

논문 2024-4-31 <http://dx.doi.org/10.29056/jsav.2024.12.31>

에너지 변화 기반의 전자화문서 위변조 검출

최용수*†

Forgery Detection Based on Energy Changes of Electronized Document

YongSoo Choi*†

요 약

디지털 콘텐츠(이미지, 오디오, 비디오 등)에 대한 위변조 검출 기술은 오랜시간 동안 연구가 되어져 왔으나 디지털 문서에 대한 위변조 검출기술에 대한 연구는 많지 않았다. 문서에 대한 위조는 문서를 거짓된 정보로 생성하는 것이며 변조는 정상적으로 만들어진 문서에 대해 지우기, 복사-붙여넣기, 추가하기 등의 과정을 통해 의도적인 정보의 오류를 생성해내는 것이다. 본 논문에서는 실제 전자화된 문서의 위변조 검출을 다루고자 한다. 디지털 문서의 위변조는 사회적으로 다양한 분야에서 발생한다. 특히, 디지털 문서는 워드 프로세서에 의해 생성된 전자문서와 스캐너 등에 의해 생성되는 전자화 문서로 나눌 수 있어 분리된 기술적 접근이 필요하다. 본 논문을 통해 전자화문서에서 실제 위변조에 의한 특징을 찾아낼 수 있는지 그리고 유의미한 위변조 특징으로서의 가치를 가지는지 확인하고자 한다. 디지털문서의 단순 위변조 현상을 측정할 결과 약 39% 픽셀에 에너지 변화가 발생하며 픽셀 평균 2.29정도의 픽셀 값 변화가 발생하는 것을 측정하였다.

Abstract

Forgery detection technology for digital contents (images, audio, video, etc.) has been studied for a long time, but there has been little research on forgery detection technology for digital documents. Fabrication of documents is the creation of false information in documents, and Falsification is the creation of intentional information errors through processes such as erasing, copying, and adding to normally created documents. This paper deals with the detection of falsification rather than fabrication. Forgery of digital documents occurs in various social fields. In particular, digital documents can be divided into electronic documents created by word processors and electronized(scanned) documents created by scanners or word processor, etc., and therefore require separate technical approaches. Through this paper, we aim to verify whether it is possible to find characteristics due to actual forgery in electronic documents and whether they have value as meaningful forgery characteristics. Through metrics, we measured that energy changes occur in approximately 39% of pixels and an average pixel value change of approximately 2.29 occurs in pixels simply by copying objects in digital documents.

한글키워드 : 위변조 검출, 문서보안, 종이지문, 신호특징, 전자화문서

keywords : Forgery Detection, Document Security, Paper Fingerprint, Characteristic, Electronized Document

* 신한대학교 미래자동차공학과

† 교신저자: 최용수(email:ciechoi@shinhan.ac.kr)

접수일자: 2024.12.08. 심사완료: 2024.12.15.

게재확정: 2024.12.20.

1. 서론

디지털 문서는 전자문서와 전자화문서로 크게

두가지로 구분할 수 있다. 전자문서는 워드프로세서와 같은 편집기를 통해 작성된 문서들을 말하며, 전자화문서는 종이문서들을 스캔해 pdf형식 또는 jpg형식 등의 그림파일형태로 저장하는 것이다. 전자문서와 전자화문서는 일반적인 저장 및 보관을 위해 생성되기도 하지만 각종 증빙들을 발급할 때 많이 이용되기도 한다. 하지만 문서편집 및 영상편집 도구들의 진화로 이와같은 전자/전자화문서의 편집이 훨씬 쉬워졌으며 이를 이용한 악용된 사례도 늘고 있는 추세다. 위변조는 상호간의 신뢰저하, 경제적 비용발생에 의한 사회적 자본의 손실, 장기적으로는 국가 이미지에도 타격을 입게될 수 있다[1-6]. 다양한 산업에서 중국의 'Made in China'를 저품질 '짜퉁'으로 취급하는 인식이 생긴 것을 봐도 그 파급성을 알 수 있다.

위변조를 방지하기 위한 기술은 크게 세가지 정도로 구분할 수 있다.

눈으로 직접 식별할 수 있는 Overt기술, 생산자 또는 유통자가 위조제품을 구분할 수 있도록 만든 Covert기술 그리고 고도의 기술이나 과학적 접근법으로 위변조를 구분할 수 있도록 만든 Forensic기술이다. 특히, 디지털 워터마킹은 Covert기술의 대표적 기술이며 다양한 문서의 위변조 탐지에 활용되고 있으나 정상적인 유통채널을 가진 분야에서 주로 활용되며 인코딩과 디코딩을 위한 하드웨어 또는 소프트웨어적인 환경이 필수적이다. 다양한 기관에서 발급한 문서들을 증빙으로 보관하고 이에 대한 위변조가 일어나는 것은 위와 같은 기술들로 탐지하는 것이 어려워 Forensic기술이 활용되어야 한다.

2005년 종이에도 고유한 무늬가 존재하며 진위의 식별방식으로 이용하자는 제안이 이루어졌다[7]. 이 논문에서는 종이에 존재하는 지문을 특징으로 정의하고 이러한 특징이 어떻게 변화하는지를 추적하여 디지털 문서의 위변조 검출을 위

한 Forensic기술의 기초적인 실험을 제시하고자 한다.

표 1. 위변조 방지 기술 특징
Table 1. Forgery Protection Technique Features

O v e r t	소비자가 눈으로 식별할 수 있는 기술	Hologram	가장 많이 알려진 기술, 3D 기술을 이용한 이미지 표시
		OVD	이미지가 변하거나 비추어 보임
		Color Shifting Security Inca	각도에 따라 색상이 변함
C o v e r t	브랜드 오퍼들이 위조제품을 구분할 수 있게 만든 기술	Invisible Printing	특별한 잉크를 사용하여 눈에 보이지 않게 프린트
		Embedded Image	보이지 않는 이미지를 삽입
		Digital Watarmarking	보이지 않는 데이터가 그래픽 안에 인코딩
		Hidden Marks and printing	특별한 마크나 프린트를 보이지 않게 프린트
F o r e n s i c	고도의 기술이나 과학적 접근법으로 구분하게 한 기술	Chemical taggants	특화된 시약으로 진품을 구분
		Biological taggants	생물학적 마커를 이용하여 포장용기등에 사용
		DNA Taggants	특수한 운,시약으로 진품 여부를 판단
		Micro taggants	미세한 입자를 이용하여 문자와 숫자가 조합된 데이터를 생성하여 암호화된 정보를 삽입

2. 디지털 위변조 방지 기술

2.1 위변조 방지 기법

미디어 위변조 검증 기술은 미디어가 변조된 이후 즉, 편집 사후 시점에 위변조 여부를 탐지하는 방법이다. 그렇다면 위변조를 사전에 차단하기 위한 방법은 무엇이 있을까? 그림 1을 통해 설명하고자 한다. 위변조 검출 기술은 크게 능동형기술과 수동형 기술로 나누어지고 능동형 기술은 위변조 사전 차단기술로 볼 수 있으며 사전에 미디어의 생성자 또는 유통자가 고유의 신호를 원본 미디어에 포함시키거나 메타데이터에 포함시켜 위변조가 발생하였을 경우 이러한 정보의 검증을 통해 위변조를 탐지한다[8-10].

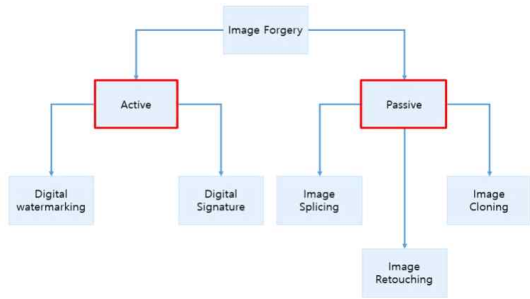


그림 1. 위변조 방지기술의 구분도
Fig. 1. Classification Diagram of Forgery Detection

디지털 영상에 대한 워터마크는 일정한 패턴을 가지는 잡음을 발생하고 해당 잡음을 원본 이미지의 픽셀값(LSB: Least Significant Bit)에 삽입한다. 삽입된 워터마크는 PSNR(Peak Signal to Noise Ratio)을 고려하여 삽입되므로 원본 콘텐츠의 시각적 지각력을 유지한 채 표현된다. 원본여부를 확인하고자 할 때 검증자는 LSB의 신호를 검출하여 원본 잡음과 비교해 봄으로써 원본 콘텐츠의 훼손여부를 확인할 수 있다.

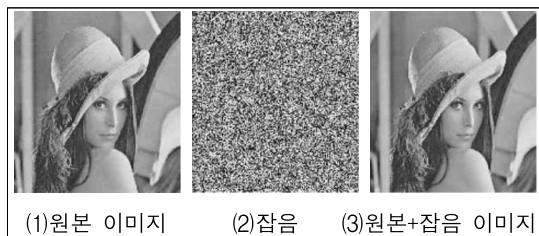


그림 2. 디지털 영상 워터마크
Fig. 2. Digital Image Watermark

워드프로세서에 워터마크 기능을 활성화하여 프린트 시 저작권자의 정보를 워터마크로 표시하는 방법이 있으며 공공기관 등에서는 그림 3과 같은 방법으로 워터마크를 삽입하여 시각적으로 원본 진위여부를 판별한다.

디지털 시그니처는 일반적으로 암호화방법으로 알려져 있어 원본 콘텐츠를 암호화하여 전혀

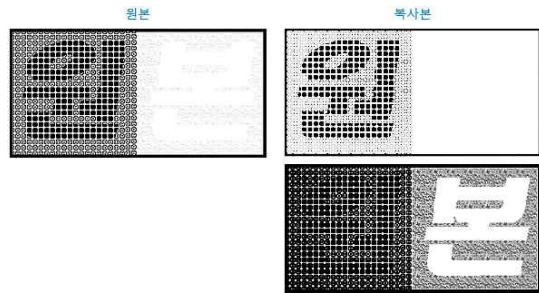


그림 3. 인터넷 증명서 위변조 검증방법
Fig. 3. Inherent Document Forgery Protection

다른 디지털 정보로 변환하여 전송하는 방식이다. 암호화는 복호화키를 가진 적법한 사용자만이 해당 콘텐츠를 복원해 보는 것이 가능하다. 인터넷상에서 발급하는 문서에서는 수신자의 생일 등 정보를 바탕으로 디지털서명된 콘텐츠를 생성해 해당 정보들을 열어볼 수 있도록 하는 간단한 보안기술로도 사용이 된다. 워터마크 기술과 디지털 서명의 가장 큰 차이는 원본의 형태를 유지하느냐의 관점이다.

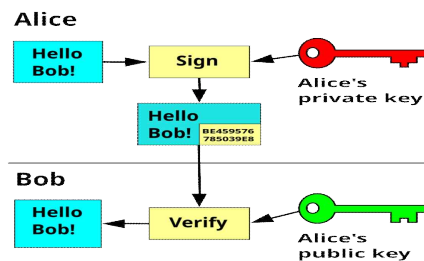


그림 4. 디지털 서명
Fig. 4. Digital Signature

수동적 위변조 방지기술로는 콘텐츠에서 일부 객체를 복사하여 다른 콘텐츠에 삽입하는 이미지 스플라이싱(Image Splicing), 콘텐츠내의 객체를 복제해 다른위치에 붙여넣기 하는 이미지 복제(Image Cloning), 콘텐츠내의 객체 등 시각적 정보를 편집기등으로 수정하는 이미지 리터칭

(Image Retouching)기술 등이 있으며 이러한 위변조를 검출해내는 기술을 디지털 신호 법과학(Digital Image Forensics)라 부른다.



그림 5. 배경, 인물의 합성이미지
Fig. 5. Spliced Image of Background and People

3. 디지털 문서의 위변조 환경 및 특징검출 방안

3.1 전자문서 생성과 객체의 복제

디지털 문서는 주로 생성과 동시에 화면에서 글씨와 그래픽을 표현하기 위한 디지털의 값(정보)을 가지게 된다. 하지만 우리가 화면에서 보는 것처럼 바탕은 흰색이고 글씨는 검은색으로 보이지만 저장된 정보들이 화면이나 종이에 출력될 때 출력장치들의 해상도 또는 시각적인 표현의 설정에 따라 임의의 값들이 생성되기도 한다.

그림 6은 주민등록표의 전자발급 문서와 발급 문서의 일부분을 확대하여 보여주는 예이다.

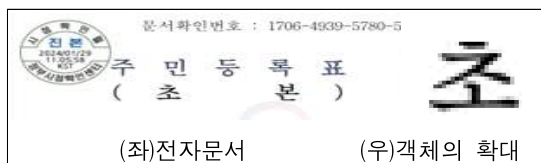


그림 6. 전자문서와 객체의 표현 예
Fig. 6. Electronic Document and Ex. of Object Representation

전자문서를 생성할 때 동일한 객체를 생성해

내는 것은 위조에 해당하게 될 것이며 위조된 문서의 원본(진본)으로서의 가치를 상실하게 되므로 본 논문의 논지에서는 제외하기로 한다. 이러한 전자문서에서 일부분의 내용을 복사붙여넣기 위변조를 하는 것을 가정하여 샘플영상을 만들어 위변조 탐지 가능성을 실험하였다. 물론 전자문서의 위변조를 위한 방법은 현재로서는 PDF편집기 또는 이미지편집기로 볼 수 있다. 실험의 과정은 그림 7과 같이 진행된다.

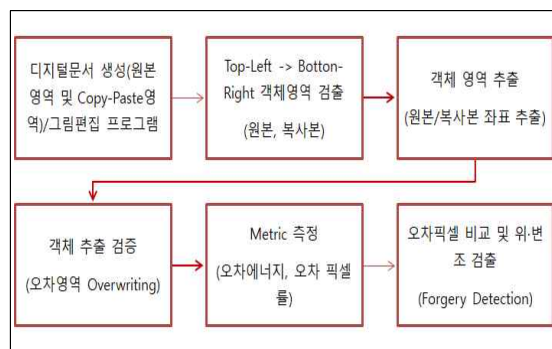


그림 7. 전자 문서 위변조 검출 프로세스
Fig. 7. Electronic Document Forgery Detection Process

3.2 전자문서 생성 및 객체 복제

그림 8의 왼쪽은 문서상의 원본 글자 그래픽이며 오른쪽은 그림판 프로그램을 활용하여 원본 글자를 복사하여 배경영역에 붙여넣기한 그래픽이다. 물론 프로그래밍 언어를 이용하여 이러한 복사 붙여넣기를 수행한다면 원본 그래픽의 값은 그대로 붙여넣기 되어지지만 논문에서는 응용프로그램을 활용하는 경우를 고려하였다.

일반적인 지각정보의 경우 그림 8의 객체는 동일하게 보일 수 있다.

3.3 문서내 객체영역 검출 및 좌표 추출

그림 8에서 좌우 그림의 객체가 같은 그림인지 확인하기 위하여 문서내에서 두 객체의 영역들을 검출하고 검출된 영역 외에 일부 영역을 확장하

여 원본영상(O)와 복사영상(F)라고 명명한다. 검출된 영역의 확장영역을 설정하는 이유는 그래픽에 의해 표현되는 문자는 디지털 잡음을 포함할 수 있어 이를 측정하기 위해서이다. 문서 내에서 배경으로 판단되는 픽셀을 제외한 픽셀들을 모두 확인하고 해당 위치들을 수집하여 문서 내 원본 영역과 복사영역의 좌표들을 확인한다.

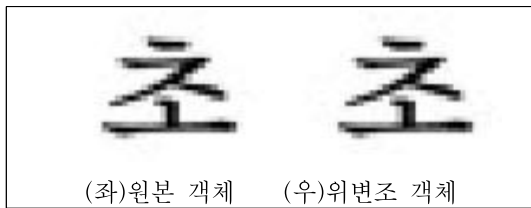


그림 8. 디지털 문서 내 객체 복제
Fig. 8. Electronic Document's Object Cloning

3.4 객체영역 좌표 추출 및 검증

문서내에서 원본 및 복제 객체로 검출된 영역들에서 추출한 좌표들이 명확하게 객체의 좌표를 대표하는지 확인하기 위해 추출된 좌표들을 문서 내의 객체영역에 덮어씌워 추출 좌표의 정확도를 시각적으로 검증(표시)하였다.



그림 9. 디지털 문서 내 객체 영역 검증
Fig. 9. Electronic Document's Object ROI

3.5 위변조 검출 Metric 측정

본 논문에서는 원본영상을 문서내에서 복사-붙여넣기 위변조를 한 경우 어느정도의 잡음(픽셀의 변화)을 일으키는지 확인하고자 하므로 변화한 픽셀의 개수(비율)과 잡음의 에너지양(총 에너지와 평균에너지)을 측정하고자 한다.

그림 9에서 O 영상(왼쪽)과 F영상(오른쪽)이 완벽히 일치하는 곳은 255의 값으로 표시되어 지고 나머지 일치하지 않는 곳은 픽셀의 차이 값이 매우 작아 위변조의 특징확인을 위해 일정비율로 증가하여 다음과 같이 차영상을 확인할 수 있었다. 차영상은 아래와 같이 구하였다.

$$Diff = (O - F) * 100 \quad (1)$$

식 1로 얻어진 차 영상에서 잡음(오류 발생) 발생한 픽셀의 수, 잡음 픽셀의 총에너지와 평균 에너지를 측정한 결과는 아래와 같다.

표 2. 디지털 문서 위변조 검출 메트릭
Table 2. Digital Document Forgery Detection Metric

척도	값
좌표 추출 정확도	100%
잡음 픽셀 수	156(39%)
잡음에너지량	426(평균 2.73)
잡음강도	8(max)

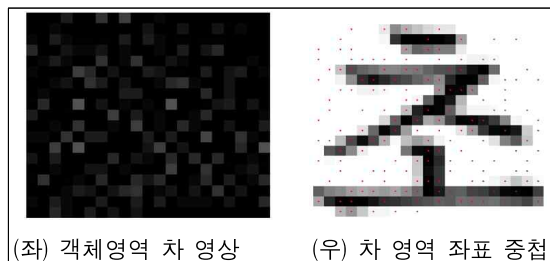


그림 10. 차영상 및 에너지 변화 영역 중첩
Fig. 10. Difference and Energy Change Overlay Image

3.6 오차 픽셀 검출 및 위변조 검출

실험에서 얻어진 차 영상은 그림 10과 같다. 메트릭에서 확인한 바와 같이 픽셀값의 변화가 표현된것을 볼 수 있다. 위변조 효과가 발생한 영역들을 확인하기 위해 원본 객체 영역에 덮어

썩은 결과를 그림 10(우)에서 확인할 수 있다. 픽셀들간의 에너지 변화량이 발생한 곳들에서 픽셀 값의 변화가 생기는 것은 추측할 수 있으나 그렇지 못한 곳들도 종종 보인다.

“본 논문은 2024년도 신한대학교 학술연구비 지원으로 연구되었음.” (“This work was supported by the Shihan University Research Fund, 2024”)

4. 결론 및 향후 연구 방향

본 논문에서는 디지털 문서(전자문서와 전자화문서)의 위변조 과정에서 발생하는 픽셀의 에너지 변화와 잡음 에너지의 생성을 측정해보고자 실험을 진행하였다. 실험에서는 디지털 문서의 객체 복사-붙여넣기 위변조를 위해 객체를 복제하고 객체추출 및 각 객체영역 정렬 그리고 정렬된 객체들 간의 에너지 변화를 측정하는 연구를 수행하였다. 서론에서 제시한 바와 같이 PC에서 주로 사용하는 그림판 프로그램을 사용하여 복사-붙여넣기 위변조를 했음에도 불구하고 객체영역과 그 외의 영역에서 잡음의 발생이 빈번하게 일어남을 알 수 있다. 검증을 실시한 영역에서 잡음이 발생한 픽셀의 비율은 39%였으며 픽셀 평균 에너지 변화량은 2.73이었으며 최대변화량은 8로 지각적으로도 그 변화를 알 수 있을 정도이다. 에너지 변화가 발생한 원인으로는 첫째, 복사-붙여넣기 이후 파일을 저장하는 과정에서 양자화와 압축의 과정을 거치며 에너지 변화가 생길 수 있다. 둘째, 프로그램의 알고리즘 특성으로 복사된 영역의 값들을 붙여넣기 하는 과정에서 특정한 값의 변화를 만들어 낼 수 있다. 결국 전자문서 또는 전자화 문서의 위변조 시 디지털 잡음을 발생한다는 것을 확인할 수 있으며 문서내에서 원래 존재하는 객체의 영역을 구분해 낼 수 있다면 복사-붙여넣기와 같은 악의적 위변조 공격을 검출해 낼 수 있다.

참고 문헌

- [1] Arpita Singh, S.K. Singh, Nilu Singh and Sandeep K. Nayak, “An Algorithm for Crime Detection in Digital Forensics”, *Journal of Survey in Fisheries Sciences*, 2023.
DOI: <https://doi.org/10.17762/sfs.v10i3S.136>
- [2] Ashlesh Sharma, Lakshminarayanan Subramanian, Eric A. Brewer, “PaperSpeckle: microscopic fingerprinting of paper”, *Proceedings of the 18th ACM conference on Computer and communications security*, 2011. DOI: <https://dl.acm.org/doi/10.1145/2046707.2046721>
- [3] Anil Dada Warbhe and R.V. Dharaskar, “V.M. Thakare, ”A Scaling Robust Copy-Paste Tampering Detection for Digital Image Forensics”, *Computer Science*, vol. 79, pp. 458-465, 2016 DOI: <https://doi.org/10.1016/j.procs.2016.03.059>
- [4] Choi, YongSoo, Atnafu, Ayalneh Dessalegn & Lee, DalHo “Hybrid Detection Algorithm of Copy-Paste Image Forgery”, *Journal of Digital Contents Society*, 2015. DOI: <https://doi.org/10.9728/dcs.2015.16.3.389>
- [5] Dessalegn Atnafu Ayalneh, YongSoo Choi & Hyoung Joong Kim “Early width estimation of fragmented JPEG with corrupted header”, *Multimed Tools Applications*, 2016. DOI: <https://doi.org/10.1007/s11042-015-2900-2>

- [6] Humaira Arshad, Aman Bin Jantan and Oludare Isaac Abiodun, "Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence", Journal of Information Processing Systems, 2018. DOI: 10.3745/JIPS.03.0095
- [7] James D R Buchanan, Russell Cowburn etc., "Forgery: 'Fingerprinting' documents and packaging", Nature, 2005. DOI: <https://doi.org/10.1038/436475a>
- [8] Priyadharsini Selvaraj, Muneeswaran Karuppiah, Enhanced copy -paste forgery detection in digital images using scale-invariant feature transform, IET Image Processing Volume 14, Issue 3 p. 462-471, 2020, DOI: <https://doi.org/10.1049/iet-ipr.2019.0842>
- [9] Reza Montasari, Richard Hill, Simon Parkinson, Pekka Peltola, Amin Hosseinian-Far, Alireza Daneshkhah, "Digital Forensics: Challenges and Opportunities for Future Studies", International Journal of Organizational and Collective Intelligence, 2018. DOI: :10.4018/IJOICI.2020040103
- [10] Raahat Devender Singh, Naveen Aggarwal, "Detection and localization of copy-paste forgeries in digital videos", Forensic Science International, Vol 281, pp. 75-91, 2017, DOI: <https://doi.org/10.1016/j.forsciint.2017.10.028>

저 자 소 개



최용수(YongSoo Choi)

1998년 강원대학교 제어계측공학과 공학사
2000년 강원대학교 제어계측공학과 공학석사
2006년 강원대학교 제어계측공학과 공학박사
2006년~2007년 연세대학교 첨단융합건설연
구단 연구교수.
2007년~2013년 고려대학교 정보보호대학원
연구교수.
2013년~2020년 성결대학교 파이데이터대학
(멀티미디어) 조교수
2020년~현재 신한대학교 미래자동차공학과
부교수

<주관심분야> Digital Forensics, Information
Hiding, Multimedia Watermarking,
Steganography