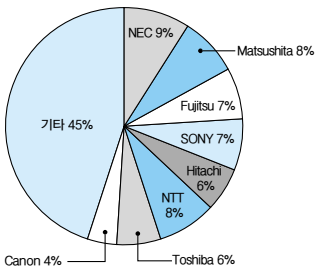
3 기술분야/연구주체별 특허동향

[표 9] 일본 내 출원인별 출원동향

출원인	NEC	Matsushita	Fujitst	SONY	Hitachi	NTT	Toshiba	Canon	기타	계
출원건수	28	24	22	21	17	24	17	12	134	299

일본 내의 출원인별 동향을 살펴보면, 국가별 점유율

〈그림 14〉 일본 내 출원인별 출원동향



에서 이미 예상할 수 있듯이, 한국 및 미국과는 달리 일본 업체가 상위 50% 이상을 모두 점유하고 있다. 특히 주목할 만한 점은 [표9]에서 보는 바와 같이 상위 8개업체의 출원량이 차이가 그리 크지 않다는 것이다. 이는 일본 내 유사업종의 다수 업체가 본 기술의 연구개발에 참여하고 있음을 고찰해 볼 수 있다.

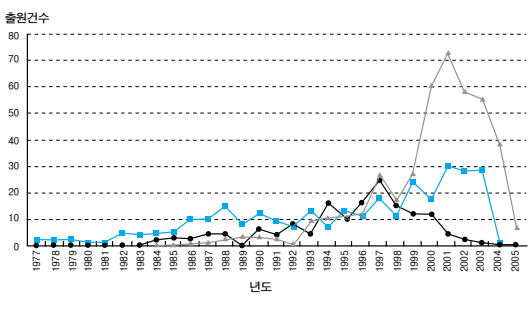
제 4 절 전체 특허동향 및 분석

1. 전체 특허동향

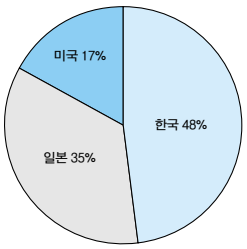
[표 10] 한미일 년도별 특허출원 개수

년도	~1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001~	계
한국	10	2	0	9	10	10	12	27	16	27	60	230	413
일본	81	9	7	13	7	13	11	18	11	24	17	88	299
미국	21	4	8	4	16	10	16	25	15	12	12	7	150
계	112	15	15	26	33	33	39	70	42	63	89	325	862

〈그림 15〉 한 · 미 · 일 3국의 출원동향



〈그림 16〉 한 · 미 · 일 3국의 특허출원 비율



2. 분석

난수발생 관련 특허의 출원은 한, 미, 일 모두 1990년대 후반부터 급증하기 시작하여 2000년대에도 꾸준한 성장을 보이고 있다. 통계상에는 한/미/일 3국 모두 최근 출원건수가 급감하는 것으로 나타나고 있으나, 이는 본 보고서의 해당 국가별 분석에서 이미 언급한 바와 같이, 한국 및 일본의 경우 출원 후 2005년 7월 31일을 기준으로 공개되지 않은 특허가 본 보고서의 통계에 포함되지 않았기 때문이고, 미국의 경우 미국의 특허제도가 2002년이후 등록제에서 공개제로 전환되면서 미국 등록특허만을 사용한 본 보고서의 통계상에 공개특허의 출원건수가 포함되지 않았기 때문이다.

결 론

난수발생장치 및 방법은 본 보고서의 서두에서도 언급하였듯이 인터넷의 발전에 따라 당연히 필요시 되는 부분으로써, 난수발생장치 및 방법 자체에 관한 기술개발과 더불어 이를 인터넷에 접목시켜 기존의 특허보다 한층 진보된 기술에 대한 개발이 동시에 이루어지고 있다.

일본의 경우 난수발생장치 및 방법 자체에 관한 특허가 전체 출원량의 상당부분을 차지하고 있으며, 특히 이러한 일본의 특허는 미국과 한국 내에도 다수 출원/등록되어 있는 상태이다.

한국의 경우는 ETRI가 일본의 출원경향과 유사한 방향으로 난수발생 관련 특허를 출원하고 있고, 기타 업체들은 난수발생장치를 인터넷에 접목시켜 보안과 암호화를 구현하는 기술에 대한 특허를 다수 출원하고 있다.

미국의 경우 일본과 유사한 방향으로 특허가 출원되고 있으나 출원량은 일본보다 현저히 적으며, 특히 다수의 일본업체들이 미국내에서 난수발생 관련 특허를 출원/등록받고 있어 향후 미국의 출원 형태가 어떤 방향으로 이루어질지 주목된다.

본 보고서를 작성하는 동안 한, 미, 일 의 여러 난수발생 관련 특허를 보던 중 난수발생장치의 시드값을 공급하기 위한 다양한 특허가 존재하고 있음을 알았고, 흥미로웠던 점은 과거에 주로 전자장치에서 발생하는 잡음을 시드값 발생원으로 이용하던 것에서 최근 촬상장치에 의해 촬상된 영상데이터의 픽셀데이터 값의 랜덤성을 이용하여 시드값을 생성하는 특허가 출원된 것이 조사되었고, 앞으로도 이처럼 우리 주변에서 랜덤성을 지닌 여러 데이터값으로 난수의 시드값을 생성하는 기술에 관한 특허가 다수 출원될 것이라는 예상할 수 있다.

[인용자료]

사이트
– 과학기술학회마을 : http://society.kisti.re.kr

논 문
– 난수 발생기의 비교
(A Note on Comparing the Random Number Generations)
저자 : 조영석, 권순일, 한영훈, 김미화, 신혜정,
출처 : 한국데이터정보과학회지, Journal of the Korean Data & Information Science Society,1225-8547, 제3권2호,pp.75-87, 1992

– 클라이언트-서버 환경에서 암호계를 위한 의사 난수 발생에 대한 연구
저자 : 김도완, 정태충
출처 : 한국정보과학회:학술대회지,
99 가을 학술발표논문집(I) – 한국정보과학회 , pp.649-651 , 1999

– 실 난수 발생기를 이용한 키 생성에 관한 연구
저자 : 차재현, 박중길, 전문석
출처 : 한국전자거래학회지 , 1226-3931 , 제6권2호 , pp.167-178 , 200