

# Digital Image Analysis and Forensics<sup>1</sup>

By Neal Krawetz(hackerfactor.com )

번역 : Kancho(kancholove@gmail.com)

디지털 카메라와 비디오 소프트웨어는 높은 품질의 사진과 동영상을 더욱 쉽게 제작하는데 도움을 준다. MySpace, Google Video, Flickr 같은 서비스들은 사진을 쉽게 배포하도록 해주며, 많은 사진들은 언론 매체에 사용되기도 한다. 그러나 여기에 문제점이 있다: 동영상이나 사진이 진짜라고 어떻게 말할 수 있는가? 컴퓨터로 만들어졌거나 수정되지 않았는가? 사진이 문자보다 더 영향력이 있는 세계에서 체계적인 방법으로 진위여부를 구별하는 것은 필수적이다. 이 문서는 디지털 이미지로부터 정보를 가져오는 몇 가지 일반적인 포렌식 방법과 많이 알려지지 않은 방법을 다룰 것이다. 그리고 이 문서는 실제 이미지와 컴퓨터로 만들어진 이미지를 구별하는 방법과 어떻게 이미지가 디지털적으로 수정되었는지 확인하는 방법을 설명할 것이다.

## 1. 용어

이 문서에서 사용되는 용어들은 다음과 같다.

- Computer generated (CG): 전체가 컴퓨터 소프트웨어로 만들어진 이미지. 예를 들어 영화 '토이 스토리'의 모든 장면은 CG이다.
- Digital Photo: 디지털 카메라로 찍은 사진 또는 수정되지 않은 스캔된 이미지
- Digitally Enhanced Photo: 수정된 디지털 사진. 이는 cropping이나 적목 현상을 완화시키는 것과 같은 수정과 색을 다시 칠하거나(re-coloring) 디지털적으로 다른 두 개의 이미지를 합치는 수정을 포함한다.
- Photoshopping: Adobe사의 Photoshop은 이미지의 질을 디지털적으로 향상시킬 수 있는 많이 사용되는 도구이다. Photoshop이나 유사한 다른 도구들(예를 들어 Gimp, Corel Draw, MS Paint)을 사용해서 이미지를 수정하는 것을 "Photoshopped" 또는 "shopped"(우리는 *뽀샵*이라고 흔히 표현합니다)라고 한다. Shopped된 이미지의 질은 도구와 사용자에 달려 있다. 많은 shopped된 이미지는 그 수정 여부를 쉽게 알 수 있지만, 매우 알아보기 어려운 것도 있다.
- Principal Component Analysis (PCA): 데이터 클러스터링에 기초한 분석적 접근
- Wavelet Transformations: signal decomposition에 기초한 분석법

---

<sup>1</sup> 이 문서는 Black Hat 2007 Briefings USA에서 발표된 문서로 디지털 이미지 분석에 대한 글입니다. 번역이 애매한 부분은 원문의 단어를 그대로 사용하거나 괄호 안에 참고할 수 있도록 하겠습니다. 그래픽 관련 전문 용어에 익숙하지 못한 관계로 번역이 매끄럽지 않음을 이해해 주시기 바랍니다. 역자의 주는 본문 내 *기울임* 꼴이나 각주로 나타내겠습니다.

## 2. 이미지와 관련된 문제점

이미지는 힘을 가지고 있다. 우주선이 발사 도중 폭발하는, 달 위를 사람이 걷는, 제 2차 세계 대전 중에 Iwo Jima의 깃발을 들고 있는 군인들<sup>2</sup>과 같은 강력한 힘을 가진 이미지들은 사회에 영향을 미친다. 정교한 디지털 이미지 소프트웨어와 실사 그래픽의 등장은 이미지에 더 많은 힘과 다른 의미를 전달할 수 있도록 만들었다. 하지만 불행하게도 많은 조작된 이미지들이 “실제”로서 존재한다.

디지털 시대 이전에는 영향력이 큰 이미지들은 때때로 negative splicing이나 airbrushing같은 기법을 통해 조작되었다. 디지털 이미지 소프트웨어의 등장으로 다시 실제로 재촬영 할 필요가 없어졌다. 이미지들은 합쳐지고, 그래픽적으로 quality가 높아질 수 있으며 또는 완전히 새로 만들어 질 수 있다. 이런 이미지들의 조작여부, 수정여부를 알아내기는 어렵다. 많은 조작된 이미지들이 논쟁을 통해 밝혀졌다. 예를 들어 Newsweek지는 2005년 3월호 표지 인물(그림1)로 Martha Stewart를 선정했다. 이는 사실 다른 사람의 몸에 Martha의 얼굴을 합성한 것이다. 이 사건은 Newsweek지의 잘못된 사진에 대한 혹평을 가져왔다.



그림1) 2005년 3월 Newsweek지의 표지는 모델의 몸에 Martha의 얼굴을 합성했다.

이미지 수정은 저작권 문제를 가져올 수 있다. 산드라 블록과 파멜라 앤더슨 같은 유명인들에게 좋지 않은 이미지를 주기 위해 나체의 여자 몸에 그들의 얼굴을 합성했다. 이런 경우 유명인들은 초상권을 가지고 있고 이런 악용은 그들의 초상권을 침해할 수 있다.

### 2-1. 아동 포르노 물

---

<sup>2</sup> 관련 배경 지식은 [http://en.wikipedia.org/wiki/Battle\\_of\\_Iwo\\_Jima](http://en.wikipedia.org/wiki/Battle_of_Iwo_Jima) 참조

디지털 이미지 조작의 어두운 면이 있다. 1996년에 미국은 아동 포르노 방지법(CPPA)을 통과시켰다. 이 법은 아동을 성적인 존재로 이용하는 것을 방지한다. 그러나 이 법은 "실제" 아동과 컴퓨터로 만들어진 또는 아동을 그린 삽화와의 구분을 만들지 않았다. 2002년 미국 연방대법원은 CPPA가 표현의 자유를 위반한다고 결정했다. 특히 만약 아동이 실제 인물이 아니라면 해를 직접 당하는 아동이 없고 따라서 CPPA는 적용되지 않는다는 것이다. 이는 "아동 포르노그래피(CP)"와 "가상 아동 포르노그래피(VCP)"와의 구분을 만들었다.

- 아동 포르노그래피: 실제 아동을 성적인 상황에 이용할 경우 CPPA의 제재를 받는다.
- 가상 아동 포르노그래피: 실제 아동이 나오지 않는 이미지는 "포르노그래피"로 분류되어 표현의 자유에 의해 보호받는다.

법적인 측면에서 CP와 VCP간의 구별은 소아성애병자를 기소하는데 매우 중요하다. VCP에 대한 사건은 CP에 대한 것보다 판단하기가 훨씬 어렵다. 결과적으로 이미지 수정에 대한 다른 관점들이 확립되어야 한다. 예를 들어 실제 사진에 oil painting 알고리즘을 적용하면, 이미지는 디지털적으로 수정되지만 여전히 실제 아동을 표현한다. 대조적으로 컴퓨터로 만든 아동 이미지는 분명히 VCP이다. "프랑켄슈타인 아이-다른 아이들의 사진을 photoshop으로 모아 하나 이상의 어린이를 이루는"를 포함하여 다른 복잡한 시나리오들은 아직 법원에서 테스트되지 않았다.

## 2-2. 디지털 인증

많은 웹 사이트들은 본인 이외의 다른 사람이 허가 없이 사용하는 것에 대한 불만을 해결하기 위해 인증을 필요로 한다. 어떤 경우는 사진이나 정부 ID(주민등록번호 같은)가 필요하다. MySpace는 사진 인증을 필요로 하는 사이트의 한 예<sup>3</sup>이다. 온라인 사기꾼이나 가로챈 계정을 이용할 경우 MySpace는 인증으로 디지털 이미지를 요구한다. 이미지는 MySpace의 계정 정보(MySpace의 Friend ID)를 담고 있는 것이어야 한다. 그러나 MySpace는 이미지를 정확하게 인증하는 방법을 가지고 있지 않다. 결과적으로 MySpace는 다음 종류의 사용자 정보를 제거했거나 가로챈 조작된 이미지를 잘못 받아들인다.

- 내가 아닌 경우: MySpace는 이미지가 실제 계정 정보를 가지고 있는지 알려줄 방법이 없기 때문에, 적절한 sign을 가지고 있는 사람은 누구나 자신이 계정 정보를 가지고 있다고 주장할 수 있다.
- 가짜 텍스트: 만약 다른 사람 계정에 대한 정보가 적힌 표지판이나 종이를 가지고 있는 이미지라면, Photoshop으로 텍스트를 바꿀 수 있다.
- 가짜 sign: 유효한 계정 정보를 담고 있는 이미지를 Photoshop을 이용해 sign을 가지고 있는 것처럼 보일 수 있다.

---

<sup>3</sup> MySpace에서는 누군가 자신의 계정이 도용 당하고 있다면 자신이 직접 적은 MySpace.com 글과 Friend ID를 자신의 사진과 함께 보내달라고 한다.

관련 공지: <http://www.myspace.com/index.cfm?fuseaction=misc.faq&Category=3&Question=26>

예제 사진: <http://www.boingboing.net/2006/08/10/confirm-your-identit.html>

조작된 이미지를 알아낼 수 있는 발전된 방법들이 있음에도 위에서 언급한 종류의 이미지들을 MySpace에 제출하면 MySpace profile이 만료되어 버린다.

### 3. 이미지를 분석하는 방법

이미지 분석은 이미지 수정에 대해 다음과 같은 의문을 던진다:

- 이미지가 진짜인가, CG인가, 디지털적으로 quality가 향상되었나
- 이미지가 진짜라면, 언제 어디서 어떻게 찍혔는가 (예를 들면 카메라 모델)
- 이미지가 디지털적으로 quality가 향상된 것이라면, 무엇이 수정되었고 어떻게 수정이 이루어졌는가
- 이미지가 CG라면, 어떻게 이미지가 만들어졌는가

이미지 분석에 4가지 다른 접근법이 있다.

- 관찰(Observation): 많은 경우 위조되거나 조작된 이미지는 직접 관찰에 의해 확인될 수 있다. 이미지 분석 도구가 필요하지 않다.
- 기본적인 이미지 향상(Basic Image Enhancements): sharpening, blurring, scaling, re-coloring 등과 같은 일반적인 알고리즘을 통해 이미지 내의 특성이 더욱 명확하게 만들 수 있다.
- 이미지 포맷 분석: 이미지의 변화는 파일 포맷을 바꾼다. JPEG과 다른 압축 손실이 많은 이미지 포맷의 경우 이미지에 변화가 생길 경우 알 수 있다.
- 향상된(Advanced) 이미지 분석: signal 분석은 수정여부를 찾아낼 수 있다. Error level 분석에서부터 principal component 분석(PCA), wavelet transformation까지 있다.

#### 3-1. 관찰에 의한 분석

가장 간단한 분석 방법은 사람의 관찰을 통해 이미지로부터 정보를 가져오는 것이다. 디지털적으로 품질이 향상(enhanced)된 것이거나 CG에는 보통 불일치(inconsistencies)가 존재한다. 이미지 내의 item은 언제 어디서 이미지가 만들어졌는지 확인하는데 사용될 수 있다. 이미지 내 찾아볼만한 item은 다음과 같다.

- Specular highlights와 그림자(shadows): 밝게 빛나는 부분과 그림자는 빛의 방향을 알려준다. Item들이 하나로 합쳐졌을 때, 빛의 방향이 다를 수 있다.
- Color tones in anti-aliasing: 이미지는 날카로운(sharp, crisp) 모서리를 보통 가지지 않는다. 대신에 anti-aliasing 기법은 인접한 색을 같이 흐리게 한다. 하나의 사진으로부터 한 부분을 잘라내어 다른 것과 같이 붙일 때, 모서리는 보통 새로운 배경색과 맞지 않는 색을 가지고 있을 수 있다.

- 반사(reflections): 이미지가 shopped(*Photoshopped*) 되었을 때, 반사는 변하지 않는다. 예를 들어 제거된 물체가 반사된 곳에는 그대로 존재할 수 있다. 비슷하게 추가된 물체는 반사된 곳에 빠져있을 수 있다.
- Scale: 이미지가 합쳐졌을 때 정확한 scale을 가지지 않을 수 있다.
- Roots: 이미지에 사람들이나 물체를 붙였을 때 “떠있는 것”처럼 보일 수 있다.
- 물체(object): 이미지 속의 일반적인 물체는 특정 지역, 시간에 있을 수 있다. 예를 들어 전기 콘센트는 나라에 따라 다르다. 이미지 속의 문자와 화폐로 지역을 확인할 수 있다. 그리고 시계나 달력은 시간을 알려준다. 비슷하게, 모니터 화면을 보여주는 사진은 특정 어플리케이션, 운영 체제, 알아볼 수 있는 웹 사이트를 알려준다.
- Duplication: 이미지 내의 아이템은 이미지의 다른 곳에 복사, 복제될 수 있다. Duplication은 수정이 안된 것, scaled, 회전된 것(rotated), flipped 또는 조작된 것일 수 있다.

불행하게도, 많은 item들은 이미지의 품질을 높이지 않으면 명확하게 분간할 수 없다. Basic image enhancement 방법은 보다 쉬운 확인을 위해 이미지 내에서 각 요소(elements)를 명확하게 한다.

### 3-2. Basic Image Enhancements

대부분의 사진 편집 툴들은 basic image enhancement 기능을 포함하고 있다. 이 기능들은 사진(또는 사진 내 부분)을 명확하게 하는데 사용될 수 있다. 일반적인 향상(enhancement) 기능은 다음을 포함한다.

- Brightness와 contrast: 이 알고리즘은 어두운 곳을 밝게, 숨겨진 물체를 보이게 또는 퇴색한 이미지의 색조를 달라지게 할 수 있다.
- Color adjustment: 빛은 이미지 내 color scheme에 크게 영향을 미친다. 많은 도구들은 이미지의 temperature(frequency range)를 바꾸거나 각 color component들을 조정할 수 있다.
- Invert: 이미지(negative image)의 inverting 부분은 유사한 색 때문에 불분명한 정보를 나타낼 수 있다.
- Sharpen and blur: 초점이 맞지 않거나 움직임 때문에 흐릿한 아이템은 이 기능으로 조정될 수 있다.
- Normalization and histograms: 발전된 도구는 색 범위(color range)를 보거나 수정을 가능하게 한다. 예를 들어, 한 이미지의 색이 너무 균등하게 되어있는 경우 normalized 이미지는 다양한 색 범위(color range)를 가질 수 있다.
- Scale: 어떤 이미지 포맷의 경우 물체가 왜곡되기 전 확대할 수 있다. 예를 들어, 고해상도의 JPEG이미지는 이미지가 크게 왜곡되기 전에 200%정도 확대할 수 있다. 비슷하게, 매우 큰 이미지는 쉽게 보기 위해 축소할 수 있다.

#### 3-2-1. 예: Warez Factory

불법 CD 복제 시설의 사진(그림2)은 최근 와레즈 전용 포럼에 올라왔다. 사진 속에는 CD 복사기,

“인증” 마크를 붙이기 위한 스탬프 그리고 심지어 CD 케이스까지 있다. 그러나 이 사진이 얼마나 인터넷을 돌아다녔는지 정확히 알 수 없다. 따라서 의문점이 생긴다: 이 사진은 언제 어디서 찍혔을까?

방 안의 두드러진 글자는 Tarzan & Jane 영화 포스터와 알코올 병에서 찾을 수 있다. 이 이미지를 sharpening하고 contrast를 enhance 시킴으로써 글자를 읽을 수 있게 되었다(그림3,4). 특히 글자가 스페인어이기 때문에 지역이 멕시코, 베네수엘라, 아르헨티나 또는 다른 스페인어를 사용하는 나라일 수 있다. 알코올 병은 “Madrileno(마드리드)”라는 글자가 적혀있어 스페인임을 암시한다. Tarzan & Jane 영화 포스터는 3월 26일에 DVD 배포 날짜가 있으나 연도에 대한 정보는 없다. 이 영화는 스페인에서 2006년 3월 26일에 DVD로 출시되었다. DVD 판촉 포스터는 보통 비디오가 나오기 전 몇 개월 전에 나오고, 나오자마자 구하기는 어렵다는 것을 고려해보면 사진이 찍힌 날짜의 범위를 추측할 수 있다: 2003년 1월~5월이다. 방에 매우 많은 물건들이 있지만 2003년 이전의 특정 연도를 확인할 수 있는 것은 없다. 날짜와 장소에 추가적으로 방의 특징을 확인할 수 있다. 예를 들어 벽의 전화 콘센트를 보면 3달러의 새로운 전화 콘센트가 있다. 이는 이 방이 원래 RJ11 jack이 있는 전화를 제공하지 않는다는 것을 말해준다. 따라서 콘센트에 연결된 전화기는 없기 때문에 컴퓨터에서 사용하기 위해 설치되었다고 할 수 있다.



그림2) 불법 CD 복제 공장.

2007년 5월 23일에 [http://www.bork.ca/pics/?incoming/warez\\_factory.jpg](http://www.bork.ca/pics/?incoming/warez_factory.jpg)에서 구했다.



그림3) Tarzan & Jane 포스터에 “3월 26일” DVD 출시를 알리고 있다.  
이 사진은 sharpened 되었다.



그림4) 스페인어가 적힌 알코올 병.  
이 이미지는 scaled, sharpened, contrast가  
조정되었다.



그림5) 벽에 전화 콘센트(위).  
electronic store part (아래)

### 3-2-2. 예: Moonwalk

2006년에 Andrea Bertaccini가 Buzz Aldrin의 유명한 moonwalk(그림6)를 rendering 한 것으로 CG Society로부터 “CG Choice Award”를 수상했다. Bertaccini에 의하면 사진은 NASA 원본 사진을 기초로 한 것이다. 그러나 사진의 구체적인 부분은 추가적인 resource를 사용한다.





그림6) Andrea Bertaccini 이미지([www.tredistudio.com](http://www.tredistudio.com), 왼쪽)와 NASA 원본 사진(오른쪽)

두 사진을 비교해보면 상당한 수의 차이를 발견할 수 있다. Bertaccini의 사진에서 달의 먼지가 많이 없는 것 외에도 다른 주목할만한 차이점을 볼 수 있다.

- 부풀림(Puffy): 원본 사진 속 우주복에 주름이 저 있다면, CG의 우주복은 “부풀려 진” 것으로 보인다.
- 섬유(Fibers): 원본 사진 속 우주복의 팔 부분에는 울 스웨터같이 명확하게 섬유가 보인다. 하지만 CG에는 빠져있다.
- 나사(Grounding screw): 원본 사진의 몸 쪽에 붙어있는 상자(그림7)는 가운데 어두운 색의 나사가 있다. 하지만 Bertaccini의 사진에는 밝은 색의 나사가 있다.
- 연결 부분(Connectors): Bertaccini의 사진에는 빨강고 푸른색의 상자 연결 부분에 6개의 반짝이는 나사가 있다. 하지만 이 나사들은 원본 사진에는 보이지 않는다. 실제 우주복에는 이 나사들이 있으나 반짝이지는 않는다.
- 허리띠(Belt): Bertaccini의 허리띠는 metal clip이 있다. 하지만 NASA의 사진에는 metal clip이 허리띠에 없다.

이런 차이점들은 원본 이미지에서부터 기인한 것일 수 있다. Bertaccini의 사진은 2006년에 발표되었다. 2005년에 IMAX는 moonwalk를 다시 구성한 위대한 황야(Magnificent Desolation)라는 영화를 만들었다. 이 영화의 촬영 뒷 이야기의 사진(그림8)을 보면 Bertaccini의 사진과 비슷한 우주복(주름지지 않았고, 팔에 섬유가 보이지 않고, 나사가 밝은 색이고, 몸 쪽의 상자의 연결 부분에 6개의 반짝이는 나사가 있고, 허리띠에 metal clip이 있는)을 볼 수 있다. Bertaccini의 사진 위치가 NASA의 사진에 기초한 것이라도 우주복은 IMAX의 영화에 기초한 것으로 보인다.





그림7) 재구성한 사진과 원본 사진의 몸 쪽 부분 확대



그림8) IMAX의 위대한 황야 영화의 촬영 뒷 이야기 사진

### 3-3. 이미지 포맷 분석

이미지는 다양한 포맷으로 저장될 수 있다. RAW 같은 것은 단지 픽셀 정보만 저장하지만 다른 포맷들은 다양한 정보를 포함한다. JPEG, GIF, PNG, TIFF와 같은 많은 포맷의 경우 이미지 그 자체만 큼 정보를 가지고 있다고 할 수 있다. 이미지의 변화는 파일 포맷의 변화를 초래한다. 이 문서가 JPEG 포맷에 초점을 맞추지만 방법은 GIF, PNG, TIFF를 포함한 다른 복잡한 포맷에도 적용될 수 있다.

JPEG 파일은 특징들이 잘 정의되어 있다. 이미지의 변화는 포맷 내의 특징을 변화시킬 것이다. 그러므로 특징이 이미지의 수정을 나타내면 이는 즉 이미지 수정을 확인할 수 있다는 것을 말한다. JPEG의 특징은 메타 데이터, 이미지 압축에 관한 quantization tables, 손실이 있는 데이터 압축, 8x8 픽셀 크기를 이용한 이미지 분할 과정을 포함한다.

### 3-3-1. 메타 데이터 분석

대부분의 JPEG 파일은 이미지 원본을 나타내는 상당한 양의 메타 데이터를 가진다. 예를 들어 디지털 카메라로 찍은 JPEG 파일은 보통 카메라 타입, 해상도, 초점 설정 등의 특징을 포함한다(아래 참조).

```
$ exiftool IM001022.JPG
MIME Type           : image/jpeg
JFIF Version        : 1.1
Make                : Hewlett-Packard
Camera Model Name   : HP PhotoSmart 618
Orientation         : Horizontal (normal)
X Resolution        : 72
Y Resolution        : 72
Resolution Unit     : inches
Y Cb Cr Positioning : Centered
Exposure Time       : 1/125
F Number            : 3.7
ISO                 : 100
Exif Version        : 0210
Date/Time Original  : 2007:05:28 09:19:49
Components Configuration : YCbCr
Compressed Bits Per Pixel : 1.6
Shutter Speed Value : 1/128
Aperture Value      : 4.0
Exposure Compensation : 0
Max Aperture Value  : 4.0
Subject Distance    : 0.13 m
...
```

디지털 카메라로 찍은 사진의 메타 데이터 예

위에서 사용한 exiftool은 <http://www.sno.phy.queensu.ca/~phil/exiftool>에서 다운로드 받을 수 있습니다. 다운로드 받아 시험삼아 JPEG 파일로 실행해 보면 다음과 같은 결과가 나옵니다.

\*\*\*\*\*

```
C:\Documents and Settings\freeman> "C:\Documents and Settings\freeman\바탕 화면\ExifTool-7.21\ExifTool(-k).exe" "C:\Documents and Settings\freeman\바탕 화면\DSCN7473.JPG"
```

```
ExifTool Version Number      : 7.21
File Name                    : DSCN7473.JPG
Directory                    : C:\Documents and Settings\freeman\바탕 화면
File Size                    : 660 kB
File Modification Date/Time   : 2003:01:01 00:00:00
File Type                    : JPEG
```

```

MIME Type                : image/jpeg
Exif Byte Order           : Little-endian (Intel)
Image Description         :
Make                      : NIKON
Camera Model Name         : E3700
Orientation               : Horizontal (normal)
X Resolution              : 300
Y Resolution              : 300
Resolution Unit           : inches
Software                  : E3700v1.2
Modify Date               : 0000:00:00 00:00:00
Y Cb Cr Positioning       : Co-sited
Exposure Time             : 1/319
F Number                  : 2.8
Exposure Program          : Program AE
ISO                       : 50
Exif Version              : 0220
Date/Time Original        : 0000:00:00 00:00:00
Create Date               : 0000:00:00 00:00:00
Components Configuration : YCbCr
Compressed Bits Per Pixel : 2
Exposure Compensation     : 0

```

...

\*\*\*\*\*

메타 데이터가 상당한 양의 정보를 제공하지만 한계가 있다. 첫 번째로 메타 데이터는 수정이 가능하다. 그렇지만 카메라 타입과 설정에 관한 잘못된 정보는 JPEG 내부적으로 바꿀 수 있다. 또한 잘못된 기본 설정이다. 예를 들어, 대부분의 디지털 카메라가 시간대나 서머타임을 지원하지 않으며 시간이 흐르는 것만 알 지도 모른다. 결과적으로 시간은 정확하지 않을 수 있다.

고의적인 메타 데이터 수정보다 더 흔한 것은 메타 데이터를 혼동하게 하는 것이다. 예를 들어, 디지털 카메라로 찍은 사진은 Photoshop으로 열고 수정할 수 있다. 사진이 저장될 때 심지어 더 이상 맞지 않는 카메라의 메타 데이터 정보를 유지한다. Photoshop은 수정사항을 저장할 때 메타 정보를 바꾸지 않는다. 결과적으로 메타 데이터는 데이터가 정확할 때 유용하지만 데이터는 정확하다고 입증하기 어렵다.

### 3-3-2. JPEG Quantization Fingerprinting

Quantization fingerprinting, 또는 ballistics<sup>4</sup>은 특정 메타 데이터와 맞지 않는 이미지를 찾아내는

---

<sup>4</sup> Hany Farid, "Digital Image Ballistics from JPEG Quantization", Dartmouth College, TR2006-583, 2006. <http://www.ists.dartmouth.edu/library/204.pdf>에서 참조가능

방법을 제공한다. JPEG 알고리즘은 이미지 압축과 품질을 조절하기 위해 일련의 quantization matrix들을 사용한다. JPEG에 있어서 이미지는 RGB에서 YCrCb로 변환된다. 하나의 quantization matrix는 휘도(luminance)(Y)를 다루고, 두 번째 matrix는 빨간색(Cr)과 파란색(Cb) 둘의 색차(chrominance)를 다룬다.

이상적으로는 quantization table은 각 이미지 별로 생성되고 최적화되어야 한다. 그러나 이런 matrix들을 계산하는 것은 시간이 소비된다; 대부분의 디지털 카메라는 CPU power를 가지고 있지 않고, 대부분의 응용 프로그램들은 이미지를 저장하기 위해 20초 정도 사용자가 기다리는 것을 원치 않는다. 이 과정을 간단히 하기 위해 가상적으로 모든 그래픽 관련 프로그램과 디지털 카메라는 hard-coded quantization table을 사용한다. 이런 기본 table은 종종 데이터 크기, 색 spectrum, 디지털 카메라 CCD properties, 제조사 needs에 따라 최적화된다. 예를 들어, 캐논 디지털 카메라로 찍은 사진은 보통 캐논 프린터에서 출력이 잘 되는데 왜냐하면 색이 제조사에 맞게 최적화되어 있기 때문이다. 그리고 세가지 품질 설정(low, medium, high)을 가지고 있는 디지털 카메라는 보통 각각에 맞는 세 개의 hard-coded quantization table을 가지고 있다.

미리 계산된 quantization table은 제조사에 맞춰져 있기 때문에, table은 응용 프로그램과 카메라 모델에 따라 다르다<sup>5</sup>. 만약 quantization table을 확인할 수 있다면, JPEG을 저장한 툴도 확인할 수 있다. 더욱 중요하게는, 만약 quantization table이 메타 데이터에서 지정한 카메라 정보와 맞지 않는다면, 그 이미지는 다시 저장되었거나 수정되었다고 할 수 있다.

### 3-3-3. JPEG Quality Detection

JPEG 이미지를 저장할 때, 대부분의 툴들은 이미지의 품질을 선택할 수 있게 한다. 일반적으로 낮은 품질일수록 이미지는 작아진다. 예를 들어, 90% 저장된 이미지는 대략 10%의 이미지 손실(픽셀의 색 정보는 원본과 정확하게 같지 않다)이 있다. 99%의 품질로 데이터 손실을 거의 없게 하면서 매우 큰 이미지를 만들 수 있다. 대조적으로 75%인 경우 상당히 작은 파일을 만들어서 충분히 원본 이미지의 의미를 전달할 수 있다.

알려진 quantization table이 품질뿐만 아니라 툴을 확인할 수 있게 함에도 불구하고, quantization table이 언제나 알려진 프로그램이나 카메라와 맞지 않을 수 있다. 이런 경우에 JPEG의 품질은 어림잡아 알 수 있다.

각 quantization table은 64 바이트를 포함한다. 첫 번째 바이트는 DC이고 scalar 값으로의 기능을 한다. 남은 63 바이트는 AC이고 frequency에 따른 압축을 정의한다. Hacker Factor Solution에 의해 개발된 JPEG 품질의 근사치를 구하는 알고리즘은 다음과 같다:

- 1) 각 quantization table의 AC값의 평균을 구한다. 예를 들어, table이 아래와 같다면,

---

<sup>5</sup> <http://www.impulseadventure.com/photo/jpeg-quantization.html>

# Quantization table	# Quantization table
# Table index=0 (luminance)	# Table index=1 (chrominance)
3 2 2 3 2 2 3 3	3 4 4 5 4 5 9 5
3 3 4 3 3 4 5 8	5 9 20 13 11 13 20 20
5 5 4 4 5 10 7 7	20 20 20 20 20 20 20 20
6 8 12 10 12 12 11 10	20 20 20 20 20 20 20 20
11 11 13 14 18 16 13 14	20 20 20 20 20 20 20 20
17 14 11 11 16 22 16 17	20 20 20 20 20 20 20 20
19 20 21 21 21 12 15 23	20 20 20 20 20 20 20 20
24 22 20 24 18 20 21 20	20 20 20 20 20 20 20 20

Table 0의 AC 평균값은 11.63이고 Table 1은 17.57이다.

- 2) 평균 압축 값은 모든 table을 통해 계산된다. 예를 들어, Table 0는 한번(Y) 사용되었고, Table 1은 두 번(Cr과 Cb) 사용되었기 때문에 평균 값은  $(11.63+17.57+17.57)/3 = 15.59$ 가 된다.
- 3) 이미지는 RGB를 이용해서 그려지지만 table은 YCrCb를 나타낸다. 변환은 다음과 같다.

$$R = Y + (R - Y) = Y + Cr$$

$$G = Y - 0.51 (R - Y) - 0.186 (B - Y) = Y - 0.51Cr - 0.186Cb$$

$$B = Y + (B - Y) = Y + Cb$$

Significant ratio가 0.51이기 때문에, 변환율(Conversion rate)은 table사이의 차이에 의해 결정된다.

$$D = \|Y - Cr\| * (1.0 - 0.51) + \|Y - Cb\| * (1.0 - 0.51)$$

$$D = \|11.63 - 17.57\| * 0.49 + \|11.63 - 17.57\| * 0.49 = 5.82$$

- 4) 변환율은 품질을 추측하는데 같이 쓰인다:  $100 - 15.59 + 5.82 = 90.23$ . JPEG 알고리즘이 실수 대신에 정수를 사용하기 때문에, 이 값은 가장 가까운 정수 값으로 변환한다. 이 예제 이미지는 90%의 품질 level로 저장되었다.

이 알고리즘은 'xv', Gimp, ffmpeg, libjpeg 등 대부분의 다른 도구들을 가지고 저장한 이미지로부터 품질을 정확하게 결정한다. 그러나 Photoshop의 경우는 백분율 계산을 다르게 하는 것 같다; Photoshop으로 저장한 JPEG은 사용자 인터페이스에서 설정한 품질과 맞지 않는 것으로 보인다. 예를 들어, Adobe Photoshop을 사용하면 "80%"("Save for Web"을 사용)로 저장한 이미지는 91%의 quantization table을 가진다.

### 3-4. 발전된 이미지 분석

이미지 포맷 분석으로 메타 데이터의 불일치를 발견할 수 있고 이미지를 마지막으로 수정한 툴이 무엇인지 알 수 있다. 그러나 포맷 분석은 이미지 자체를 검사하지는 않는다. Principal component 분석이나 error level 분석, wavelet transformation과 같은 방법으로 특정 이미지 수정 여부를 알

수 있다.

### 3-4-1. Principal Component 분석

JPEG은 손실이 많은 압축 알고리즘을 사용한다; JPEG 파일로 그려진 이미지는 원본 이미지의 완벽한 복사판은 아니다. JPEG 이미지가 그래픽 편집 툴에 의해 다시 저장될 때 마다(심지어 편집 툴로 이미지를 바꾸지 않아도) 이미지 품질이 낮아진다. 이는 quantization table 분석을 어렵게 한다; 만약 75%의 품질로 저장된 이미지를 그래픽 프로그램으로 로드하여 90%로 다시 저장한다면, 이미지의 품질이 67.5%(75%의 90%)임에도 quantization table은 90%를 나타낼 것이다.

JPEG에서의 오류는 blocky artifacts와 색의 왜곡으로 나타난다. Blocky artifacts는 JPEG 알고리즘에 의해 사용된 8x8 픽셀 범위에서 나타난다. 많은 경우에 JPEG artifacts는 너무 미묘해서 사람 눈으로 발견하기 어렵다. 그러나 principal component 분석(PCA)은 이러한 JPEG artifacts를 확인할 수 있다.

#### 3-4-1-1. PCA의 이해

PCA는 데이터 점(data points)을 클러스터링 하기 위해 사용된다<sup>6</sup>. 각 principal component는 데이터 set 전역에 걸쳐 평면을 형성한다. 첫 번째 principal component(PC1)는 데이터에서 가장 넓은 편차(variance) 범위의 평면을 결정한다. 사실상 모든 점으로부터 PC1 평면 사이의 평균 거리는 최대가 된다. 두 번째 principal component(PC2)는 PC1에 관해 두 번째로 넓은 편차(variance) 평면을 결정한다. 3차원이기 때문에 3개의 principal component가 있다. 마지막 component(PC3)는 가장 작은 편차(variance)를 가진다; 각 점으로부터 PC3까지의 평균 거리는 가장 작다.

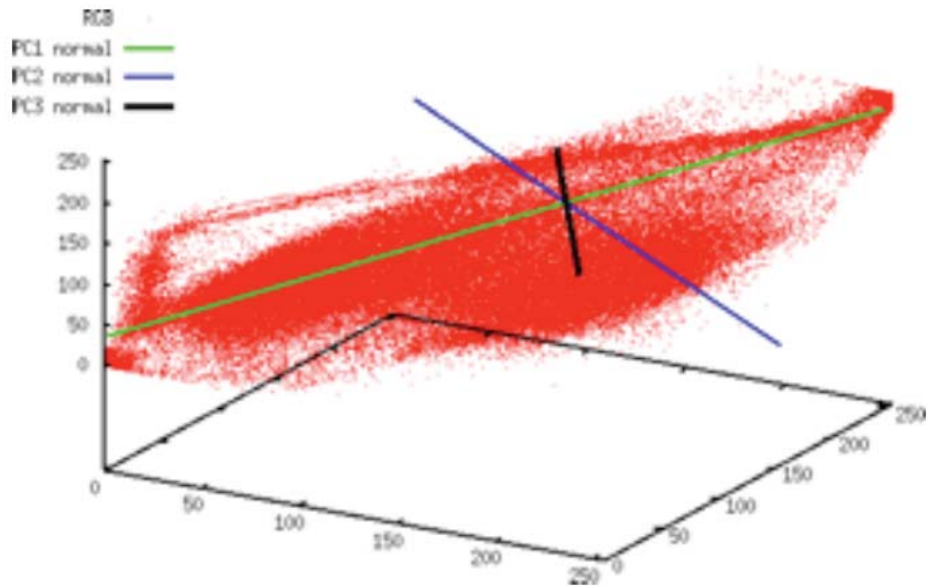
PCA 분석은 일반적으로 클러스터링, robotic vision, 데이터 압축 같은 information reduction problem을 위해 사용된다. 예를 들어, PC3은 가장 작은 편차(variance)를 포함하는 반면 PC1은 데이터 내에 가장 큰 편차(variance)를 가진다. 손실이 큰 데이터 압축에서 PC3에 있는 값들은 가장 적은 영향으로 제거될 수 있다. 각 principal component는 information의 다른 측면을 강조한다.

이미지 분석에서 PCA는 이미지 내의 color spectrum을 확인하기 위해 사용된다. 픽셀 색에 기초한 전체 이미지를 고려할 때 (R,G,B)는 (x,y,z)에 mapping된다(아래 그림). 대부분의 이미지들은 커다란 클러스터처럼 보이는 좁은 범위의 색을 가진다. PC1은 color set에서 가장 넓은 범위를 가진다. 다른 color set을 가지는 서로 다른 두 개의 이미지들이 서로 합쳐졌을 때, 보통 두 개의 구별되는 클러스터를 형성한다. PCA를 이용해서 다른 클러스터로부터 온 사진 내의 부분은 두드러지게 다른 값을 가질 것이다.

---

<sup>6</sup> Jonathon Shlens, "A Tutorial on Principal Component Analysis", Salk Institute for Biological Studies, 2005. <http://www.sn1.salk.edu/~shlens/pub/notes/pca.pdf> 참조





< 이미지의 plot scatter와 principal components의 예 >

#### 3-4-1-2. PCA 시각화 옵션

각 픽셀로부터 principal component까지 거리를 그리는 방법은 두 가지가 있다(그림9). 첫 번째로 각 점에서부터 평면까지 거리는 최대 편차(variance)를 가지며 측정 가능하다. 일반적으로 PC1은 매우 또렷한 gray-scale의 사진을 생성한다; 이는 가장 많은 정보를 포함한다. 대조적으로 PC3은 보통 규칙적인 색을 가지는 것처럼 보이는데 왜냐하면 모든 점들은 PC3 평면으로부터 비슷한 거리에 있기 때문이다. PC3가 가장 적은 양의 정보를 정의함에도 불구하고, 이는 보통 JPEG artifacts를 확인하는데 가장 유용하다.

일반적인 선으로부터 데이터 집합의 가운데를 통과하는 평면까지의 거리 역시 측정 가능하다. PC1에 있어서 각 점으로부터 선까지의 평균 거리는 가장 좁은 편차(variance)를 가진다; 이는 가장 많은 정보의 양을 통한 가장 적은 편차(variance)이다. PC1 선을 이용하여 그리는 것은 보통 균일한 색을 가지는 것처럼 보인다. 대조적으로 PC3 선은 매우 또렷한 사진을 보여준다; 이는 가장 적은 정보 양을 통한 가장 큰 편차(variance)이다. PC1 선으로부터 PC3 평면까지의 거리에 기초한 이미지는 매우 유사해 보일 수 있음에도 불구하고, PC1 선은 더 많은 정보를 포함한다. 이 글에서의 모든 PCA 분석은 일반적인 선에서 principal component의 평면을 이용한다.

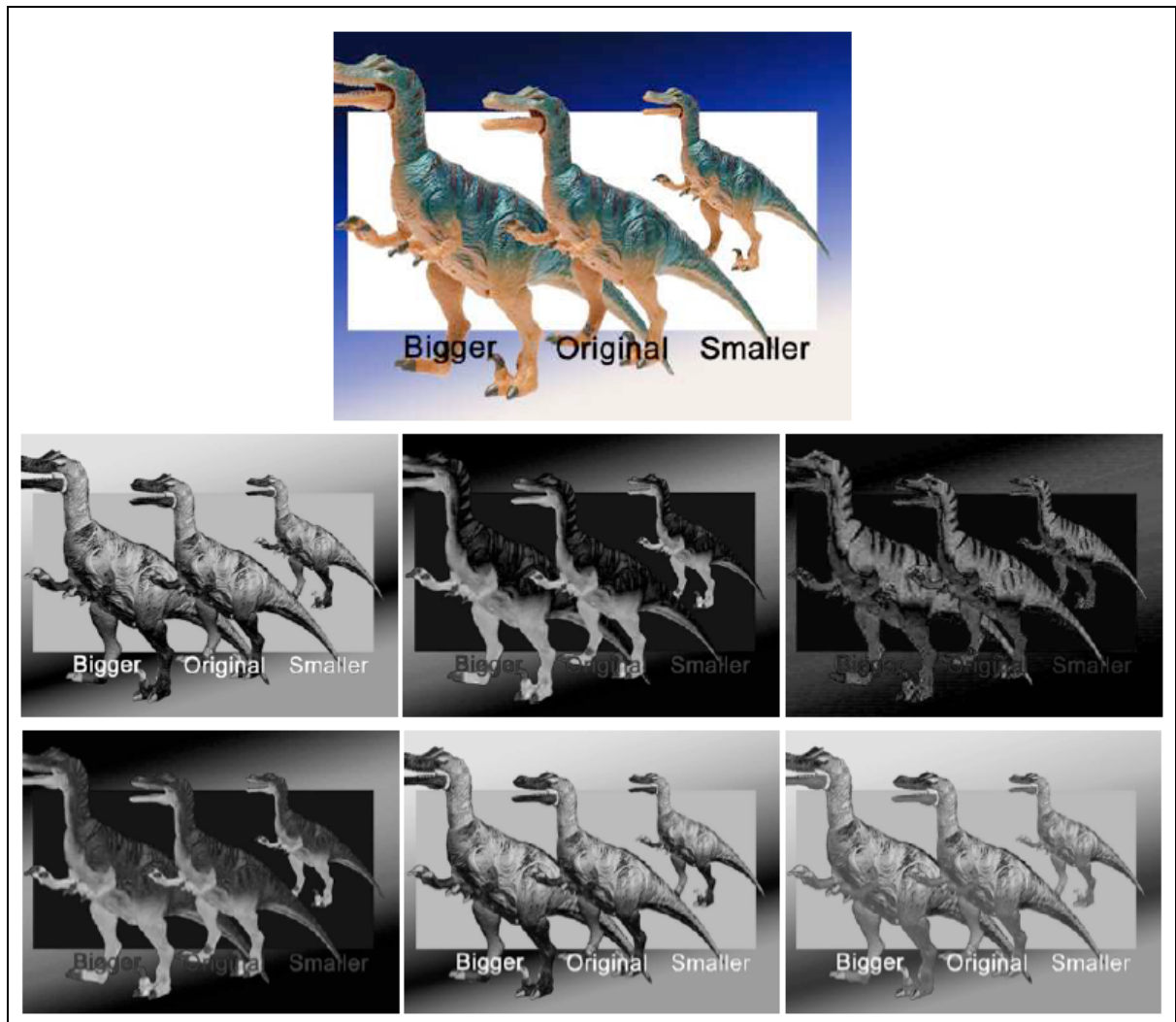


그림9) 윗줄 : 초기 이미지, 가운데 줄 : 평면으로부터 거리에 기초한 PC1, PC2, PC3 색, 아랫줄 : 일반적인 선으로부터 평면까지의 거리에 기초한 PC1, PC2, PC3 색

### 3-4-1-3. PCA를 이용한 JPEG Artifact 탐지

JPEG artifacts는 PC1 선이나 PC3 평면을 이용하여 그릴 때 보통 보여진다. 이러한 artifacts는 배경에 직사각형이나 사진 주위에 왜곡으로 보여진다(그림10). 그러나 PC3 평면은 보통 오직 한 번의 JPEG resave로부터 artifacts를 보여준다. 품질이 다른 두 개의 사진을 합칠 때, 사진들은 다른 JPEG artifacts를 가지고 온다. PC1 선에 기초한 그리기는 관찰자가 합쳐진 이미지를 확인할 수 있게 하면서 이런 차이를 특히 밝게 한다(그림11).

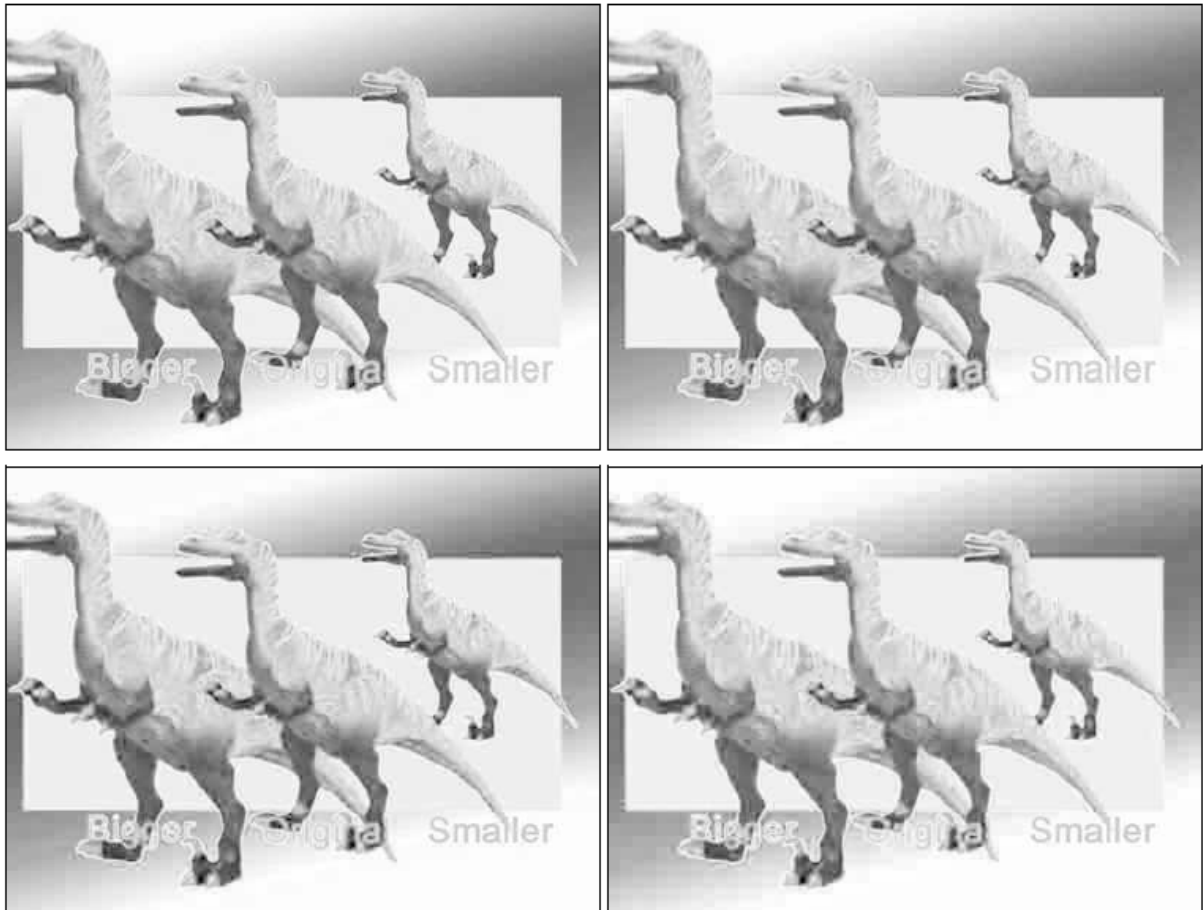


그림10) PC1 line을 이용한 JPEG artifacts.

이미지들은 90%, 80%, 70%, 50%이며 명료함을 위해 invert되었음.



그림11) 두 개의 이미지를 합침으로써 생긴 PC1. 왼쪽의 이미지는 90%였고 오른쪽은 75%이었다.

Blocky JPEG artifacts는 75% 이미지일 때 더욱 두드러진다.

### 3-4-1-5. PCA 예: Moonwalk

앞에서 언급했던 moonwalk 예제를 보자(섹션 3.2.2). 예술가는 이미지가 3DS MAX를 사용해서 만들어졌고 Combustion과 Photoshop을 이용하여 후속 작업을 했다고 한다<sup>7</sup>. Quantization matrix는 Photoshop의 'high(8)' 품질과 일치하고, 89%로 저장된 JPEG과 같다. 그러나 PC1 선을 이용하면 상당한 수의 40%정도의 품질과 유사한 artifacts를 볼 수 있다(그림12). 이것은 이미지가 여러 번에 걸쳐 저장되었다고 할 수 있다.

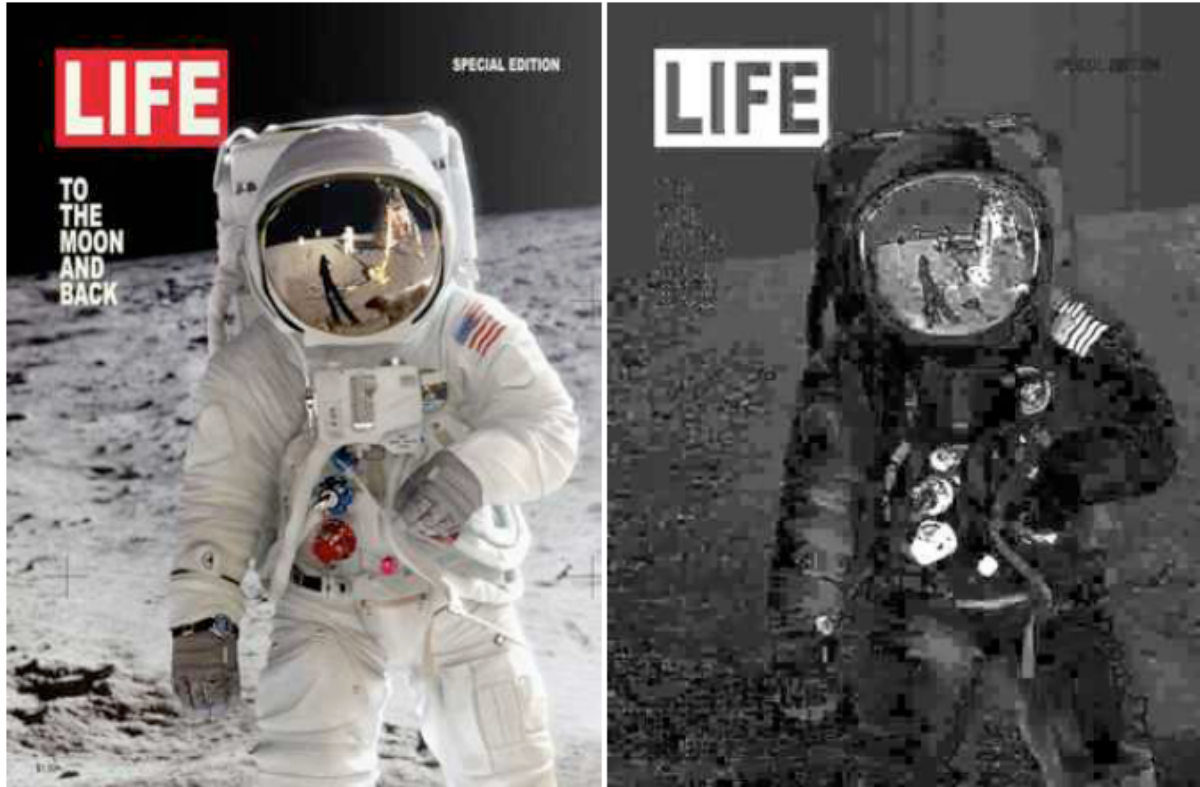


그림12) Moonwalk와 PC1

여러 번의 저장과 더불어서, 예술가가 배경과 헬멧 반사는 우주인이 그려진 다음에 추가된 bitmap이라고 이야기한 것으로도 알 수 있듯이, 우주복은 배경과 헬멧 반사보다 더 많은 artifacts가 있다. PC1으로 또한 빨간 색과 파란 색 컨넥터를 확인할 수 있는데, 빨간색의 "LIFE" 배경과 이 이미지 상에서 다른 색 scheme을 가지고 있는 미국 국기를 볼 수 있다(흰색은 PC1 선으로 부터 멀리 떨어진 것을 나타낸다). 이러한 부분은 예술가에 의해 처음 그려진 이후 품질이 향상된 것이다.

### 3-4-2. Error Level 분석

JPEG은 손실이 많은 포맷이지만 매번 다시 저장할 때마다 발생하는 Error의 양은 linear하지 않다. 90%의 이미지가 90%로 다시 저장된 경우는 처음에 81%로 저장한 것과 같다. 비슷하게 75%로

<sup>7</sup> <http://forums.sgsociety.com/showthread.php?t=323490>



이미지를 저장한 뒤 이를 다시 90%로 저장하면 90%에서 75%로 저장한 것이나 처음 67.5%로 저장한 것과 같다<sup>8</sup>. Error의 양은 JPEG 알고리즘에 사용되는 8x8 cell에 한정된다; 대략 64회에 걸친 저장 이후, 사실상 거의 변화가 없다. 그러나 이미지가 수정된 경우, 수정된 부분을 포함하는 8x8 cell은 수정되지 않은 다른 부분과 같은 Error level을 더 이상 가지지 않는다.

Error level 분석(ELA)은 의도적으로 이미지를 95%같은 알려진 error rate으로 다시 저장해서 이미지 간의 차이를 계산함으로써 이루어진다. 만약 변화가 없다면, cell은 그 품질 level에서의 최저 error 값을 가질 것이다. 그러나 많은 변화가 있다면 픽셀은 그 최저 값을 가지지 않고 사실상 “원본”과 같다. 그림13은 원본 이미지와 75%로 다시 저장된 원본 이미지이고 다시 또 75%로 저장한 이미지이다. 각 이미지 3개에 대한 95% ELA는 원본 픽셀을 포함하는 영역을 보여준다. 원본 이미지에서 거의 모든 픽셀은 최저 값을 가지지 않는다. 처음 75%로 다시 저장한 것은 최저 값을 가지는 픽셀들이 넓은 영역에 있다는 것을 보여준다. 두 번째 다시 저장한 것은 error에 대한 최저 값을 가진다.

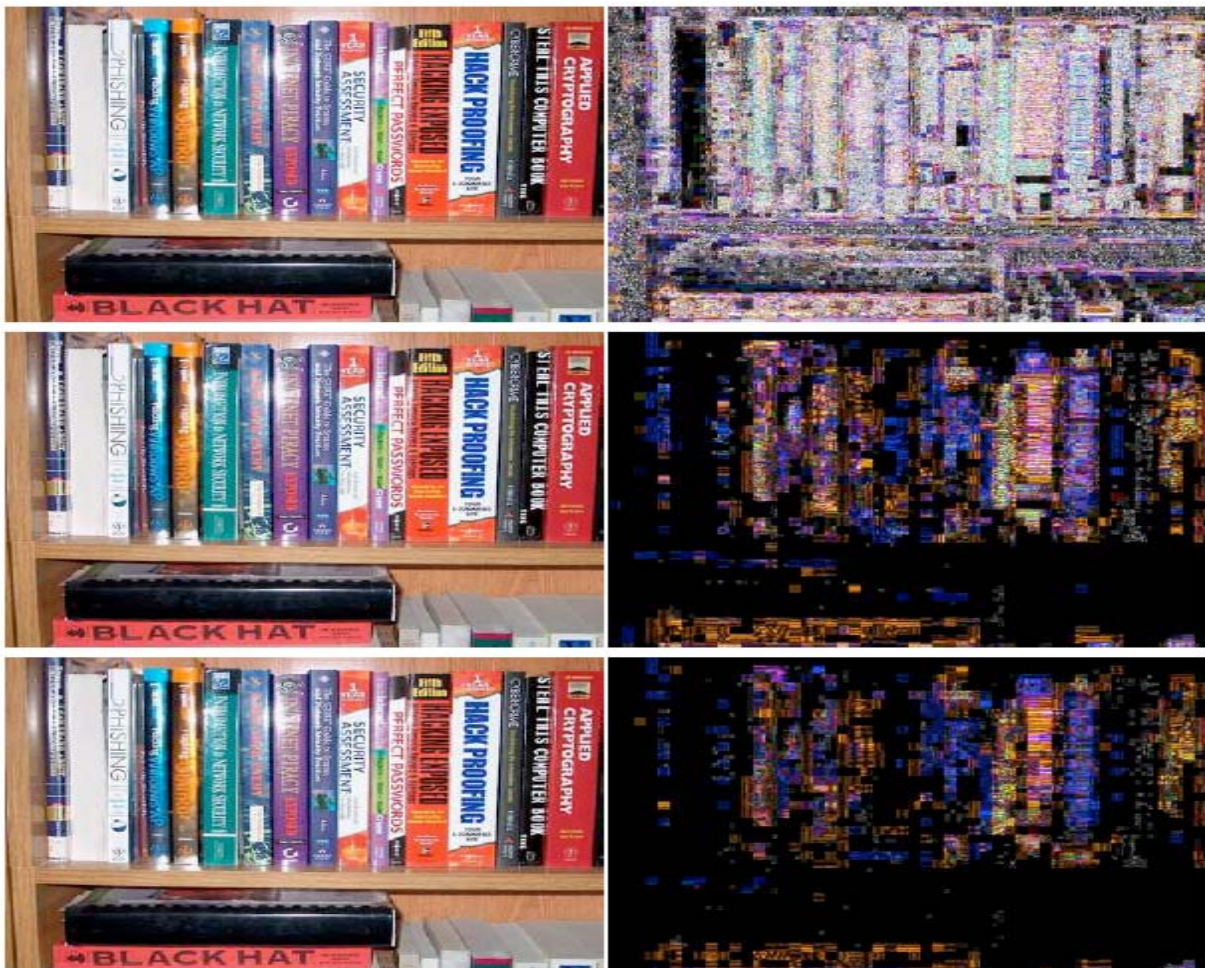


그림13) 디지털 카메라로 찍은 원본 사진, 75%로 다시 저장한 사진, 다시 75%로 저장한 사진.  
각 사진은 이미지에 대해 95% ELA를 적용했다.

<sup>8</sup> JPEG 알고리즘이 실수 대신 정수를 사용하므로 75%→90%이미지는 거의 90%→75% 이미지와 동일하다. 하지만 완벽하게 같다고는 할 수 없다.

사진에 대한 수정은 안정된 영역(추가 error가 없는)을 불안정한 영역으로 바꾼다. 그림14는 Photoshop으로 수정된 이미지이다. 수정된 사진은 처음 75%로 다시 저장한 것에 기초했다. 책장의 책은 복사되었고 공룡 장난감은 책장에 추가되었다. 95% ELA는 최저 error level이 아닌 영역임을 통해 수정 여부를 확인한다. 사진의 추가 영역은 약간 더 volatility를 보여주는데 왜냐하면 Photoshop은 여러 layer에서, 사실 많은 픽셀을 수정해서 정보를 합쳤기 때문이다.



그림14) 처음으로 다시 저장된 이미지(75%)는 수정되었다.

95% ELA는 수정된 영역을 알 수 있게 한다: 책장의 책은 복사되었고 공룡은 추가되었다.

#### 3-4-2-1. 예: Alf Kid

“Alf Kid” 또는 “Fat Alf Kid”(그림15)는 인터넷 상에서 거의 틀림없이 가장 많이 Photoshop된 사람 중 한 명이다. 보통 사람들은 그의 셔츠를 수정하거나 그를 재미있는 상황에 놔두곤 한다(그림16). ELA는 그의 이미지에 마지막으로 가해진 수정을 알 수 있다. 모순적이게도 대부분의 사람들에게 의해 사용된 “원본” 사진은 반복해서 저장되고 photoshop된다; 마지막 수정은 필요 없는 부분을 잘라낸 것이다(높은 ELA 값을 통해 밑부분과 오른쪽 여백을 보면 알 수 있다). 그리고 “ALF”라는 글자가 그의 셔츠에 추가되었다. 사실 원본 사진은 그의 셔츠에 ALF 글자가 없었을 지 모른다; 술한 다시 저장하기가 해당 정보의 손실을 가져왔다.





그림15) 원본 Alf Kid 이미지와 95% ELA를 겹친 이미지

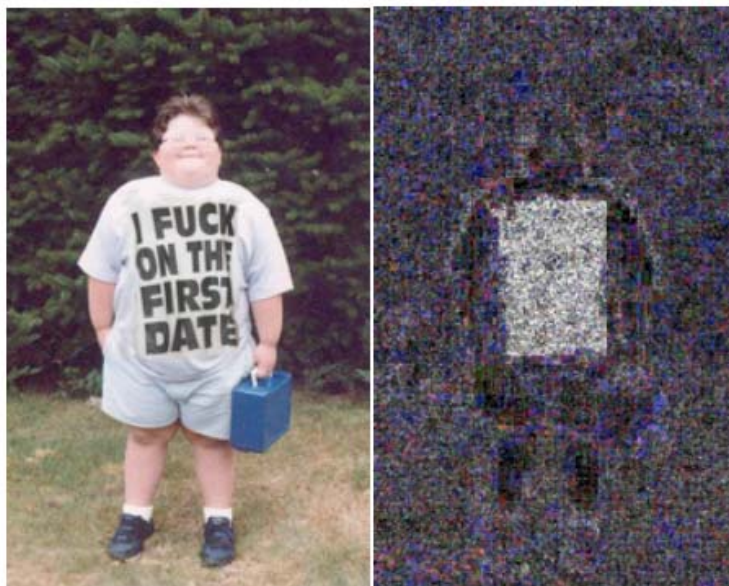


그림16) 셔츠가 수정된 Alf Kid와 그 옆의 오사마 빈 라덴. 95% ELA는 셔츠의 수정과 오사마 빈 라덴 사진의 다른 영역과 다른 낮은 Error level을 Alf Kid를 볼 수 있다.

### 3-4-2-2. 예: WTC Crash

2001년 9월 11일이 지난 지 얼마 안 있어, 비행기가 World Trade Center를 향해 날라오는 도중에 관광객이 그 건물 옥상에 서있는 사진이 나왔다(그림17). 예상대로 이 이미지는 조작이라고 발표되기 전에 많은 논쟁을 가져왔다. 95% ELA는 이 이미지에 마지막 수정이 있었다는 것을 알려준다: 날씨가 추가되었고, United Airlines의 줄이 비행기의 머리 부분에 위치하게 되었으며, 사람에 약간의 수정이 이루어졌다. 비행기가 이 사진에 추가되었음에도 불구하고 ELA로부터 정보를 알아보기에는 다시 저장하기가 많이 이루어졌다.



그림17) 충돌 사진과 95% ELA를 겹친 사진

### 3-4-3. Wavelet Transformations

ELA가 resave 횟수에 상대적으로 최근의 수정 사항을 알 수 있게 하는데 유용하지만, resave를 많이 하거나 매우 낮은 품질의 JPEG 사진인 경우 ELA 결과를 믿을 수 없다. 그러나 사진의 수정 사항은 wavelet transformations를 통해 여전히 확인할 수 있다.

Wavelet은 신호 분해(signal decomposition)에 사용된다<sup>9</sup>. 하나의 wavelet은 알려진, 잘 정의된 신호이다. 이 신호는 더 복잡한 신호를 만들기 위해 서로 크기가 조정되고(scaled) 합쳐진다. 실제 신호는 합쳐질 때의 대략적인 신호들의 집합으로 나눌 수 있다(그림18).

---

<sup>9</sup> Amara Graps, "An Introduction to Wavelets". IEEE Computational Science and Engineering, Summer 1995, vol.2, num 2. <http://www.amara.com/ftpstuff/IEEEwavelet.pdf> 참조

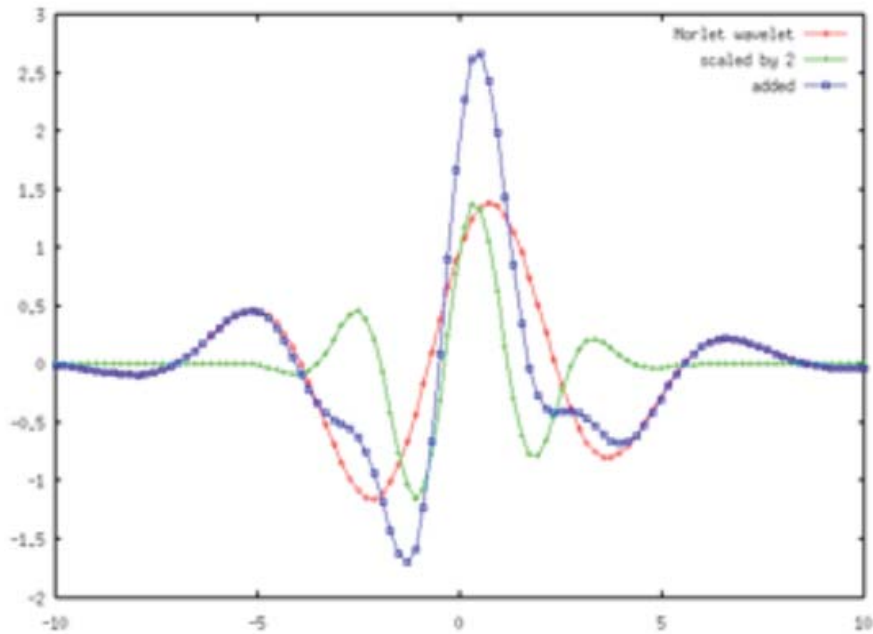


그림18) Morlet wavelet(빨강), scaled(녹색), 합쳐져서 생성된 더 복잡한 신호(파랑)

Wavelet이 어떤 신호의 근사치를 구할 수 있음에도 불구하고, 몇 개의 신호 종류는 근사치를 구하기 어렵다. Square wave나 급격하게 색이 변화하는 영역은 근사치를 구하기 어렵다. Square wave에서 평평한 부분은 빨리 근사치를 구할 수 있음에도 불구하고, 가파른 부분은 신호에 적절히 맞추려고 할 때 많은 wavelet이 필요할 수 있다. 비슷하게 linear transition은 단계적인 square wave로 근사치를 구할 수 있다. 추가적으로 극한의 값(검은색 또는 흰색)은 근사치를 구하기 어렵다. 하지만 wavelet으로 디지털 카메라로 찍힌 "자연적인" 색과 화려한 이미지의 근사치를 구하는 데는 매우 좋다.

디지털 사진의 경우, 사진은 신호이고 wavelet은 이미지의 근사치를 구한다. 800x600 픽셀의 이미지를 그리는데 각 color channel당 480,000 이상의 wavelet이 완벽하게 다시 사진을 그리는데 필요하다. 그러나 단지 적은 비율의 wavelet만 사용되면 사진의 주요 특성이 흐리더라도 보여진다. 더 많은 wavelet이 사용되면 이미지는 또렷해진다. 그리고 더 많은 wavelet은 색을 더 미세 조정한다.

이런 wavelet의 특징 - 흐린 것에서 색을 명확하게 하는 - 은 이미지 수정 여부를 확인하는데 사용될 수 있다. 특히 이미지 전체가 같은 비율로 또렷하게 될 수 있다. 만약 사진 특정 부분의 크기가 조정되거나 다른 초점으로부터 합쳐진 경우, 해당 부분은 다른 비율로 또렷하게 될 것이다.



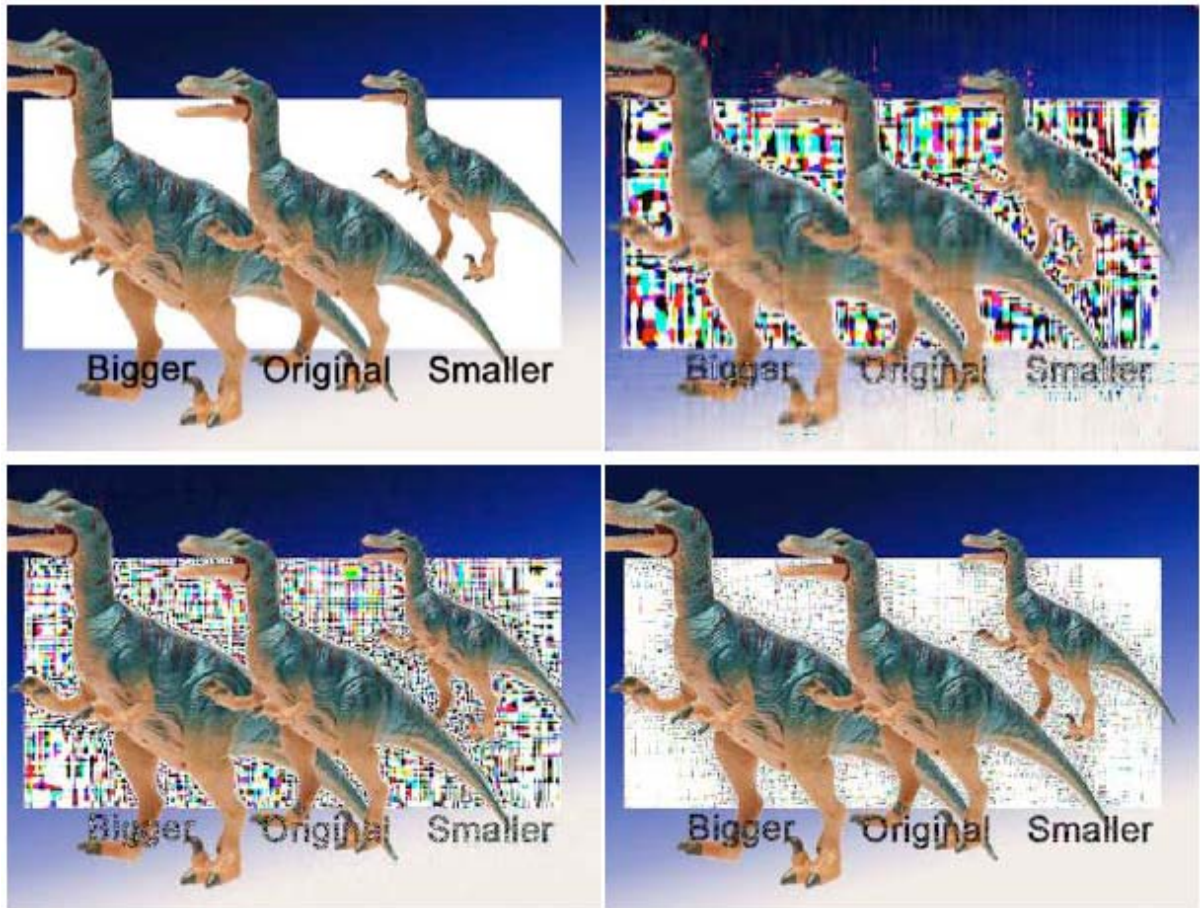


그림19) 크거나 작게된 공룡(좌측 상단), 1%의 wavelet으로 그린 것(우측 상단), 5%(좌측 하단), 20%(우측 하단)

그림19의 공룡 예제를 보자. 이 사진은 하나의 공룡 이미지이다<sup>10</sup>. Photoshop을 사용해서 이미지는 확대되거나 축소되었다. 1%로 그려진 wavelet에서 전체 이미지는 흐리게 나온다. 극단의 색(흰 배경과 검은 글자)은 적절히 그려지지 않는다. 2%에서 다른 곳은 흐린 데 비해 작은 공룡의 어깨와 엉덩이는 또렷해진다. 3%에서는 작은 공룡 전체가 또렷해진다 – 추가적인 wavelet은 색을 미세 조정하지만 또렷하지는 않다. 원래 크기의 공룡은 5%에서 또렷해지며 큰 공룡은 8%에서 또렷해진다. 8% 이상에서 추가적인 wavelet은 색을 미세 조정하지만 또렷하게는 하지 않는다.

#### 3-4-4. Wavelet 예: 힐러리

유명인이나 정치인은 자주 가상적인 상황에 photoshop된다. 그림20을 보자. 이 이미지는 이미지 수정 콘테스트의 한 부분으로 "redcard"에 의해 만들어졌다. 5%의 wavelet으로 이미지를 그린 것은 또렷한 몸과 또렷함이 약간 덜한 팔과 다리를 보여준다. 그러나 얼굴은 흐리게 보인다. 흐린 것은 턱 아래로는 사라진다. Wavelet 분석을 통해 머리 부분은 힐러리 클린턴 상원의원이고, 목과 몸통 부분은 다른 곳에서 왔으며, 팔과 다리는 또 다른 곳에서 온 것이라고 생각할 수 있다.

<sup>10</sup> <http://images.amazon.com/images/P/B00004L8M7.01.LZZZZZZZ.jpg>



그림20) 힐러리 클린턴 얼굴로 photoshop한 이미지(좌측), 5%의 wavelet을 이용한 이미지(우측)

### 3-5. 분석의 한계

이 글에서 논의한 방법은 이미지를 평가하는데 매우 강력한 도구를 제공한다. 하지만 이런 방법들은 모든 사진에 적용될 수 없고 분석 결과도 결정적이지 않을 수 있다. 예를 들어 매우 작은 이미지는 여러 분석 방법을 무효화할 수 있다. Wavelet은 각 방향마다 적어도 몇 백 개의 픽셀의 이미지를 필요로 하고(크면 더 좋음), 이미지 크기 조정은 ELA와 PCA가 제대로 되지 않도록 할 수 있다.

품질이 낮은 이미지는 JPEG 품질 설정이 매우 낮기 때문이거나 색 reduction(예, GIF) 때문에 대부분의 분석 방법을 방해할 수 있다. 게다가 이미지가 저장된 곳을 바꾸는 것(media transition)은 이미지에 영향을 미칠 수 있다. 사진을 스캐닝하는 것, 즉, 잡지 사진을 JPEG으로 바꾸거나 TV 신호를 캡처하는 것은 변환 과정에서의 artifacts를 야기할 수 있다.

더욱 복잡한 분석 시스템은 이미지 품질에 의존적이다. 예를 들어 급격한 명암 대비의 사진이나 잘 정의된 패턴은 ELA와 wavelet 결과를 혼동시킬 수 있다. Wavelet은 다른 신호 특징을 가지고 있는 두 사진들이 합쳐지는 harmonic convergences를 이끌 수 있고, 사진의 남은 부분을 통해 alternate rate을 resolving하는 변하지 않은 영역을 이끌 수 있다(섹션 4 참조).

많이 색을 바꾼(brightening, pallet skew 등) 이미지 역시 잘못된 결과를 야기할 수 있다. Re-coloring은 수정된 이미지(ELA)나 많은 layers(wavelet)를 구별할 수 없게 할 수 있다.



때때로 숙련된 사람은 이 모든 평가 방법을 통과할 수 있는 진짜 같은 사진을 만들 수 있다. 그러나 이런 실력의 사람은 정말 드물다. 진짜 같은 사진을 만들 수 있는 톨이 있음에도 이미지의 품질은 대부분 사용자에게 달려있다. 더 일반적인 경우에 품질을 향상시켰거나 CG 이미지는 이러한 평가 방법 중 하나 이상을 통과할지 모르나 모두를 통과하기는 힘들다.

#### 4. 예: 군인 사진

수정된 이미지는 큰 염려 없이 온라인 포럼이나 텔레비전, 영화, 광고에 자주 등장한다. 그러나 이런 이미지들이 언론 등에 나타날 때 문제가 존재한다. 왜냐하면 뉴스 출처는 사실로부터 나온 것일 의무가 있는데 품질이 향상되거나 수정된 이미지는 쉽게 실제 상황을 잘못 전하거나 독자들을 오해하게 할 수 있다.

2003년도에 사진 작가 Brian Walski는 바스라에서의 영국 군인의 사진을 신문에 제출했다. 이 사진은 군중 속의 사람들이 복사되어있는 것을 알아챈 편집자에 의해 가짜임이 드러났다 – Walski는 Los Angeles Times에서 해고당했다<sup>11</sup>. 이 사진은 다른 두 개의 Walski 사진으로부터 합성되었다고 널리 믿어지게 되었다(그림21).



그림21) 첫 번째와 두 번째 원본 사진(상단)은 합쳐져 좌측 하단의 허위 사진을 만들었다. 우측 하단 사진은 Gimp를 사용하여 원본들을 겹쳐 허위 사진을 만들려고 시도한 것이다.

<sup>11</sup> [http://blog.wired.com/wiredphotos54/2007/05/double\\_vision\\_i.html](http://blog.wired.com/wiredphotos54/2007/05/double_vision_i.html)



두 개의 원본 사진은 합쳐져 허위 사진을 만들 수 있고, 또한 어떻게 만들어졌는지 알게 해 준다. 이미지를 관찰해보면 허위 사진의 주요 부분이 첫 번째 원본 사진에서부터 왔다고 알 수 있다 - 군인 오른쪽에 위치한 모든 것은 그대로 존재한다. 두 번째 원본 사진은 잘려져 군인과 그 왼쪽에 위치한 사람들만 남겨졌다. 두 번째 원본 사진은 크게 확대되어 첫 번째 사진과 합성되었다. 마침내 합성 부분이 다시 색칠해졌고 하늘도 수정되었다.

그러나 원본의 출처는 보통 알려지지 않는다. 이 문서에서 다른 방법들을 이용하여 가짜 이미지는 원본 이미지 없이 분석될 수 있다(그림22).

- 관찰 : 합쳐진 사진에서 쪼그리고 앉아있는 흰 옷의 사람(군인 다리 뒤에 왼쪽 아래 부분)은 군인의 무릎 앞에 위치한 사람을 복사한 것이다. 그러나 복사한 것이 동일하지 않다; 하나 또는 둘 다 크기가 조정된 것으로 보인다.
- Meta 정보 : JPEG은 카메라 정보를 포함하지 않는다. 그러나 Adobe 툴을 이용해서 편집되었다면 Adobe에 관한 meta 데이터를 포함한다.
- Quantization Table 분석 : quantization matrix는 알려져 있지 않지만, 품질은 거의 72%이다.
- ELA : Error level 분석을 통해 하늘은 one error level이지만 모든 사람들은 다른 error level이라는 것을 알 수 있다. 이것은 이미지 re-coloring 때문이지만 ELA는 오직 "a" 변화만 확인한다.
- PCA : PC1은 하늘이 여러 번 다시 저장되었음을 보여준다. 군인과 그 왼쪽의 사람들은 fuzzy artifact halo에 의해 나타나진 것처럼 몇 번 저장되었다. 군인의 다른 사람들은 여러 번 저장되지 않았다. PC1은 이미지를 세가지 영역으로 축약한다; 하늘, 군인과 그 왼쪽에 위치한 사람들, 군인 오른쪽의 사람들.
- Wavelets : 8%의 wavelet에서 군인은 명확하게 보이지만 급격하게 색이 변하는 많은 영역이 있다. 이는 그의 이미지가 사진에 맞게 크기가 조정되었다는 것을 말한다. 격자무늬의 셔츠를 입은 사람(오른쪽 구석)은 명확하게 얼굴이 보인다; 대략 2%의 wavelet으로 resolve되었다. 그러나 그 뒤에 흰 옷을 입은 사람과 그 앞의 어린이는 얼굴이 흐리고 세가지 다른 층이 있다. Full wavelet 분석을 통해 사람들이 9개의 다른 층을 구성한다고 볼 수 있다.

ELA, PCA, 확인된 복사, wavelet의 다른 비율을 통해 이미지가 수정되었음이 분명하다. 그러나 수정의 자세한 사항은 결정적으로 알 수 없다. 상당한 re-coloring, 작은 크기, 낮은 해상도는 분석에 있어서 긍정 오류(false-positive)를 증가시킨다. 만약 이러한 문제들이 무시된다면 사진은 이미지를 형성하기 위해 합쳐진 11개나 그 이상의 다른 층을 포함한다고 볼 수 있다. 그러나 이 이미지는 상당히 수정되었다. 분석을 통해 이미지가 세 가지 층 정도를 포함한다고 알 수 있다: 군인과 그의 왼쪽에 위치한 사람들, 군인의 오른쪽에 땅과 사람들, 하늘.

분석에서 가장 큰 불일치(inconsistency)는 PCA와 wavelet 분석에서 보인다(다른 사진에 있어서는 다른 분석 방법이 불일치한 결과를 야기할 수 있다). 이런 경우에 wavelet 분석은 격자 무늬 셔츠를 입은 사람이 빨리 resolve하는 것을 보여준다. 이는 수정 때문이 아니라 frequency harmonic

때문이다. 특히 원본 이미지들에서 격자 무늬의 사람이 불규칙하게 보이지 않지만, 다시 만들려는 시도(그림22)는 동일한 wavelet 특징을 보여준다.

Cynthia Baron은 harmonic convergence 영역을 확인하기 위해 다음을 제안했다. Wavelet 분석은 대칭적인 이미지 크기를 사용하고(예, 512x512 또는 1024x1024) 다른 방향 전에 한 방향을 먼저 처리(예, 수직 방향 하기 전 수평 방향 먼저)한다. Wavelet 분석을 하기 전에 이미지를 회전하는 것은 harmonic convergence의 위치를 옮기거나 없앨 수 있다. 이런 경우 가짜 이미지를 회전하는 것은 격자 무늬 셔츠의 또렷함을 없애고 그 사람 얼굴의 또렷함 역시 감소시킨다.



그림22) Brian Walski에 의해 수정된 사진(좌측 상단), 95% ELA(우측 상단), 명암을 향상시킨 PCA(좌측 하단), wavelet 8% 사용

##### 5. 예: Dr. Ayman al Zawahiri

As-Sahab은 알 카에다의 비디오 제작 지부이다. 그들은 주기적으로 사람들에게 알 카에다의 존재, 이슈에 대한 위협, 인원 모집과 잠재적으로 흩어져 있는 테러리스트들에게 명령을 내리는 숨겨진 통신망(covert channel)을 위한 비디오를 배포한다. As-Sahab에 의해 만들어진 많은 비디오들은 수정된 것으로 보인다.

2006년 12월 20일 Ayman al Zawahiri 박사(알 카에다 서열 2번째)의 비디오를 배포했다. USA

Today는 비디오 배포를 헤드라인으로 다루었다(그림23)<sup>12</sup>. 비디오에 대해 USA Today는 “그는 검은 색 터번을 썼고 흰 옷을 입었다...그는 오른쪽 어깨 뒤로 평범한 갈색 벽에 기댄 라이플 총을 가지고 있었다”고 묘사했다. 이는 As-Sahab 비디오에 대한 설득력 있는 묘사임에도 USA Today에 사용된 사진은 그 이미지가 아니었다. 대신에 USA Today는 2006년 9월 28일의 다른 비디오의 사진을 사용했다. 이것은 낱자 라벨을 잘못 붙인 이미지에 대한 예이다.

USA Today가 사용한 사진은 많은 다른 흥미로운 특징들을 포함한다. 첫 번째는 IntelCenter ([www.intelcenter.com](http://www.intelcenter.com) – 테러리스트 활동을 쫓는 조직)에 있다. IntelCenter는 비디오의 우측 상단에 그들의 로고를 넣는다. 그러나 회사 이름은 명확하게 잘려져 있다 – USA Today와 같이. 실제 비디오에서의 같은 프레임을 비교해보면 육안으로 많은 다른 점이 보인다. 특히 IntelCenter는 사진의 색과 선명도를 조정했다(그림24).



그림23) USA Today가 잘못된 사진과 함께 게재한 비디오 배포 관련 뉴스와  
정확한 비디오에서부터 가져온 프레임

<sup>12</sup> [http://www.usatoday.com/news/world/2006-12-20-al-qaeda-palestinians\\_x.htm](http://www.usatoday.com/news/world/2006-12-20-al-qaeda-palestinians_x.htm)



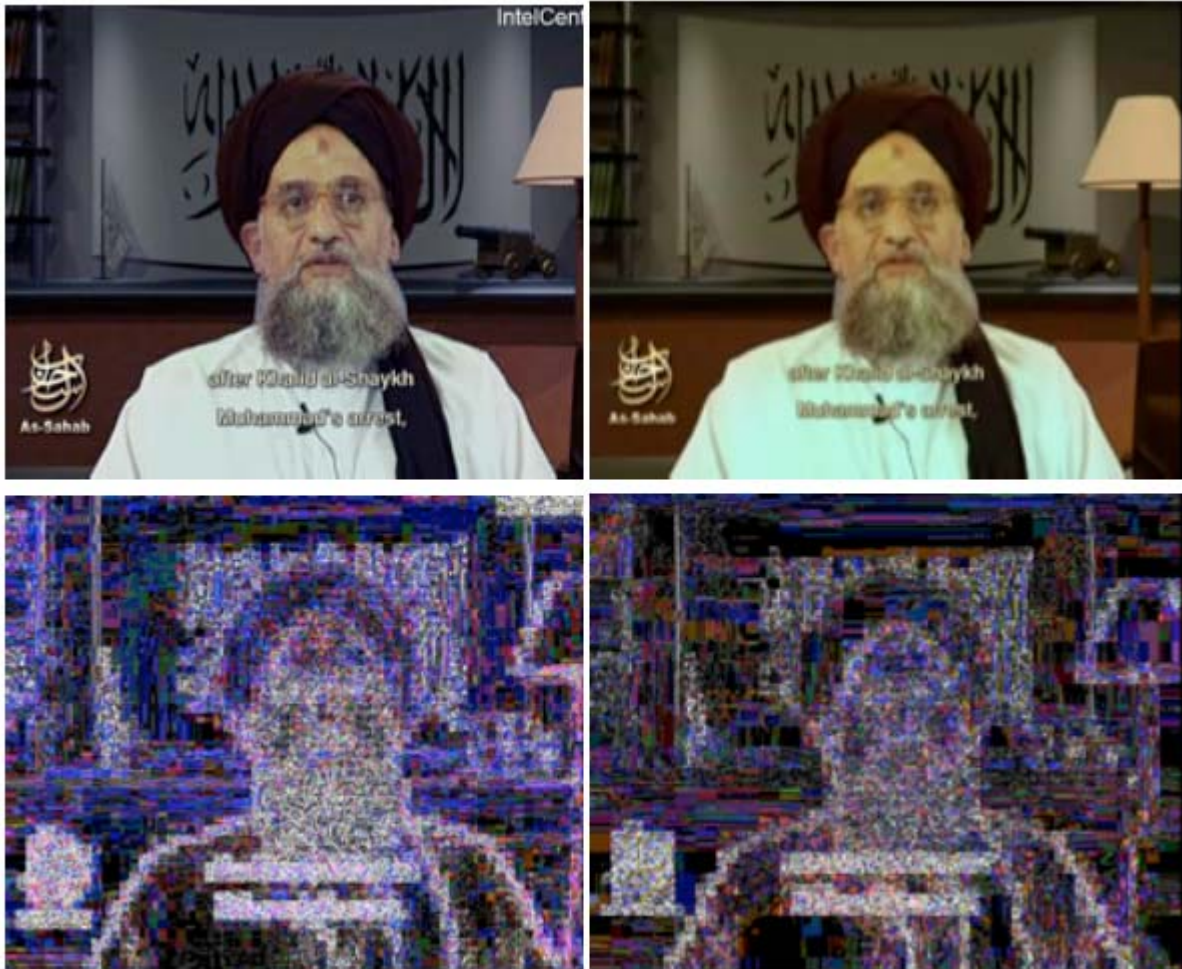


그림24) IntelCenter에 의해 제공되고 USA Today에 게재된 이미지(좌측 상단)와 실제 비디오에서 가져온 프레임(우측 상단). 하단은 각 이미지의 95% ELA를 나타냄.

95% ELA를 통해 관찰해보면 수정의 순서를 볼 수 있다. 가장 최근에 한 것부터 수정 사항을 살펴 보면:

- 잘려짐(Cropped): 마지막 수정은 이미지가 잘려진 것이다.
- IntelCenter: IntelCenter가 로고를 추가했다.
- Recolored: 이미지에 error rate을 수정하면서 re-coloring했고 선명도가 높아졌다.
- As-Sahab : As-Sahab 로고와 작은 표제가 추가되었다.
- Al Zawahiri : Zawahiri가 사진에 추가되었다. ELA는 명확하게 그와 배경간의 분명한 error level의 변화를 보여준다. 이런 error-level 후광(halo)의 종류는 chroma-key(녹색 스크린) 이미지에 있어 일반적이다. 특히 chroma-key 교체에 의해 생성된 눈에 띄는 error level 특징이 있다: 대부분의 chroma-key 교체 알고리즘은 채도나 밝기가 아닌 색조에 바탕을 두기 때문에 붙인 곳을 따라 다른 색 channel은 다른 error level을 가진다.
- 현수막(Banner) : 비어있는 sign에 문자가 추가될 수 있듯이(Section 2.2), Zawahiri 뒤 현수막에 어떤 사람이 문자를 추가했다.

이 이미지에 대한 PC1과 wavelet 분석은 이런 발견점을 뒷받침해준다. 배경의 사무실은 여러 번 저장된 하나의 층으로 보인다. 현수막의 글자는 Zawahiri가 추가될 때 동시에 추가된 것이며, As-

Sahab 로고와 작은 표제는 마지막으로 추가되었다.

### 5-1. 다른 Al Zawahiri 비디오

2006년 9월 28일의 비디오만이 조작된 것은 아니었다. 사실 al Zawahiri가 나온 비디오는 chroma-key masking에 확실하게 테스트된다. 2006년 7월 27일에 나온 비디오를 보자<sup>13</sup>(그림25). 이 비디오에서 al Zawahiri는 비디오 스튜디오에 앉아있다.

이 비디오가 나왔을 때, 많은 미국인들은 정부에 대해 매우 분노했다. 주된 원인은 하나의 주장에서 나왔다: al Zawahiri가 비디오를 만드는 스튜디오에 앉아있다면, 왜 그를 잡지 못하는가? 정답은 간단하다. 그는 스튜디오 안에 없다.

- 관찰: 스튜디오의 배경을 보면 발판 위에 반사가 보인다. 그러나 그 밑에 그림자가 없다.
- ELA: 95%의 ELA로 보았을 때 Zawahiri 근처에 chroma-key 후광(halo)이 보인다. As-Sahab 로고가 마지막에 추가되었다. 배경에는 단색의 반복적인 패턴이 보인다. 디지털 카메라로 찍으면 이미지에 노이즈가 발생하기 때문에, 단색은 디지털 카메라로부터 찍은 것이 아니다; 배경은 그려졌다.
- PCA PC1: PC1으로부터 만들어진 선은 배경이 반복적으로 저장되었고, Zawahiri 뒤의 3개의 사진은 각기 다른 resave level을 가지고, Zawahiri도 다른 level을 가진다. As-Sahab 로고는 JPEG artifacts를 가지지 않는다. 이는 사진이 적어도 6개 layer를 사용해서 만들어진 것임을 말해준다.
- PCA PC3: 첫 번째 principal component의 평면뿐만 아니라 세 번째 principal component의 선까지의 거리는 방의 조명을 강조한다. Zawahiri와 배경에 큰 동그란 모양의 조명이 관찰된다. Zawahiri 뒤의 밝은 지역은 그에게 비친 것보다 약간 더 넓기 때문에, 배경화면은 그에게서부터 1~2피트 이내 이다. 조명은 사진 속의 커다란 스튜디오와는 상반된다.
- Wavelets: 5%에서 wavelet은 6개의 구분되는 layer를 볼 수 있다. Mohammad Alef(배경 왼쪽)은 매우 흐리고, World Trade Center도 흐리고, Mohammad Atta(배경 오른쪽)는 거의 또렷하고, As-Sahab 로고는 색깔과 더불어 매우 또렷하다.

배경은 그린 것으로 보이고, 다른 사진은 추가된 것에 대해 의문점이 생긴다: 다른 이미지는 어디서 온 것인가? Mohammad Atta의 사진(배경 오른쪽)은 9/11 위원회의 최종 보고서<sup>14</sup>에 있는 사진을 사용한 것으로 보인다. 이 이미지는 크기가 줄어들었고 배경에 맞추기 위해 비뚤어졌다. 제작자는 아래 구석에 있는 정부 태그를 삭제했다. Mohammad Alef(배경 왼쪽)의 이미지는 그의 딸과 오사마 빈 라덴 아들의 결혼식 비디오에서 온 것으로 보인다.

---

<sup>13</sup> [www.archive.org/details/Crusaders-and-Zoinism-war-on-Gaza-and-Lebnon](http://www.archive.org/details/Crusaders-and-Zoinism-war-on-Gaza-and-Lebnon)

<sup>14</sup> [www.rcfp.org/moussaoui/jpg/size600/GX00004.2-1.jpg](http://www.rcfp.org/moussaoui/jpg/size600/GX00004.2-1.jpg)

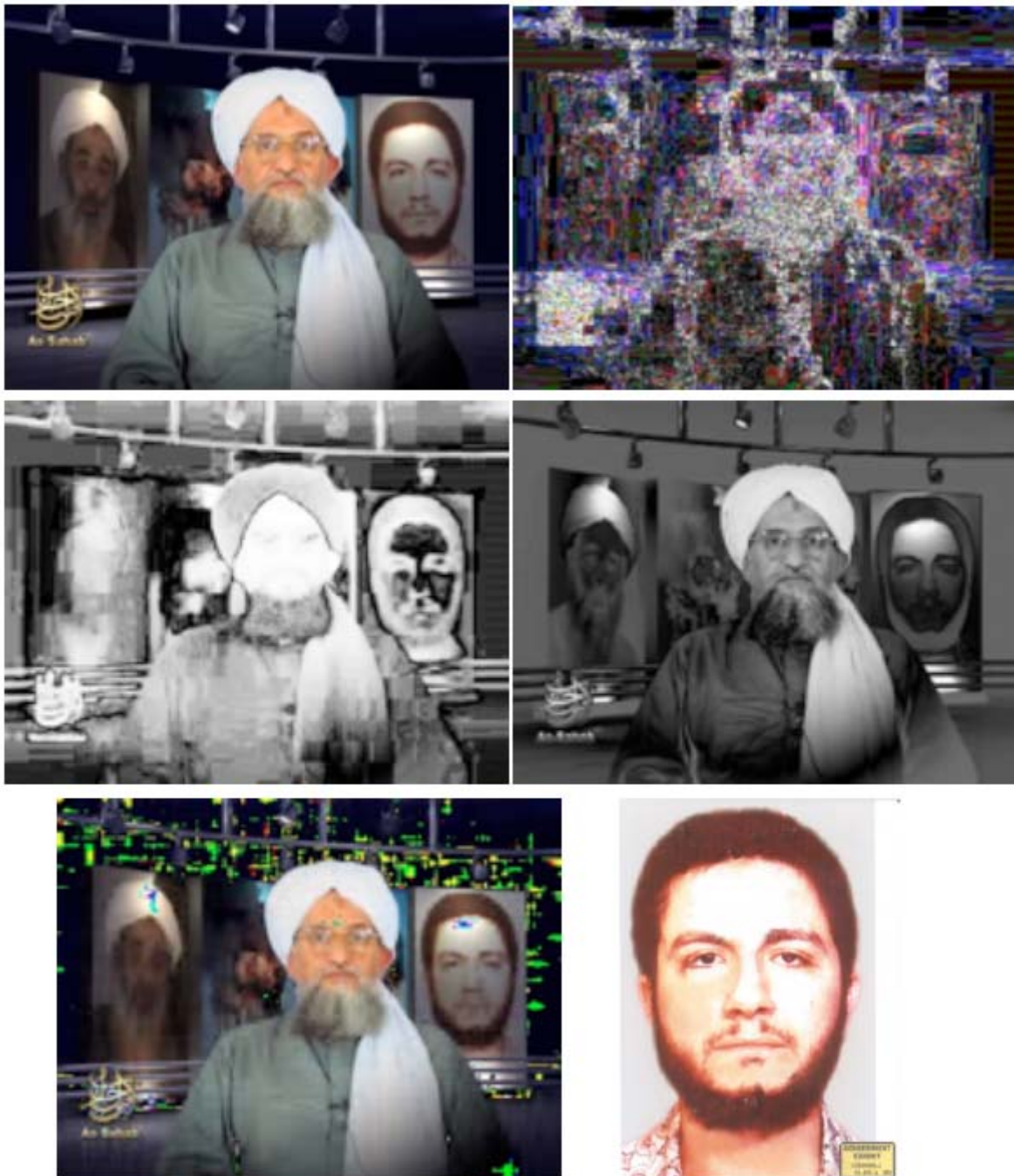


그림25) (위에서부터) 2006년 9월 28일 비디오에서의 스틸 프레임,  
95% ELA, PC1, PC3, 5% wavelets, 미 정부의 9/11 리포트에서의 Mohammad Atta 사진

## 5-2. 검은 배경

Chroma-key 배경이 있다는 주장은 실제로 보는 것과 같지 않다. 2007년 1월 22일, SITE Institute([www.siteinstitute.org](http://www.siteinstitute.org))-테러리스트 활동을 추적하는 기관-는 알 카에다 비디오가 공개적으로 발표되기 전에 가로챘다고 발표했다; SITE는 이를 발표했다. 3일 후 As-Sahab 역시 비디오를 발



표했다<sup>15</sup>.

비디오(그림26)에서 보면 al Zawahiri가 검은 커튼 앞에 있다는 것을 볼 수 있다. 카메라가 보기에 커튼이 적절하게 가운데 위치하지 않았다-오른쪽 상단 구석에 실제 배경에서는 뾰족 모양의 물건이 있다. 이미지의 밝기를 변화하면 커튼이 bar에서부터 걸쳐져 있다. 평범한 검은색 천이면서 균일한 색조를 가진다. 천은 'chroma-key sheet'라고 불리는 chroma-key 배경 종류라고 할 수 있다. 보통 chroma-key 배경은 고르지 않은 조명을 야기시킬 수 있는 것을 줄인다. 그러나 chroma-key sheet는 metal frame에 걸려있고(그림27), suspension fold를 보여준다.



그림26) 2005년 1월 25일 As-Sahab 비디오 프레임(왼쪽), color enhanced(오른쪽)



그림27) Chroma-key sheet

### 5-3. 다른 알 카에다 비디오

Al Zawahiri 비디오만 단지 변조된 As-Sahab 비디오는 아니다. 2006년 9월 2일 azzam al-Amriki(Azzam은 Adam Gadahn라고 또한 알려져 있다)가 비디오에 나왔다(그림28). 비디오에는 하얀 방에 책상, 컴퓨터, 몇 권의 책과 함께 그가 나온다. 그러나 95% ELA에서 보면 책은 방에 존재하지 않는다. 컴퓨터, 벽, 책상, Azzam은 하나의 error level을 가지는 반면에 책, 부제, As-Sahab 로고는 다른 error level이 나타난다. PC1은 책의 색상 범위가 이미지의 남은 부분이 다른 곳에서부터 와서 그런지 매우 다르다.

<sup>15</sup> [www.archive.org/details/Correct-Equation](http://www.archive.org/details/Correct-Equation)

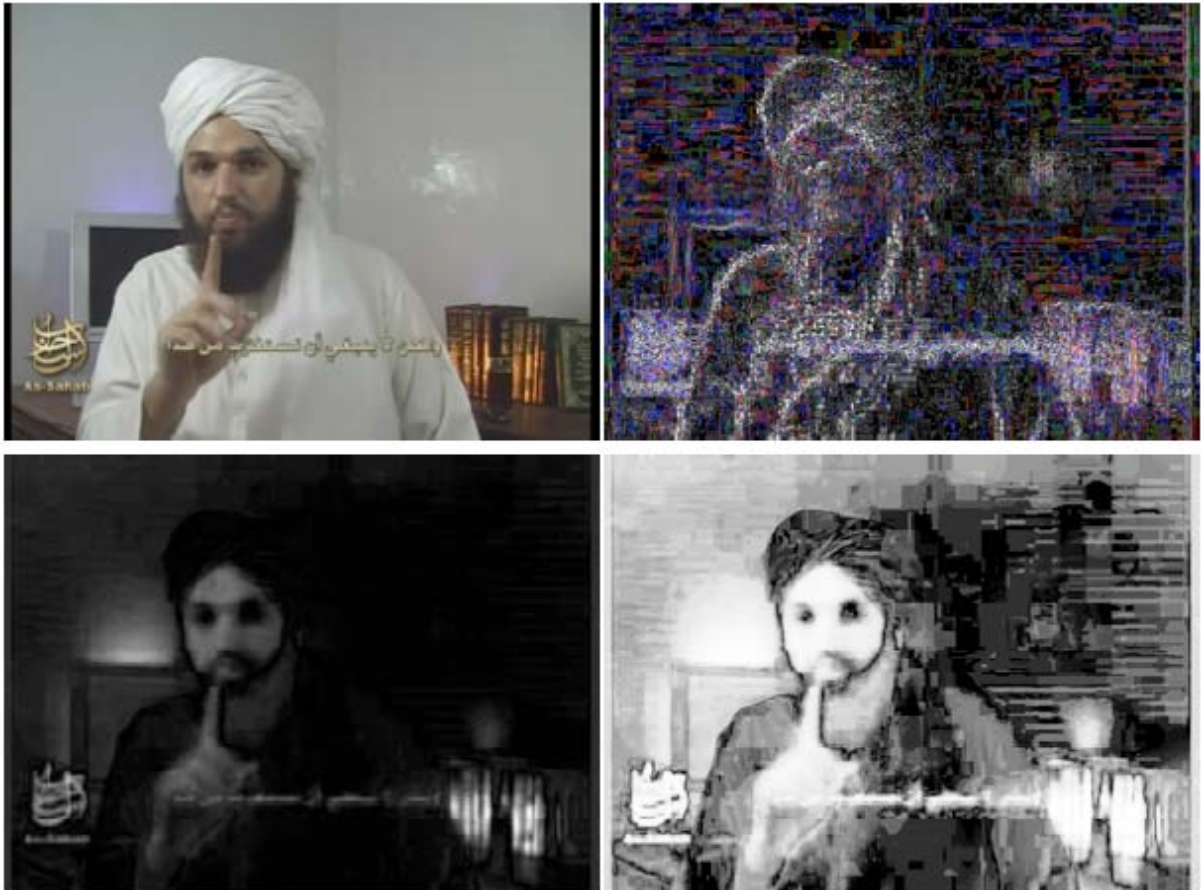


그림28) 2006년 9월 2일 비디오의 Azzam al-Amriki(좌측 상단), 95% ELA(우측 상단), PC1(좌측 하단), enhanced 명암 PC1(우측 하단)

조정된 명암의 PC1(그림28 우측 하단)은 수평 선 패턴을 보여준다. 이는 media artifact이다; Azzam의 원본 비디오는 첫 번째 principal component에 의해 확인된 여러 비디오가 조합된 것을 사용했다. 그러나 수평 선은 배경에서 잘 보이고 Azzam에게는 다소 부드럽게 보이는 반면에, 책이나 As-Sahab 로고에는 보이지 않는다. 이는 이미지들이 조합된 비디오에서부터 온 것이 아님을 말해준다.

Al-Amriki 비디오에서 사용된 색의 흩뿌려진 plot은 3개의 구분된 색 구역(그림29)을 보여준다. 주요 색이 밀집된 구역은 사진의 대부분에 나타나는 색을 포함한다: Azzam, 벽, 책상, 컴퓨터. Plot의 가운데 작은 끝은 As-Sahab 로고와 부제에서 볼 수 있는 색으로 구성되어 있다. 이런 색은 이미 여러 군데서 보이지 않고 독립적인 클러스터를 형성한다. 주 이미지 스펙트럼의 밖에는 책에서 볼 수 있는 색이 있다. 책의 색 스펙트럼은 이미지의 주 색과는 구분된다. 이는 책이 al-Amriki와 같지 않음을 말해준다.

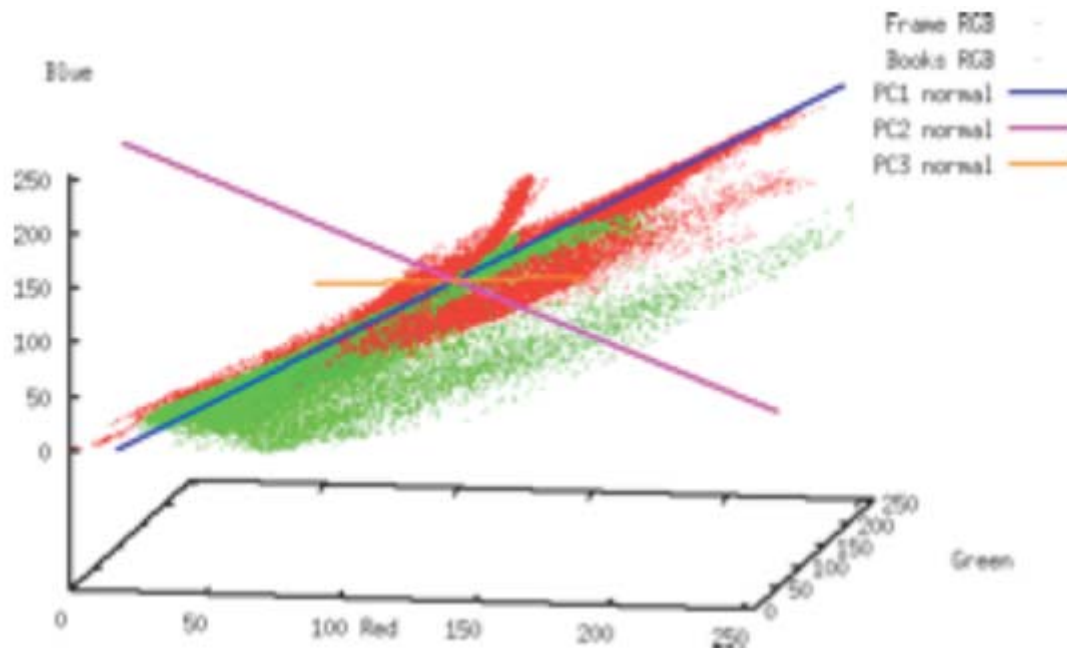


그림29) Azzam al-Amriki 비디오 프레임의 scatter plot. 책의 색깔은 초록색이다.

## 6. 추가 연구 사항

이 글에서 다룬 접근법들은 Hacker Factor Solutions와 일반적인 분야에서 진행중인 작업이다. 디지털 이미지 기술들이 발전함에 따라 조작이나 실제와의 차이점을 탐지하는 방법도 발전한다. 이는 완전히 새로운 분야이며 대부분의 연구자들은 다른(그러나 연관된) 기술을 가지고 일하고 있다. 연구 프로젝트 예제를 보면,

- Hany Farid(Dartmouth College): 이미지 수정 탐지
- Jessica Fridrich(Binghamton University): 스테가노그래피와 변경 탐지
- Shih-Fu Chang(Columbia University): 신호 처리와 통계 패턴 인식을 이용한 Media 포렌식
- Nasir Memon(Polytechnic University): 이미지 스테가노그래피와 수정 탐지
- Min Wu(University of Maryland): 디지털 media fingerprinting

추가적으로 로봇틱 비전과 같은 분야도 포렌식 이미지 분석에 활용할 수 있게 발전 중인 기술이다.

## 7. 결론

주장의 영향력을 크게 하기 위해 사진이 수정되는 것을 고려하면, 이미지 분석과 디지털 포렌식은 중요성이 커지고 있다고 할 수 있다. 이 문서는 이미지를 보고 분석하는 여러 방법을 다루었다. 하나의 이미지는 하나 또는 두 개의 테스트를 통과할 수도 있지만, 수정된 이미지는 모든 테스트를 통과할 수 없다. 추가적으로 이러한 방법들은 가능한 분석 방법의 시작에 불과하다. 다른 방법들도 존재하며 다른 이미지 수정 기술을 탐지하기 위해 기획되었다.