Journal of Convergence for Information Technology
Vol. 9. No. 1, pp. 92-98, 2019
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2019.9.1.092

홀로그램 용 증강현실 객체의 네트워크 랜더링을 위한 보안 기법 설계

김석수[1*], 김동현[2]
[1]한남대학교 멀티미디어 교수, [2]한남대학교 멀티미디어학과 학생

Design of Security Method for Network Rendering of Augmented Reality Object

Seoksoo Kim[1*], Donghyun Kim[2]
[1]Professor, Multimedia , Hannam University
[2]Student, Multimedia , Hannam University

요 약 홀로그램 디스플레이 기술의 발전으로 인하여 증강현실에 대한 실감형 콘텐츠를 제공하기 위한 다양한 연구들이 진행되고 있다. 홀로그램용 HMD의 경우 소형의 프로세서에서 증강현실의 객체를 랜더링하여 제공하여야 하기 때문에 저용량의 콘텐츠를 사용해야하는 문제점이 있어 이를 해결하고자 네트워크를 통해 콘텐츠의 리소스를 제공하여 랜더링하는 기술이 필요하다. 기존의 증강현실 시스템의 경우 내부 저장 공간에서 리소스를 불러와 랜더링하기 때문에 콘텐츠 변조의 문제점이 없으나 네트워크를 통해 리소스를 제공할 경우 콘텐츠의 변조, 악의적인 코드 삽입 등 보안의 문제점을 고려해야 한다. 따라서 본 논문에서는 홀로그램 HMD 디바이스에서 증강현실 콘텐츠를 제공함에 있어 보안 기법을 적용한 네트워크 랜더링 기법을 제안한다.

주제어 : 증강현실, 랜더링, XML 암호화, 3D 워터마킹

Abstract Due to the development of hologram display technology, various studies are being conducted to provide realistic contents for augmented reality. In the case of the HMD for hologram, since augmented reality objects must be rendered by a small processor, it is necessary to use a low-capacity content. To solve this problem, there is a need for a technique of rendering resources by providing resources through a network. In the case of the existing augmented reality system, there is no problem of contents modulation because the resources are loaded and rendered in the internal storage space. However, when providing resources through the network, security problems such as content tampering and malicious code insertion should be considered. Therefore, in this paper, we propose a network rendering technique applying security techniques to provide augmented reality contents in a holographic HMD device.

Key Words : Augmented Reality, Rendering, XML Encryption, 3D Watermarking

*This work (Grants No. C0549901) was supported by project for Cooperative R&D between Industry, Academy, and Research Institute funded Korea Ministry of SMEs and Startups in 2017.

*Corresponding Author : Seoksoo Kim(sskim@hnu.kr)

Received November 26, 2018 Revised December 20, 2018
Accepted January 20, 2019 Published January 28, 2019

1. 서론

가상현실 기술의 발전에 더불어 사물인터넷(Internet of Things), 컴퓨터 비전, 인공 지능 등 ICT(Information Communication Technology) 핵심 기술들이 발전하면서 첨단센서를 통해 현실 환경 정보를 습득하고 이를 통해 사용자에게 다양정보와 편의를 제공해주는 서비스들이 실생활에 적용되기 시작하였다.

이러한 서비스들의 변화로 인하여 현실 환경 정보를 기반으로 한 데이터, 음성 및 영상과 같은 멀티미디어 콘텐츠들을 제공하는 실감 콘텐츠에 대한 관심이 높아지게 되었다[1].

HMD(Head Mounted Display) 기술의 발전으로 가상현실을 증강현실의 형태로 구현하면서 증강현실은 가상현실의 한 분야로써 정의 내려졌다. 이로 인해 가상·증강현실 시장은 HMD 기기에서 효율적으로 실감 콘텐츠를 제공하는 가상현실 기술들이 주도하고 있다[2].

증강현실 HMD들의 경우 현실공간에 가상의 정보를 합성하기 위한 방안에 대한 연구를 중심으로 연구가 진행되고 있다.

그러나 증강현실 HMD 기기들은 추가적인 디바이스 없이 독립적인 형태로 구성되어 있기 때문에 모바일 디바이스의 하드웨어적 한계 중 데이터저장 공간 및 프로세스 처리속도에 대한 문제점으로 인하여 대용량, 다수의 콘텐츠를 제공할 경우 사용자에게 제공하는 어플리케이션의 용량이 증가하거나 데이터를 처리하는 속도가 감소되어 실시간 콘텐츠 제공시 딜레이 타임이 존재하여 객체 증강에 문제점이 존재한다.

이를 위해서 현실대상의 객체를 실시간으로 인식하고 이에 대한 좌표를 물리기반 모델링을 통해 서버에서 전송된 리소스 또는 오브젝트 정보를 물성치에 따른 외형정보로 변경하여 증강하는 네트워크 랜더링에 대한 연구가 진행되고 있다.

그러나 이와 같은 방식들은 전송되는 리소스, 오브젝트에 대한 보안 검사 또는 암호화 작업이 이루어지지 않아 변조된 리소스 또는 악성코드를 배포하기 위한 태그 정보가 포함되어 전송되는 오브젝트에 대한 취약점이 존재한다.

따라서 본 논문에서는 깊이 인식 카메라, 적외선 센서를 이용하여 3차원 공간정보를 획득하고 획득한 정보를 기반으로 증강되는 객체를 암호화하여 네트워크를 통해 제공하는 랜더링 시스템을 적용한 입체 증강현실 시스템을 제안한다.

2. 관련 연구

네트워크를 통해 증강되는 콘텐츠의 리소스를 제공하기 위해서는 3차원 오브젝트의 Geometry 정보가 태그 형태로 구성되어야 한다.

3차원 오브젝트의 리소스 포맷 중 태그 형태를 가지는 포맷은 ASE, XML이 있다.

ASE 파일의 경우 보안 태그를 삽입하기 어려우나 XML 파일의 경우 자체적 보안 표준 기법이 적용되어 인가되지 않은 사용자의 경우 태그의 접근이 불가능하다.

그러나 XML 보안 표준 기법의 경우 엘리먼트와 같은 아주 작은 단위의 접근이 불가능하다.

아주 작은 단위의 태그나 엘리먼트의 접근이 불가능할 경우 랜더링시 Geometry의 Vertex 정보에 대한 좌표 정합이 되지 않아 랜더링이 불가능하다는 문제점이 있다.

따라서 XML 문서의 접근 제어의 경우 문서의 집합이나 하나의 엘리먼트 등 다양한 단계에서 접근이 가능하도록 지원해야한다.

XML DOM 트리[3]는 XML 문서의 엘리먼트에 접근할 수 있는 API를 제공한다.

XML 문서에 대한 접근 제어에 있어서 전체의 DOM 트리가 메모리 상에 적재되어야 하고, DOM 트리의 모든 노드에 접근 권한을 설정하기 위한 반복적인 트리의 모든 노드에 접근 권한을 설정하기 위한 반복적인 트리 검색으로 인하여 많은 메모리가 사용되며 복잡한 권한의 평가 과정으로 인하여 실시간으로 제공되어야 하는 디지털 콘텐츠의 경우 표준화된 XML 암호화 기법을 사용하기가 어렵다.

이를 해결하고자 실시간으로 제공되는 콘텐츠에 대하여 XML 암호화를 적용하여 패키징하는 기법이 연구되었다[4].

이 기법들은 콘텐츠의 메타데이터의 형식에 따라 태그를 분류하여 구성하는 방식으로 디지털 콘텐츠의 유통에 관여한 모든 참여자들의 메타데이터를 하나로 구성하는 정적(static)인 메타데이터, 디지털 콘텐츠의 메타데이터를 공통 영역과 특정 영역으로 구분하여 구성하는 동적(dynamic) 메타데이터, 참여자가 디지털 콘텐츠의 메타데이터를 첨부해 나가는 계층 메타데이터로 분류한다.

분류된 메타데이터로 구성된 XML 문서는 인증 과정

을 거친 사용자가 문서를 요청하게 되면 시스템은 사전 정의된 해쉬 알고리즘을 통하여 XML 문서에 대한 메시지 축약값을 추출한다. 추출된 메시지 축약값에 공유키를 적용하여 데이터를 암호화 한다. 이때 암호화는 분류된 메타데이터를 기반으로 암호화 과정을 수행하며 사용자는 인증 과정을 거친 후 역할을 할당받아 문서를 요청하게 된다.

데이터 암호화가 되면 사용자의 인증을 위하여 접근이 혀용된 문서만 할당할 수 있도록 사전에 공유된 난수와 킷값을 가지고 개인키를 생성하고 이를 기반으로 XML 인증문서를 생성한다.

사용자가 XML 데이터를 요청하게 되면 서버는 사용자에게 XML 인증문서와 데이터파일을 전송하게 되는데 사용자는 개인키를 가지고 인증을 수행하고 이를 통해 사용자의 역할에 해당하는 부분에 대한 데이터를 확인하게 된다.

3. 증강객체 네트워크 랜더링 기반 증강현실 시스템

XML 보안기법, 워터마킹 기법을 적용한 입체 증강현실 시스템의 구성도는 다음 Fig. 1과 같다.

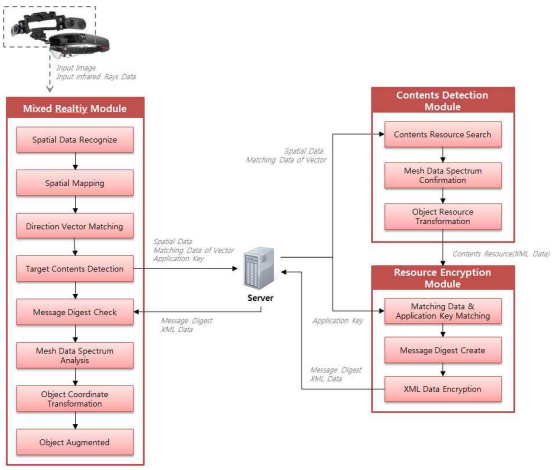

Fig. 1. System Structure

3.1 객체 검출

홀로그램 HMD의 경우 공간과 검출 대상을 추출하기 위하여 적외선 센서와 깊이 인식 카메라를 통해 공간 데이터를 인식한다.

본 논문에서는 실제 공간 및 벡터 정보를 검출하기 위하여 Hololens의 Kninect 기반 인식 기술[5]을 이용한다.

그러나 Kineinect의 인식 기술은 홀로그램의 가상 공간 정보에 기초한 콘텐츠 자원을 이용하고 있기 때문에 객체를 증강함에 있어 가상공간의 오브젝트 정보(Rotation, Scale, Point)가 상이하기 정합되어야 한다. 따라서 증강현실 콘텐츠를 제작하는 과정에서 생성된 가상공간과 증강현실에서 콘텐츠를 제공하는 가상공간이 부정합하다는 문제가 있다. 따라서 Fig. 5와 같이 추출된 벡터영역의 에지 정보를 기반으로 직선의 강도가 높은 영역에 진보된 허프 변환 알고리즘(Probabilistic Hough Transform,PPHT) [6]을 사용하여 Fig 2와 같이 임의의 모서리점 한 개를 지정하고 이에 대한 직선의 강도가 높은 에지를 지나는 모서리점을 선택하여 이에 대한 벡터정보를 계산한다. 위 과정을 반복하여 직선의 강도가 강한 에지의 누적이 0이 될 때 까지 반복하여 정합될 현실 객체의 위치를 재추출한다.

재추출 된 영역에 기초하여 가상 정보를 합성하는 영역인지 인식 할 영역을 추가적으로 선택하고 선택된 벡터정보를 서버로 전송하여 벡터 정보에 따른 내용정보를 할당받는다[7,8].

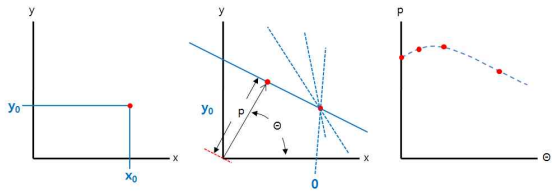

Fig. 2. Progressive Probabilistic Hough Transform Method in Vector

3.2 콘텐츠 검색

객체를 검출하여 도출된 벡터 정보를 기반으로 기준 벡터 정보를 확인하기 위해서는 특징에 대한 정보를 저장하고 있는 기준 파일이 필요하다. 따라서 본 논문에서는 다음 Fig. 3과 같은 기준 파일을 이용하여 패턴 분석을 한다.

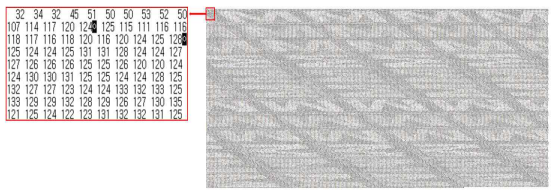

Fig. 3 Basic Pattern File

기준 패턴파일과 비교 분석을 수행하기 위하여 특징 벡터 정보를 다음 Fig. 4와 같은 형태로 변환하고 이를 기반으로 Fig. 3의 기준파일과 동일 패턴 텍스트를 갖는 상관성을 분석한다.

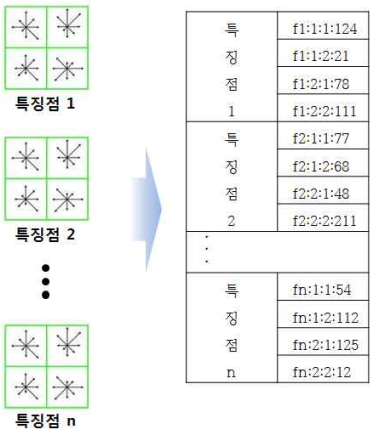

Fig. 4 Pattern Array Text

동일한 패턴 텍스를 가진 기준 패턴을 검색하고 이와 연계된 콘텐츠의 ASE 파일을 검색한다.

3.3 매쉬 데이터 변환

3차원 오브젝트를 제작하여 저장하는 콘텐츠를 XML 포맷 형태로 저장하게 되면 지정된 보안 기법에 따라 XML 태그가 정형화되기 때문에 본 논문에서는 서버에 저장된 3차원 오브젝트 파일을 태그 형태로 Geometry 정보만을 저장하고 있는 ASE 파일로 저장하고 있는다.

ASE 파일의 경우 단순 아스키코드로 Geometry 정보만 표현하기 때문에 콘텐츠의 변조, 불법복제가 용이하다 따라서 본 논문에서는 오브젝트 리소스 파일자체에 워터마킹을 수행하여 데이터 변조 및 복제를 차단하도록 한다.

기존의 디지털 콘텐츠의 경우 공간 도메인 워터 마킹 기법과 주파수 정보를 이용한 워터마키 기법으로 분류되어 사용되었다[9].

기존의 디지털 워터마킹 기법의 경우 2차원 영상 또는 이미지에 대한 스펙트럼 정보를 가지고 워터마킹작업을 수행하기 때문에 실시간으로 영상을 랜더링 하는 3차원 오브젝트의 매쉬 데이터에 대한 스펙트럼 추출이 어렵다는 문제가 있다.

따라서 본 논문에서는 디지털 워터 마킹기법 중 공간 도메인을 통해 데이터 변조를 막는 3D 메시 워터마킹(3D Mesh Water Marking)기법[10]을 적용하여 서버에서 전송되는 증강 객체의 변조를 막는다.

3D 메시 워터마킹(3D Mesh Water Marking)기법의 경우 메쉬(Mesh) 정보에 대한 폴리곤의 벡터 정보를 기반으로 도메인을 생성하고 이를 기반으로 워터마킹을 수행하는 과정을 거친다.

그러나 본 논문에서는 내부 저장소에 있는 리소스 파일의 메쉬 데이터를 이용하여 랜더링하는 것이 아니라 태그 형태의 지오메트리(Geometry) 정보를 기반으로 랜더링을 수행하기 때문에 지오메트리 정보중 점(Vertex)에 대한 폴리곤을 도출하고 도출된 폴리곤의 정점을 연결하는 정점 좌표를 계산한다.

계산된 정점 좌표를 직교기저하는 각 좌표의 벡터들을 투영하여 스펙트럼을 계산한다.

이때 네트워크를 통해 전송된 태그 정보와 함께 외부 맵핑 데이터에 대한 스펙트럼 정보가 포함되어 있기 때문에 지오메트리정보를 통해 추출된 스펙트럼 정보와 비교하여 정점좌표를 다음 식을 통해 추출한다.

$$(x_1, x_2, \cdots x_n)^T = r_s,_1 e_1 + r_s,_2 e_2 + \cdots + r_s,_n e \qquad (1)$$
$$(y_1, y_2, \cdots y_n)^T = r_s,_1 e_1 + r_s,_2 e_2 + \cdots + r_s,_n e_n$$
$$(z_1, z_2, \cdots z_n)^T = r_s,_1 e_1 + r_s,_2 e_2 + \cdots + r_s,_n e_n$$

식 1에서 r_s은 스펙트럼 계수 벡터이며, ${}_n e_n, \cdots, {}_n e_n$은 n개의 정규화된 고유 벡터이다.

정점 좌표가 도출되면 다음 Fig. 5와 같이 스펙트럼에 워터마킹을 삽입하기 위한 벡터를 계산해야한다.

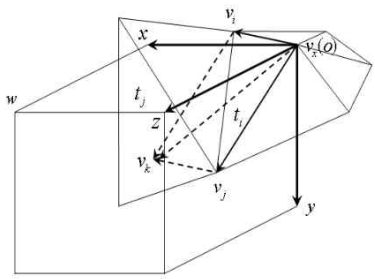

Fig. 5. Object Resource Vector using Watermarking

정점 좌표에 근교한 3개의 폴리곤 t_i, t_j, t_k의 방향에 대한 벡터 v_i, v_j, v_k를 도출한다. 도출된 3개의 벡터를 통해 원점 0에 해당하는 꼭지점 v_x에 일치 시킨다.

이때 일치된 벡터는 x,y축에 대한 각도만 계산되어 있기 때문에 다음 식 2를 통해 z축의 각도를 계산하여 일치시킨다.

$$\theta = \cos^{-1}\frac{\overrightarrow{oz} \cdot \overrightarrow{v_x v_k}}{\| \overrightarrow{oz} \| \ \| v_x v_k \|} \qquad (2)$$

식 2를 통해 도출된 x, y, z축에 대한 각도가 계산되면 이를 기반으로 정점 좌표에 근교한 폴리곤 t_i, t_j, t_k에 벡터 방향에 따라 RGB 색상의 변조를 준다. 이때 변조된 색상 값은 흰색.(000),빨강(001), 파랑(010), 노랑(011), 녹색(100), 검정(101)이다.

3.4 콘텐츠 리소스 변형

ASE 파일의 경우 스펙트럼 및 오브젝트의 지오메트리 정보를 포함하고 있으나 암호화된 키 값에 대한 권한 설정이 불가능하기 때문에 태그 정보에 대한 권한 설정을 적용하기 위하여 ASE 파일의 지오메트리 정보에 워터마킹 기법을 통해 적용된 스펙트럼 변조 정보를 포함하여 리소스파일을 생성한다.

생성된 파일은 XML 표준 문서 기법에 따라 새로운 형태로 태그 정렬하여 변경된다.

워터 마킹 기법이 적용된 ASE 파일의 지오메트리 정보에서 변환된 정보를 가지고 있는 GEOMOBJECT 태그, MESH 태그에 대한 정보를 그룹화하여 지오매트릭스 태그의 하위태그로 구성한다.

이때 매쉬 태그에는 기존의 ASE 파일의 매쉬 태그 정보에 매쉬 데이터 스팩트럼을 확인한 검출데이터를 추가하여 워터마크데이터를 삽입하여 Table. 1과같은 형식의 XML 파일 태그를 생성한다.

그러나 기존의 XML 파일 태그의 경우 기존의 XML 암호화기법[11]에 따라 워터마킹이 삽입된 형태로 파일을 생성할 경우 실시간 태그 전달로 인하여 랜더링 과정 중에 버퍼 메모리에 저장되는 태그 데이터가 딜레이 되는 현상이 발생하기 때문에 상위 태그에서 데이터의 권한을 먼저 확인하고 랜더링을 수행하기 위한 오브젝트 정보를 실시간으로 접근하도록 접근 권한의 과정을 축소시켜야한다.

따라서 사전에 정의된 해쉬 함수 알고리즘(SHA-1)[12]에 적용하여 난수 값을 생성하고 이를 기반으로 메시지 축약 값을 산출한다.

Table 1. XML tag of contents resource

```
*GEOMETRIX {
    GEOMOBJECT {
            *NODE_NAME ""Teapot01""
            *NODE_TM {
                    *NODE_NAME ""Teapot01""
                    *INHERIT_POS 0 0 0
                    *INHERIT_ROT 0 0 0
                    *INHERIT_SCL 0 0 0
                    *TM_ROW0 -0.0000 0.1933 0.0000
                    *TM_ROW1 -0.1933 -0.0000 -0.0000
                    *TM_ROW2 0.0000 -0.0000 0.1933
                    *TM_ROW3 -0.0000 0.2256 0.0000
                    *TM_POS 0.0000 0.2256 0.0000
                    *TM_ROTAXIS 0.0000 0.0000 1.0000
                    *TM_ROTANGLE 1.5708
                    *TM_SCALE 1.0000 1.0000 1.0000
                    *TM_SCALEAXIS 0.0000 0.0000 1.0000
            *TM_SCALEAXISANG 1.5708
            }
    MESH {
            *TIMEVALUE 0
            *MESH_NUMVERTEX 530
            *MESH_NUMFACES 992
            *MESH_VERTEX_LIST {
            *MESH_VERTEX 0  -0.0000   1.1593  1.6007
            *MESH_VERTEX 1  -0.0000  1.1463  1.6499
            *MESH_VERTEX 2  -0.0000   1.1614  1.6664
            *MESH_VERTEX 3  -0.0000   1.1922  1.6499
                                ⋮
}
```

메시지 축약 값이 산출되면 사전에 공유된 공유키(어플리케이션 키)와 패턴 ID를 기반으로 데이터를 암호화한다.

이때 암호호된 파일의 접근을 확인하기 위하여 암호화된 데이터는 XML 전자서명 값(Signature Value)을 가지는 파일과 문서 원본(Document D)으로 분류되어 암호화되어 홀르그램용 HMD로 전송되어진다.

3.5 콘텐츠 리소스 확인 및 객체증강

서버로부터 암호화된 콘텐츠 리소스 파일(XML 서명 문서, 메시지 축약값)을 전송 받으면 XML 서명 문서 파싱(Parsing)하여 이를 해독 및 검증해야 한다.

본 논문에서는 암호화된 리소스 파일이 전송되어지면 검출된 패턴 ID와 어플리케이션 키 값을 사전에 정의된 해쉬 알고리즘(Hash Algorithm)에 적용하여 메시지 축약값을 산출한다.

메시지 축약값이 산출되면 이를 기반으로 사전에 공유된 공개키를 이용하여 사용자 인증을 수행한다.

사용자 인증이 수행되면 변형된 메시지 축약값 을 서버로 전송하여 복화화된 메시지 축약 값과 동일한지 확인한다.

서버에서 전송된 메시지 축약값의 동일성을 판단하

여 동일시되었을 경우 원본문서 접근 권한을 제공한다. 만약 메시지 축약값이 동일시 되지 않을 경우 미인증 파일 전송을 확인하여 콘텐츠 리소스를 재전송한다.

증강현실에서는 실시간으로 패턴을 검출하고 객체를 증강해야 하기 때문에 ms 단위로 복호화가 이루어져야 한다.

따라서 사용자 인증이 완료된 클라이언트의 경우 메시지 축약 값을 저장하고 패턴이 검출될 때마다 패턴 ID와 함께 이를 전송한다. 서버에서는 메시지 축약 값과 패턴 ID가 동시에 전송되면 메시지 축약값에 대한 암호화만 수행하여 랜더링에 필요한 태그인 GEOMOBJECT, SCENE 태그이외에 불필요한 태그는 제거하여 암호화한다.

인증이 완료된 후 전송된 XML 리소스 파일의 경우 메시지 축약값에 SAVE(Static Analyzer of Vicious Executables)[13] 기법을 적용하여 GEOMOBJECT, SCENE에 대한 데이터만 복호화[12][13] 없이 호출한다.

XML 파싱이 완료되면 제공된 콘텐츠 리소스가 변조되었는지 확인하기 위하여 MESH 정보를 기반으로 스펙트럼 분석을 수행한다. 이대 변조를 알아보는 식은 다음과 같다.

$$q_j = \frac{1}{3}\sum_{l\in(s,t,u)}\sum_{i=j\cdot c}^{(j+1)\cdot c-1}\left(\widehat{r_{l,i}} - r_{l,i}\right) \cdot p = \frac{1}{3}\sum_{l\in(s,t,u)}\sum_{i=j\cdot c}^{(j+1)\cdot c-1} b'_i \cdot a \cdot p'_i \tag{3}$$

식 3을 통하여 워터마킹을 확인하여 워터마킹이 존재하는 매쉬가 있다면 이를 랜더러로 전송한다. 그러나 워터마킹이 존재하지 않으면 전송된 파일을 제거하고 서버로 리소스 파일을 재요청하게 된다.

랜더러로 전송된 증강객체는 검출된 현실 대상의 객체의 3차원 좌표에 맞춰 매칭되어야 한다[14-16].

되며 그식은 다음과 같다.

$$s'\begin{bmatrix} x \\ y \\ 1 \end{bmatrix} = K[R|t]\begin{bmatrix} X \\ Y \\ Z \\ 1 \end{bmatrix} = K[r_1, r_2, r_3, t]\begin{bmatrix} X \\ Y \\ 0 \\ 1 \end{bmatrix} = K[r_1, r_2, r_3]\begin{bmatrix} X \\ Y \\ 1 \end{bmatrix} \tag{4}$$

변환된 투영행렬 식 4를 증강객체의 위치를 고정시키기 위한 주점으로 다음 식 5를 통해 변환하으 객체를 증강한다.

$$K = \begin{bmatrix} f & s & c_x \\ 0 & af & c_y \\ 0 & 0 & 1 \end{bmatrix} \tag{5}$$

4. 결론

HMD 기술의 발달과 홀로그램 기술의 발달로 인해 실제 공간과 가상 정보가 다양한 장치를 통해 합성되는 컨버전스 현실이 사회적 이슈로 대두되고 있다. 컨버전스 현실을 제공하는 기술 중에서 홀로그램 렌즈를 사용하는 증강 현실 시스템은 가상 공간 객체 및 정보를 구성하기 위해 객체에 리소스를 추가해야하므로 리소스를 추가 할 때마다 어플리케이션을 업데이트해야한다. 홀로그램 HMD의 경우 소형의 프로세스에서 데이터를 처래해야하기 때문에 하드웨어의 용량 제한으로 인해 콘텐츠의 용량을 경령화해야 한다. 이러한 문제점을 해결하기 위해 서버에서 디바이스로 콘텐츠의 리소스를 전송하거나 디바이스에서 렌더링을 수행하기 위해 객체에 대한 정보 만 전송하는 방법을 도입한다.

그러나 기존의 증강현실 시스템에서는 내부 저장소에서 데이터를 저장하고 있기 때문에 네트워크 랜더링 과정간 제공되는 오브젝트의 태그 정보에 대한 변조 및 악의적 코드가 삽입되는 문제등을 고려하고 있지 않아 보안적 위협 요소가 존재한다.

이 문제를 해결하기 위해 본 논문에서는 물리적 기반 모델링을 이용하여 서버에서 전송 된 자원 또는 객체 정보를 외부 정보로 변환하여 객체를 실시간으로 인식한다. 또한 인식된 좌표 정보를 기반으로 증강되는 3차원 객체에 대한 폴리곤 메쉬 데이터의 스펙트럼에 기반한 워터 마킹 기술을 적용한 콘텐츠를 XML 보안 기법에 의해 암호화 하여 권한이 없는 클라이언트는 랜더링을 수행하지 못하게 하며 전송되는 콘텐츠의 변조여부를 확인하게 된다. 이를 통해 보안에 취약한 증강현실 콘텐츠를 선별하여 제공함으로써 보안 위협 요소를 제거하였다. 그러나 홀로그램을 이용한 증강 현실에서는 현실 공간 좌표의 좌표와 가상 공간의 좌표를 일치시키는 과정이 네트워크상에서 동시에 수행되므로 서버에서 데이터를 전송하기위한 처리 시간이 길어진다. 따라서 네트

워크 렌더링 기술에 대하여 추가적으로 연구할 것이다.

REFERENCES

[1] K. J. Lee & W. S. Jeong. (2011). An Analysis of the Economic Effects for the Immersive Media Industry. *The Journal of Korean Institute of Communications and Information Sciences*, 36(7), 795-805.

[2] S. Jonathan. (1992). Defining virtual reality: Dimensions determining telepresence. *Journal of communication 42(4),* 73-93.

[3] E. Damiani, S. Vimercati, S. Paraboschi & P. Samarati. (2000). Securing XML Documents. *Proceedings of the 2000 International Conference on Extending Database Technology(EDBT2000).*

[4] Q. Wen, Y. Wang & P. Li. (2018). Two Zero-Watermark methods for XML documents. *Journal of Real-Time Image Processing, 14(1),* 183-192.

[5] J. L. Raheja, A. Chaudhary, K. Singal. (2011). Tracking of fingertips and centers of palm using kinect. *In Computational intelligence, modelling and simulation (CIMSiM),* 248-252.

[6] S. A. Kumar. (2017). Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images. *Multimedia Tools and Applications 76(6),* 8881-8900.

[7] S. H. Kim. (2016). Realtime 3D Human Full-Body Convergence Motion Capture using a Kinect Sensor. *Journal of Digital Convergence, 14(1),* 189-194.

[8] K. W. Park & J. Y. Lee. (2015). A Morphology Technique-Based Boundary Detection in a Two-Dimensional QR Code. *Journal of Digital Convergence, 13(12),* 159-175.

[9] S. M. Jung., J. G. Song, D. J. Hwang, J. Y. Aan & S. S. Kim. (2010). A Study on Software-based Sensing Technology for Multiple Object Control in AR Video. *Sensors, 10(11),* 9857-9871.

[10] J. U. Hou, D. G. Kim & H. K. Lee. (2017). Blind 3D Mesh Watermarking for 3D Printed Model by Analyzing Layering Artifact. *IEEE Transactions on Information Forensics and Security, 12(11),* 2712-2725.

[11] A. F. Tawfiq & J. Lu. (2017). Securing Financial XML Transactions Using Intelligent Fuzzy Classification Techniques: A Smart Fuzzy-Based Model for Financial XML Transactions Security Using XML Encryption. *Ontologies and Big Data Considerations for Effective Intelligence. IGI Global, 201,* 214-326.

[12] K. Fatma. (2017). High Performance and Reliable Fault Detection Scheme for the Secure Hash Algorithm. *Indian Journal of Science and Technology 10(19).*

[13] S. R. Kokate & S. G. Salunke. (2017). Implementation of Intelligent Malware Detection System Using Post Processing Techniques. 2017 International Conference on Computing, Communication. *Control and Automation (ICCUBEA),* 1-4

[14] S. W. Jeong, U. R. Chio & I. G. Lee. (2018). Cyber KillChain Based Security Policy Utilizing Hash for Internet of Things. *Journal of Digital Convergence, 16(9),* 179-185.

[15] H. U. Kim, H. J. Kim, J. H. Kang & M. S. Jun. (2017). A Study on Analysis and Countermeasure of Security threat in NFC. *Journal of Digital Convergence, 14(12),* 183-191.

[16] K. H. Ko. (2018). An Estimating Algorithm of Vehicle Collision Speed Through Images of Blackbox. *Journal of Digital Convergence, 16(9),* 173-178.

김 석 수 (Seoksoo Kim) [정회원]

- 1989년 2월 : 경남대학교 컴퓨터공학(공학사)
- 1991년 2월 : 성균관대학교 정보전산학과(공학석사)
- 2002년 2월 : 성균관대학교 컴퓨터공학(공학박사)
- 현재 : 한남대학교 멀티미디어학과 교수
- 관심분야 : 멀티미디어 통신, 멀티미디어 저작, 컴퓨터 네트워크, 정보보호
- E-Mail : sskim@hnu.kr

김 동 현 (Donghyun Kim) [정회원]

- 2012년 2월 : 한남대학교 멀티미디어공학(공학사)
- 2014년 2월 : 한남대학교 멀티미디어(공학석사)
- 현재 : 한남대학교 멀티미디어 박사과정
- 관심분야 : 영상처리, 증강현실, 정보보호
- E-Mail : donghyunk1986@gmail.com