포렌식에서 디지털 증거의 우선순위 스케줄링

이종찬 · 박상준*

Priority Scheduling of Digital Evidence in Forensic

Jong-Chan Lee · Sang-Joon Park*

Department of Computer Information Engineering, Kunsan National University, Gunsan 573-701, Korea

요 약

범죄 증거의 새로운 형태인 디지털 증거는 기존의 증거와 기능 및 역할에 있어서 거의 차이점이 없으며, 증거로서의 법적 인정 및 역할이 점차 증가할 것으로 예상된다. 포렌식 수사관은 다수의 증거 보유 장치(예, 컴퓨터 시스템, 저장 매체 등)에 저장되어 있는 막대한 양의 데이터로부터, 사건과 관련된 실마리를 찾기 위하여 많은 시간을 소모해야 한다. 따라서 조사 시간을 단축하기 위해서는 잠재적인 관련 증거의 중요성에 근거하여 순서화 및 순위화가 필요하다. 본 연구에서는 포렌식 조사 시에, 정확한 증거를 선정하게 함으로서 증거 분석 우선순위를 결정하는 방법을 제안한다. 제안된 방식은 증거 조사 소요시간, 증거의 가치, 증거간의 연관성 그리고 사건과 시간과의 연관성과 같은 다수의 부정확한 요소가 퍼지 집합 함수를 사용한 의사 결정에 사용되는 다기준 의사 결정에 근거한다.

ABSTRACT

Digital evidence which is the new form of evidence to crime makes little difference in value and function with existing evidences. As time goes on, digital evidence will be the important part of the collection and the admissibility of evidence. Usually a digital forensic investigator has to spend a lot of time in order to find clues related to the investigation among the huge amount of data extracted from one or more potential containers of evidence such as computer systems, storage media and devices. Therefore, these evidences need to be ranked and prioritized based on the importance of potential relevant evidence to decrease the investigate time. In this paper we propose a methodology which prioritizes order in which evidences are to be examined in order to help in selecting the right evidence for investigation. The proposed scheme is based on Fuzzy Multi-Criteria Decision Making, in which uncertain parameters such as evidence investigation duration, value of evidence and relation between evidence, and relation between the case and time are used in the decision process using the aggregation function in fuzzy set theory.

키워드 : 디지털증거, 조사, 포렌식, 퍼지 다기준 의사 결정

Key word : Digital Evidence, Investigation, Forensic, FMCDM, etc

접수일자 : 2013. 04. 20 심사완료일자 : 2013. 09. 04 게재확정일자 : 2013. 09. 12

* **Corresponding Author** Sang-Joon Park(E-mail:lubimia@kunsan.ac.kr, Tel:+82-63-469-4859)

Department of Computer Information Engineering, Kunsan National University, Gunsan 573-701, Korea

Open Access <http://dx.doi.org/10.6109/jkiice.2013.17.9.2055>

print ISSN: 2234-4772 online ISSN: 2288-4165

©This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(<http://creativecommons.org/licenses/by-nc/3.0/>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
Copyright © The Korea Institute of Information and Communication Engineering.

I. 서 론

IT 기술의 발전 및 급격한 정보화 사회로의 변화는 정보의 디지털화를 가속화시키고 있으며, 현재 그리고 기존에 생성된 정보의 대부분이 디지털 기술로 저장 또는 사용되므로 디지털 증거(digital evidence)는 가장 보편적인 증거 형태가 될 것으로 예상된다. 컴퓨터 관련 범죄뿐만 아니라 일반 범죄에서도 컴퓨터를 포함한 디지털 정보기에 주요 증거와 단서를 보관하는 경우가 증가함에 따라, 증거 수집 및 분석을 위한 전문적인 디지털 포렌식 기술이 요구되고 있다. 디지털 포렌식은 디지털 증거 자료의 수집, 보존, 분석, 문서화, 그리고 재판 과정에서 증거로 제출하기까지의 모든 과정을 포함하는데, 지금까지는 컴퓨터의 하드디스크에 있는 개인작성의 데이터를 확보하는 것이 주류였으나 디지털 기술의 발달로 그 증거자료가 네트워크, 인터넷, 데이터베이스, 모바일, 휘발성 메모리 등 다양한 곳에서 존재함으로써 그 전문성이 더욱 심화되고 있다[1-3]

포렌식에서 가장 중요한 요건은 증거 수집과, 그 증거로부터 얼마나 신속히 사건을 인지하고 정확하게 분석하여 사건을 재구성하는 가이다. 그러나 디지털 증거는 원본과 복사본의 구분이 어렵고 조작 및 생성, 전송, 삭제가 매우 용이하기 때문에, 의도적 삭제, 증거 은닉 등과 같은 안티 포렌식(Anti-Forensic) 등을 고려하여야 한다. 이와 같은 디지털 데이터가 법적 증거가 되기 위해서는 크게 증거 수집 단계, 증거 조사 단계, 증거 분석 단계, 증거 제출 단계와 같은 과학적이고 체계적인 포렌식 절차를 통하여 디지털 증거의 신뢰성을 확보해야 한다[3-4].

포렌식 수사의 주요단계는 현장에서의 증거수집으로부터 시작된다. 지능적인 용의자는 포렌식 수사관 시각으로 증거를 은닉하는 방법을 사용하기 때문에, 사건 현장에서 사건의 본질에 연관된 중요한 증거를 확보할 수 있다. 증거를 확보하기 위해서는 사건의 본질에 따라서 상당한 시간이 소요된다. 예를 들어, 용의자의 3 Tera 기억장치를 복사(bit stream 복사)하기 위해서는 10시간 이상이 소요될 수 있다(미국 Intelligent Computer Solution의 포렌식용 HDD 복제 툴 'Solo4'기준). 특히 범죄 수사 절차를 습득하고 있는 용의자들은 진보된 기술을 이용하여 증거를 남기지 않거나 은닉하려는 시도를 반복적으로 수행함으로써, 정보 복구와 은닉 정보의 탐색에

상당한 시간이 소요된다. 이런 상황 하에서 수집된 증거를 분석하기 위해서는 또한 상당한 비용 및 시간이 소요될 수 있다[5-6]. 따라서 디지털 증거가 포함된 조사 과정은 물리적 증거의 조사과정에 비하여 절차가 복잡할 뿐만 아니라 시간 소요 문제를 유발할 수 있다. 즉, 대부분의 디지털 증거는 암호 알고리즘으로 보호되는 잠재적 데이터와 파일을 포함하기 때문에, 디지털 증거와 관련된 대표적인 범죄 사례인 명의도용의 경우 포렌식 수사를 위하여 25-30여개의 증거를 필요로 한다.

포렌식 수사관은 범죄의 형태에 따라 증거의 조사상의 가치와 소요시간을 반드시 인지해야 한다. 사건에 대한 증거들을 확보한 후에, 취득한 증거를 그 가치와 소요시간 등의 디지털 증거 요소(digital evidence parameter)에 근거하여 순서화할 필요가 있다. 따라서 본 연구에서는 현장에서 증거가 수집된 후에, 수집된 증거들의 분석 우선순위를 결정함으로써 최적의 증거 선정과 스케줄링을 수행하는 DePS(Digital Evidence Priority Scheduler)를 제시한다. 이를 통하여 불필요한 증거를 제거할 수 있으며, 최적의 조사시간을 유지할 수 있고, 최적의 분석을 유도할 수 있다.

II. 증거의 순서화 기본 구조

그림 1. DePS의 증거선정 절차

Fig. 1 Evidence Selection Procedure of DePS

그림 1은 디지털 증거 선정을 위한 블록 다이어그램을 보인다. 퍼지화 모듈은 증거 선정 정보를 받은 후, 각 소속 함수를 통하여 적절한 퍼지 입력 제어량(fuzzy input vector)으로 변환한다. 퍼지 추론 엔진에서 퍼지

규칙을 이용하여 증거 선정 요소의 수준에 대한 소속 함수 값, 증거 선정 정책에 대한 가중화된 소속 함수 값 등의 퍼지 출력 제어량(fuzzy output vector)을 결정한다. 마지막으로 이 퍼지 제어량은 비퍼지화 모듈을 통하여 증거 순위 결정을 위한 실수 값으로 변환된다.

III. DePS 구조

3.1. 퍼지화 모듈

퍼지화 모듈에서는 디지털 증거 선정 요소의 입력 값이 소속 함수에 의하여 적절한 퍼지 입력 제어량으로 변환된다.

3.1.1. 증거 선정 요소를 위한 의사결정함수 결정

증거 선정 요소로서 증거 조사 소요 시간, 증거의 가치, 증거간의 연관성, 그리고 사건-시간과의 연관성을 고려한다. 선정 요소와 그 요구 사항은 표 1과 같다.

표 1. 주 선정 요소와 요구사항

Table. 1 Main selection parameter and requirements

증거 선정 요소	요구 사항
증거의 가치(V)	가치의 최대화
증거간의 연관성(E)	증거간의 연관성의 최대화
사건-시간과의 연관성(S)	사건과 시간과의 연관성 최소화

- 디지털 증거의 조사 소요 시간이 고려된다. 매년 포렌식 수사관이 조사해야 할 증거의 양은 기하급수적으로 증가되고 있다. 이런 현실에서 방대한 양의 로그와 대용량 디스크의 수많은 데이터를 전수조사하거나 여러 가지 단순도구나 스크립트를 사용해서 증거물을 수집하기 위해서는 많은 시간이 소요된다. 위와 같은 이유로 해당 사건이 증거로부터 분석에 많은 시간이 소요되는 지 여부는 극히 중요한 요소이다. 상대적으로 적은 시간에 획득될 수 있는 증거와 휘발성 데이터나 임시 파일 시스템과 같이 생존 시간이 짧은 데이터를 가진 증거의 경우는 높은 우선순위를 가져야 한다.
- 디지털 증거의 가치가 고려된다. 각 사건에서 수집된 증거의 가치를 판단하는 기준으로서, 특히 사이버 침해사고의 경우 수많은 데이터에서 침해사고의 증거

를 정확히 식별하고 포렌식 절차에 맞추어 증거를 수집하는 것은 어렵다. 증거의 가치 판단 여부에 따라, 그 사건 전체의 해결에 상당한 영향을 미친다.

- 디지털 증거간의 연관성이 고려된다. 수집된 증거들 간에는 연관성을 가지고 있으므로, 각 사건의 형태에 따라 연관성이 있는 증거들을 연속적으로 분석함으로써 범죄 사건의 효율적인 분석이 가능하다.
- 시간과의 연관성이 고려된다. 어린이 유괴, 성도착자, 실종자 탐문 등과 같은 범죄 사건의 경우는, 사건 해결에 시간이 가장 중요하다. 이런 종류의 사건에서, 혐의자 또는 범죄현장을 다루는 포렌식 수사관은 신속한 증거 확보 및 분석이 필요하다.

$D_i(i=1,2,...,n)$ 를 증거 선정 요소 $Y_j(j=1,...,4)$ 에 의하여 평가되는 대안들, 즉 증거 후보로 정의하자 [7-8]. 각 증거 후보가 증거 선정 요소를 만족시키는 정도를 표현하기 위하여 의사 결정 매트릭스 X 를 식 (1)과 같이 정의한다.

$$X = \begin{bmatrix} T_{11} & V_{12} & E_{13} & S_{14} \\ T_{21} & V_{22} & E_{23} & S_{24} \\ \vdots & \vdots & \vdots & \vdots \\ T_{n1} & V_{n2} & E_{n3} & S_{n4} \end{bmatrix} \quad (1)$$

여기서, x_{i4} 는 증거 선정 요소 $Y_j(j=1,2,3,4)$ 을 갖는 증거 후보들 $D_i(i=1,2,...,n)$ 의 언어적 판단 결과를 나타낸다. 이는 VP, P, F, G, VG의 언어 변수 집합으로 표현한다. 의사 결정 매트릭스에 사용된 증거의 퍼지 수는 그림 2와 같다. 여기서 X 축은 증거의 퍼지 수, Y축은 각 증거의 소속 함수 값을 나타낸다.

그림 2. 증거 요소를 위한 의사 결정 매트릭스

Fig. 2 Decision matrix for evidence parameters

3.1.2. 증거 선정 요소를 위한 가중치 벡터 결정

증거 선정 요소에 대한 가중치 벡터 W 은 식 (2)와 같이 표현된다.

$$W = (w_j^T, w_j^V, w_j^E, w_j^S) \quad (2)$$

여기서 w_j 는 각 증거 후보들 $D_j(j=1,2,...,n)$ 의 가중치이다. 이는 LTI(Least Important), LSI(Less Important), I(Important), MEI(More Important), MTI(Most Important)의 언어 변수 집합으로 표현한다. X 축은 가중치의 퍼지 수, Y축은 가중치 값을 나타낸다. 가중치 벡터 W 의 소속 함수는 그림 3과 같다.

그림 3. 증거 요소를 위한 가중치 벡터
Fig. 3 Weighting vector for evidence parameters

3.2. 퍼지 규칙

3.2.1. 가중치 벡터 결정

가중치는 아래의 두 조건에 근거하여 표 2와 같이 가중치를 결정한다.

표 2. 증거 후보의 상태 수준과 가중치 결정 규칙

Table. 2 State Information of candidate evidence and rule for deciding weighting value

규칙	증거의 상태 수준		가중치			
	시간성	가치성	T	V	E	S
1	Low	Low	I	I	I	I
2	Low	Middle	MEI	MTI	MTI	MEI
3	Low	High	MTI	MTI	MTI	MTI
4	Middle	Low	LSI	LSI	LSI	LSI
5	Middle	Middle	I	MEI	I	I
6	Middle	High	MEI	MTI	MEI	MEI
7	High	Low	LTI	LTI	LTI	LTI
8	High	Middle	LSI	I	I	LSI
9	High	High	I	MTI	LTI	LTI

① 범죄 사건의 형태에 따른 가중치 결정 - 증거 확보 시간이 극히 민감한 사건인지, 아닌 지의 여부에 따라 가중치를 결정한다.

② 증거가 갖는 가치 형태에 따른 가중치 결정 - 사건에 따라 증거의 가치가 서로 다르므로, 그 형태에 따라 해당 파라미터에 높은 가중치를 부여한다.

3.2.2. 소속 함수 값 결정 규칙

본 연구에서는 [9]에서 제시한 퍼지 언어변수 모형을 이용하고 이를 근거로 퍼지 소속 함수를 정의한다. 각 증거 후보의 선정 요소의 수준에 대한 소속 함수 값을 정의하면 표 3과 같다. 여기서 적용할 퍼지 소속 함수의 수준은 식 (3-6)에서 산출된 μ_R 의 값에 의하여 결정된다.

표 3. 증거 요소에 대한 소속 함수

Table. 3 Membership function for parameters

파라미터	수준	소속 정도				
		VP	P	F	G	VG
T	T1	0	0	0	0.5	1.0
	T2	0	0.5	0.5	0.7	0
	T3	1.0	0.5	0	0	0
V	V1	0	0	0	0	1.0
	V2	0	0.3	0.7	0.5	0
	V3	1.0	0	0	0	0
E	E1	0	0	0	0.5	1.0
	E2	0	0	0.5	0.7	0
	E3	1.0	0.5	0.5	0	0
S	S1	0	0	0	0.8	1.0
	S2	0	0	0.5	1.0	0.5
	S3	1.0	0.7	0.5	0	0

현장에서 수집된 증거의 조사 시간을 이용하여 $\mu_R(T_i)$ 를 정의하고 이를 식 (3)에 보인다. 여기서 T_i 은 각 증거 조사에 걸리는 시간을 의미한다. t_1 는 하한 값(lower_limit)이고 t_2 는 상한 값(upper_limit)이다.

$$\mu_R(T_i) = \begin{cases} 1, & T_i < t_2 \\ 1 - \frac{|T_i - t_2|}{|t_1 - t_2|}, & t_2 \leq T_i \leq t_1 \\ 0, & T_i > t_1 \end{cases} \quad (3)$$

증거의 가치에 근거하여 소속 함수 $\mu_R(V_i)$ 를 식 (4)와 같이 정의한다. 여기서 V_i 는 증거의 가치를 나타내

고, v_1 은 하한 값, v_2 는 상한 값이다.

$$\mu_R(V_i) = \begin{cases} 0, & V_i < v_2 \\ 1 - \frac{|V_i - v_1|}{|v_1 - v_2|}, & v_2 \leq V_i \leq v_1 \\ 1, & V_i > v_1 \end{cases} \quad (4)$$

증거간의 연관성을 이용하여 소속 함수 $\mu_R(E_i)$ 를 식 (5)와 같이 정의한다. E_i 는 증거간의 연관성을 나타내고, e_1 은 하한 값, e_2 는 상한 값이다.

$$\mu_R(E_i) = \begin{cases} 0, & E_i < e_2 \\ 1 - \frac{|E_i - e_1|}{|e_1 - e_2|}, & e_2 \leq E_i \leq e_1 \\ 1, & E_i > e_1 \end{cases} \quad (5)$$

시간과의 연관성을 이용하여 소속 함수 $\mu_R(S_i)$ 을 정의하고 식 (6)에 보인다. 여기서 S_i 는 사건과 시간 사이의 연관성을 나타내고, s_1 은 하한 값, s_2 는 상한 값을 나타낸다.

$$\mu_R(S_i) = \begin{cases} 0, & S_i < s_2 \\ 1 - \frac{|S_i - s_1|}{|s_1 - s_2|}, & s_2 \leq S_i \leq s_1 \\ 1, & S_i > s_1 \end{cases} \quad (6)$$

3.3. 퍼지 추론 엔진

퍼지 추론 엔진은 퍼지 규칙을 이용하여 증거 선정을 위한 퍼지 제어량을 산출한다.

3.3.1. 소속 정도의 계산

각 증거 선정 정책에 따라 각 증거의 소속 정도를 구하기 위하여, 각 증거 선정 요소의 선정 정도를 산출해야 한다. 산출된 각 증거 선정 요소에 대한 소속 정도를 구하기 위하여 [9]에서 정의된 소속정도 계산 방식을 확장하여 식 (7)에 적용하였다.

$$R_{ij} = \frac{\mu_R}{\sum_n F_{ijn}} \otimes \left[\begin{matrix} VG \\ (+) \\ n = VP \end{matrix} Q_{ijn} \oplus F_{ijn} \right] \quad (7)$$

여기서,

i = 증거 후보

j = 증거 선정 요소

n = 소속 정도를 나타내는 언어 변수 값 즉, $n = \{VP, P, F, G, VG\}$

Q_{ijn} = 증거 후보 i , 증거 선정 요소 j 의 수준에 대한 퍼지 수

F_{ijn} = 증거 후보 i , 증거 선정 요소 j 의 수준에 대한 소속 함수 값

3.3.2. 가중화된 소속 정도 결정

퍼지화 절차를 통하여 성능 매트릭스 $\delta \in [0, 1]^{i \times 4}$ 을 산출한다. 여기서 각 요소 δ_{i4} ($i = 1, 2, \dots, n$)은 i -번째 증거 후보가 각 선정 요소를 어느 정도 만족하는가를 나타낸다[7-8]. 산출된 의사 결정 매트릭스에 가중치 벡터의 논리곱으로서, 식 (8)의 성능 매트릭스를 산출한다.

$$\delta_{i4} \cong \begin{bmatrix} \delta_{11} & \delta_{12} & \delta_{13} & \delta_{14} \\ \delta_{21} & \delta_{22} & \delta_{23} & \delta_{24} \\ \vdots & \vdots & \vdots & \vdots \\ \delta_{i1} & \delta_{i2} & \delta_{i3} & \delta_{i4} \end{bmatrix} \quad (8)$$

퍼지 추론 엔진으로부터 식 (9)의 퍼지 출력 제어량은 다음의 근사공식에 의하여 구할 수 있다. 여기서 증거 선정 요소에 대한 소속 정도는 $R_{ij} = (o_{ij}, p_{ij}, q_{ij}, r_{ij})$, 가중치 결정 규칙은 $W_j = (w_{ij}, x_{ij}, y_{ij}, z_{ij})$ 이라고 정의한다. 중심 가중 평균(center weighted average) 방식을 사용하여 퍼지수를 산출한다.

$$\delta_i \cong (\delta_{i1}, \delta_{i2}, \delta_{i3}, \delta_{i4}) \quad (9)$$

여기서,

$$\delta_{i1} = \sum_{j=T}^S \frac{o_{ij} \cdot w_{ij}}{w_{ij}}, \delta_{i2} = \sum_{j=T}^S \frac{p_{ij} \cdot x_{ij}}{x_{ij}}, \delta_{i3} = \sum_{j=T}^S \frac{q_{ij} \cdot y_{ij}}{y_{ij}}, \delta_{i4} = \sum_{j=T}^S \frac{r_{ij} \cdot z_{ij}}{z_{ij}} \text{ 이다.}$$

3.4. 비퍼지화 모듈

퍼지 추론 제어량은 비퍼지화를 위하여 실수 값으로 변환되고 실제 제어 가능한 양으로 변경해야 한다. 본

연구에서는 소속 정도 퍼지 집합을 순위화하기 위하여 GMV(Generalized Mean Value) 방법을 사용한다. 가중화된 소속 정도 $m(\delta_i)$ 에 대한 GMV는 식 (10)로부터 계산된다. $m(\delta_i)$ 이 크면 클수록 선정 가능한 최적의 증거가 된다.

$$m(\delta_i) = \frac{(\delta_{i3} + \delta_{i4})^2 - (\delta_{i1} + \delta_{i2})^2 + \delta_{i1} \cdot \delta_{i2} - \delta_{i3} \cdot \delta_{i4}}{3 \cdot [(\delta_{i3} + \delta_{i4}) - (\delta_{i1} + \delta_{i2})]} \quad (10)$$

IV. 시뮬레이션과 성능평가

제안된 방법의 타당성을 검증하기 위하여 특정 사건에 대한 증거들을 확보하고 이를 순서화함으로써 순서화하지 않았을 경우와의 비교·평가를 수행한다. 특정 사건과 관련된 모든 정보는 성공적으로 획득되었다고 가정하며, 증거의 선택 및 순서화를 통한 스케줄링에 중점을 둔다. 표 4와 같이 특정 사건으로부터 확보된 16개의 증거를 가정한다. DePS의 성능을 평가하기 위하여 시뮬레이터 저작 도구인 MODSIM을 이용하여 시뮬레이션프로그램인 ForensicSimulatorV1-1을 개발하고 이를 바탕으로 하여 시뮬레이션을 수행하였다.

표 4. 증거들에 대한 평가 값
Table. 4 Evaluation value for evidences

증거	선정요소	증거조사 소요시간	증거의 가치	증거 연관성	사건-시간 연관성
증거 1		0.3	0.5	1	0.7
증거 2		1	1	0.7	0.7
증거 3		0.6	0.5	0.3	0.8
증거 4		0.7	0.9	0.4	1
증거 5		0.7	1	0.7	0.8
증거 6		0.5	0.3	0.5	1
증거 7		0.3	0.3	0.5	0.3
증거 8		0.7	0.7	0.7	0.7
증거 9		0.3	0.6	0.9	0.6
증거 10		0.3	0.4	0.4	0.1
증거 11		0.6	0.5	0.6	0.4
증거 12		0.5	0.5	0.2	0.4
증거 13		0.4	0.7	0.4	0.2
증거 14		0.7	0.3	0.8	0.2
증거 15		0.5	0.9	1	0.7
증거 16		1	0.6	0.2	0.9

그림 4는 전체적인 시뮬레이션 시나리오를 보인다. 평가 시스템은 취득된 16개의 증거를 입력으로 DePS를 실행함으로써 증거의 분석 우선순위를 결정한다. 불필요한 증거를 배제하고, 분석을 위한 최적의 증거 집합을 선정하고 증거 분석 시간을 산정한다.

그림 4. 시뮬레이션 시나리오
Fig. 4 Simulation scenario

그림 5는 증거들의 수에 따른 분석 시간을 비교한 결과이다. 여기서 Random 방식은 증거들을 무작위로 선정하여 분석 시간을 산출한 방식이다. 분석시간은 최대 임계치로 48시간으로 한정하였으며, 그래프의 Y축은 분석 시간으로서 48시간을 백분율로 계산하였다.

그림 5. 분석 시간의 비교
Fig. 5 Comparison of time of analysis

DePS는 Random 방식에 비하여 분석 시간이 현저히 감소됨을 알 수 있다. 이는 수집된 증거들의 분석 우선순위를 결정함으로써 최적의 조사시간을 유지할 수 있고, 최적의 분석을 유도할 수 있기 때문이다. 또한 우선 순위가 낮은 증거의 경우, 증거 분석 효율에 미치는 영

향이 줄어들게 되어 시스템 전체적으로 분석 시간을 줄이는 결과를 가져온다. 특히 Random 방식의 경우, 분석할 증거의 수가 증가함 (여기서는 7개 이상)에 따라 분석 시간 배분의 불균형으로 인하여 분석 시간이 현저히 증가함을 알 수 있다.

V. 결 론

본 연구에서는 사건 현장에서 수집된 증거들의 분석 우선순위를 결정함으로써 최적의 증거를 선정하고 스케줄링 방법을 제시하였다. 제안된 방식은 다기준 의사 결정을 이용하여, 증거 조사 소요시간, 증거의 가치, 증거간의 연관성 그리고 사건과 시간과의 연관성과 같은 다수의 부정확한 요소를 기반으로 증거의 우선순위를 결정한다. 이를 통하여 불필요한 증거의 제거, 최적의 조사시간 유지, 그리고 최적의 분석을 유도할 수 있다.

감사의 글

이 논문은 2012학년도 군산대학교 대학자체 학술공모과제 연구비 지원에 의하여 연구되었음.

REFERENCES

- [1] Digital Forensic. Available: <http://blog.naver.com/gadzetlee/90016576709>.
- [2] H. Yang, M. Xu and N. Zheng, "Improved Method for Ranking of Search Results Based on User Interest" in *Proceeding of IFIP International Conference on Network and Parallel Computing*, Shanghai, pp. 132-138, 2008.
- [3] K. Krishna, A. Kalpana, and T. Velayutham, "Customizable Ranking Method for Digital Evidence Search through Interestingness Injection," in *Proceeding of Third International Conference on Multimedia Information Networking and Security*, Shanghai, pp. 288-291, 2011.
- [4] S. Saleem, O. Popov, and R. Dahman, "Evaluation of security methods for ensuring the integrity of digital evidence," in *Proceeding of International Conference on Innovations in Information Technology*, Abu Dhabi, pp. 220-225, 2011.
- [5] A. Grillo, A. Lentini, G. Me, and M. Ottoni, "Fast user classifying to establish forensic analysis priorities," in *Proceeding of Fifth International Conference on IT Security Incident Management and IT Forensics*, Stuttgart, pp. 69-77, 2009.
- [6] E. Mabuto and H. Venter, "User-generated digital forensic evidence in graphic design applications," in *Proceeding of International Conference on Cyber Security, Cyber Warfare and Digital Forensic*, Kuala Lumpur, 195-200, 2012.
- [7] C. Naso and B. Turchiano, "A Fuzzy Multi-Criteria Algorithm for Dynamic Routing in FMS," in *Proceeding of International Conference on Systems, Man, and Cybernetics*, pp. 457-462, 1998.
- [8] C. H. Yeh and H. Deng, "An Algorithm for Fuzzy Multi-Criteria Decisionmaking," in *Proceeding of International Conference on Intelligent Processing Systems*, Beijing, pp. 1564-1568, 1997.
- [9] S. Y. Jung and S. K. Cho, "Determination of Risk Level Using Fuzzy Multi - Criteria Decision Method," *Journal of the Korean Institute of Industrial Engineers*, Vol.24, No.4, pp. 627-638, Dec. 1998.

이종찬(Jong-Chan Lee)

1996년: 송실대학교 컴퓨터학과 (공학석사)
 2000년: 송실대학교 컴퓨터학과 (공학박사)
 2000년 ~ 2005년: ETRI 연구원
 2005년 ~ 현재: 국립군산대학교 부교수
 ※관심분야: 디지털 포렌식, 역공학

박상준(Sang-Joon Park)

1998년: 송실대학교 컴퓨터학과 (공학석사)
2002년: 송실대학교 컴퓨터학과 (공학박사)
2002년 ~ 2003년: 런던대 ISG 박사후과정
2004년 ~ 2007년: 송실대학교 전임연구교수
2007년 ~ 현재: 국립군산대학교 부교수
※관심분야: B3G 이동통신, 인터넷 망 분석