

# تجزیه و تحلیل جرایم تصاویر دیجیتالی و فتوشاپ

مرتضی اکبری کارشناس ارشد شیمی پلیمر دانشگاه تهران

تاریخ دریافت: ۸۸/۷/۲۴ تاریخ پذیرش: ۸۸/۹/۲۳

از صفحه ۶ تا ۳۱

## چکیده

امروزه از تصاویر دیجیتال به طور وسیعی در جوامع استفاده می‌شود. با توسعه فناوری تصاویر دیجیتال، نرم‌افزارهایی نیز برای ویرایش و اصلاح تصاویر خلق شده‌اند. متأسفانه گاهی اوقات استفاده از این نرم‌افزارها وسوسه‌آمیز است و سبب ایجاد مشکلاتی برای جامعه می‌شود، برای مثال ایجاد تغییرات ناپسند در عکس افراد مورد نظر و اخاذی کردن از آنها یکی از این موارد است. در این میان نرم‌افزار فتوشاپ نقش مهمی را هم برای کارآگاهان و هم برای تبه‌کاران ایفا می‌کند. در این مقاله استفاده از این نرم‌افزار برای جعل سازی و همچنین برای کشف جرم توسط کارآگاهان، و نیز کاربرد فتوشاپ در بهینه‌سازی اثر انگشت در انگشت‌نگاری نشان داده شده است. با توجه به رشد فزاینده دوربین‌های دیجیتال و نرم‌افزارهایی مثل فتوشاپ در کشور، به نظر می‌رسد جرایم تصاویر دیجیتال یکی از دغدغه‌های مقامات ذیربط باشد.

کلیدواژه‌ها: فتوشاپ، جرایم دیجیتالی، تصاویر دیجیتال، جعل، کاربرد جنایی

کارگاه

دوره دوم  
سال دوم  
پاییز ۸۸  
شماره ۸

## مقدمه

نرم افزار ویرایش تصاویر به سرعت در حال تبدیل شدن به یکی از ابزارهای عمومی رایانه مانند مجموعه آفیس است. مهم نیست که چه نوع سند رسمی توسط این نرم افزار تغییر می یابد - از پول گرفته تا کارت شناسایی و گواهینامه رانندگی - ولی در هر صورت جامعه ماست که متحمل ضرر می شود و اقتدار بدنه جامعه به مخاطره می افتد. همچنین در زمان مناسب، منجر به جعل موفق اسناد و پول می شود و مردم رفته رفته اعتمادشان را نسبت به سازمان ها و توانایی آنها برای ایجاد فرم های واقعی و اصلی مانند گواهینامه رانندگی یا کارت شناسایی از دست می دهند. در بدترین حالت، اقتصاد دچار گسیختگی می شود و منجر به فروپاشی دولت ها می شود.

با وجود این خطرات، جامعه ما میل آشکاری به جلوگیری از همه اشکال جعل اسناد، پول و ... دارد. هر وقت که تهدید جدیدی آشکار می شود، دولت ها و سازمان ها برای پیدا کردن جاعلان و خاتمه دادن به فعالیت آنان تلاش می کنند. به همین دلیل است که قرص های دارویی در بطری هایی وارد بازار می شوند که به آسانی قابل تقلید یا تغییر نیستند. کارت های اعتباری و پول ها هولوگرام دارند و ساخت بسته بندی هایی که تراشه هایی در اندازه نانو دارند رو به افزایش است.

متأسفانه همه قواعد و قوانین و مقررات، امنیت مطمئنی را در برابر جعل ایجاد نمی کنند و جعلیات اغلب موفق هستند، زیرا ما با نمونه واقعی آشنایی نداریم و هیچ وقت هم بدقت به آن نگاه نمی کنیم. برای لحظه ای تصور کنید که آیا می توانید یک اسکناس ۱۰۰۰۰ ریالی جعلی را از اسکناس واقعی تشخیص دهید؟ یا اینکه آیا می توانید اسکناس یورو یا دلار جعلی را تشخیص دهید؟ اگر شما فکر می کنید که نمی توانید، مطمئن باشید که تنها نیستید. اسکناس های نامناسب زیادی در بازارهای بین المللی رد و بدل می شوند، و این هنگامی اتفاق می افتد که افراد با پول رایج خارجی (ارز) آشنایی ندارند.

بدتر از آن این است که اسناد جعل شده ای که در معرض دید عموم قرار می گیرند، اگر در یک نگاه ساده رسمی به نظر برسند پذیرفته خواهند شد. هدف هایی که مورد کلاهبرداری

قرار می‌گیرند، متوجه نیستند که ویرایش یک سند واقعی یا خلق سند جعلی چه اندازه آسان است. متأسفانه، حتی وقتی که سندی جعلی در معرض دید گذاشته می‌شود، هیچ تضمینی برای وجود جعلیات مشابه نخواهد بود. وقتی کلاهبرداری عموم جامعه را در بر گیرد، این کلاهبرداری کم‌رنگ‌تر می‌شود و افراد جدیدی ممکن است مورد هدف قرار بگیرند. اگر کلاهبرداری در مورد سند چاپ شده باشد، هنرمند کلاهبردار می‌تواند به محل جدیدی برای کلاهبرداری نقل مکان کند و یا هویت جدیدی را قبول کند. اگر کلاهبرداری در اینترنت باشد، ممکن است قلمروی جدیدی با نام مالک و نشانی جدید به صورت آنی ایجاد و اداره شود.

### جعل اسکناس

از همه اشکال جعل سازی وابسته به فتوشاپ، جعل پول یکی از جدی‌ترین و وسوسه‌انگیزترین آنهاست. امروزه عجیب به نظر می‌رسد، اما تا اواخر قرن ۱۹ میلادی بسیاری از کشورها پول رایج کشور خودشان را چاپ نمی‌کردند. در ایالات متحده تا زمان جنگ داخلی، پول توسط بانک‌ها و ایالت‌های مشخص چاپ می‌شد، هیچ عقیده ثابتی روی اسکناس وجود نداشت و هر اسکناس متفاوت طراحی می‌شد که این باعث می‌شد هر کسی ب راحتی پول چاپ کرده و آن را منتشر کند (شکل ۱).



شکل ۱: هر کدام از این اسکناس‌ها قبل از سال ۱۸۶۲ در ایالات متحده قانونی بودند. توجه داشته باشید که هیچ کدام از اسکناس‌ها سبز رنگ نیستند.

در انتهای جنگ پر واضح بود که کاری باید در این مورد صورت گیرد. دولت، ناامیدانه برای مهار کردن نظام مالی و خنثی کردن جعل سازی متداول، سرویس مخفی را بنا نهاد. از آن زمان تا آغاز عصر رایانه، برای ورود به عرصه جعل پول موانع نسبتاً عظیمی وجود داشت. دستگاه‌های چاپ، پر سر و صدا و اجسام بزرگ بدقواره فلزی وجود داشتند. برای ایجاد یا تغییر یک صفحه چاپ، نیاز به یک گراور ساز، آهنگر تعلیم دیده با مهارت هنرمندی، صبر و حوصله و چشمی برای دیدن جزییات بود. توافق‌های بین مؤسسات به محققان دولت اجازه می‌دهد که فهرست عاملان جرایم سازمان یافته و گروه‌های چاپ مستقل پول را محدود کنند.

در مقابل، چند دهه گذشته برای جاعلان اسناد و نوشته‌ها سودمند بوده است. با ورود فناوری کپی رنگی، اسکنر و نرم افزار ویرایش تصاویر، هر فردی با مقدار کمی پول برای سرمایه گذاری،

صبر و حوصله و تمایل به دزدی می تواند ضرابخانه‌ای ایجاد کند.

ایالات متحده در مورد کاغذهای مخصوص چاپ پول دقت زیادی به خرج داده است و در مجاب کردن مردم به تشخیص اسکناس‌های واقعی از جعلی با تمرکز روی این قسمت برجسته و بی نظیر نسبتاً موفق بوده است. پول رایج ایالات متحده دارای نخ‌های رنگی است که داخل آن جا داده شده‌اند و شکل مشخصی دارند که بیشتر کاغذهای رایج با آن همخوانی ندارند. متأسفانه، یکی از حقه‌های کنونی موجود در دنیا برای جعل پول، استفاده کردن از مواد شیمیایی برای از بین بردن رنگ اسکناس‌های کم ارزشتر مثل یک و پنج دلاری و سپس چاپ یک اسکناس ۵۰ یا ۱۰۰ دلاری روی کاغذ اسکناس سفید شده است. در این صورت اسکناس واقعی به نظر می‌رسد زیرا کاغذ آن اصل است (Douglas, K.S. et al. ۲۷: ۱۹۹۷).

#### واکنش صنف تولید کنندگان نرم افزار ویرایش تصویر

شرکت‌هایی مثل ادوبی که محصول‌های تولیدیشان ممکن است برای جعل سازی مورد استفاده قرار گیرد به درخواست دولت برای ایجاد تغییراتی در نرم افزارهایشان لبیک گفته‌اند و تغییراتی را برای اصلاح بیشتر طرح‌ها اعمال کرده‌اند. برخی کپی‌کننده‌های رنگی، قابلیت ردیابی و شناسایی تصویر اسکناس و ته نقش کپی شده در اسکناس را دارند. اگر شما سعی در کپی کردن پول داشته باشید نرم افزار خود به خود از محیط کار خارج می‌شود و نیاز به راه اندازی مجدد خواهد داشت. تکنسین دستگاه این تلاش برای کپی کردن پول را که در حافظه کپی‌گر ثبت شده است، گزارش می‌دهد (P. S. Hiremath et al. ۲۰۰۷).

در برخی نرم افزارهای ویرایش تصویر، سیستم ردیابی تعبیه شده است که اگر شما از یک اسکناس اسکن یا عکسبرداری کنید و آن را در نرم افزار ادوبی فتوشاپ CS یا نسخه‌های بالاتر از CS باز کنید، کادری روی صفحه ظاهر می‌شود و به شما هشدار می‌دهد که تصویر، مربوط به پول رایج است و شما را به سایتی متصل می‌کند که مهمترین قوانین پول رایج کشورهای مختلف در آن موجود است. (این شیوه مختص به فتوشاپ نیست، بلکه نرم افزارهای ویرایش

تصویر رقیب فتوشاپ، مثل پینت شاپ پرو<sup>۱</sup> هم این محدودیت‌ها را اعمال می‌کنند. در مورد اینکه، نرم افزار دقیقاً چه عملی را برای پول انجام می‌دهد کاملاً ثابت نیست و با توجه به نوع نسل CS که شما استفاده می‌کنید متغیر است (شکل ۲ و ۳).



شکل ۲: وقتی در حال کار کردن با فتوشاپ CS یا نسخه‌های بالاتر هستید، پیام‌های متفاوتی را دریافت خواهید کرد.



شکل ۳: هنگامی که همان فایل را در فتوشاپ CS باز می‌کنید، این پیام را دریافت خواهید کرد.

مربیان، طراحان و هنرمندان از تصاویر اسکناس‌ها به دلایل مختلفی استفاده می‌کنند، از تحقیق‌های مدرسه برای درس تاریخ پول گرفته تا مبارزه‌های انتخاباتی و طرح‌های مربوط به هنرهای زیبا از تصاویر اسکناس‌ها استفاده می‌شود. برای برآورده کردن نیاز این قشر، اداره

## 1. Paint Shop Pro

خزانه داری ایالات متحده تصاویری از اسکناس ها را برای دانلود فراهم کرده است (<http://www.moneyfactory.gov/newmoney>).

به نظر می‌رسد که دولت در حال رفع این مشکل است، ولی متأسفانه، این اقدامات پیشگیرانه بندرت دانش منطقی کاربر فتوشاپ را کم می‌کند و جاعل توانمند کار خود را انجام می‌دهد. فتوشاپ CS و CS2 را به آسانی می‌توان برای ویرایش اسکناس فریب داد. فایل را در ایمپج ریدی<sup>۱</sup> باز کنید و سپس از منوی File گزینه ویرایش در فتوشاپ را انتخاب کنید (شکل ۴). فتوشاپ براحتی فایل را باز می‌کند و به شما اجازه ویرایش و ذخیره آن را می‌دهد. وقتی که فایل را ذخیره کردید، فتوشاپ بعداً هم می‌تواند بدون هیچ مشکلی فایل را دوباره باز کرده و برای شما چاپ کند (Witkowski, Jill ۲۷۳: ۲۰۰۲).



شکل ۴: نسخه‌های CS تا CS3 فتوشاپ محتوای فایل وارد شده از ایمپج ریدی را برای اینکه اسکناس است یا نه بررسی نمی‌کنند.

ولی فتوشاپ CS3 اجازه چنین کاری را نمی‌دهد. اگر بخواهید می‌توانید تصویر اسکناس را در محیط ادوبی فایروورک<sup>۲</sup> باز کنید (در نسخه CS3 ایمپج ریدی از کار افتاده) و آن را چاپ کنید. اما اگر شما سعی کنید، عکس را بعد از اینکه به فرمت PSD ذخیره کردید چاپ کنید در فایروورک فتوشاپ هنوز هم قادر به تشخیص اسکناس است. با وجود این فتوشاپ CS3

1. Image Ready
2. Adobe Fireworks

تصویر اسکناسی را که قبلاً با ویرایش‌های قبلی فتوشاپ CS یا CS۲ ذخیره شده، باز نموده و چاپ خواهد کرد.

کار جعل کردن به زمان اولین سکه ساخته شده در قلمروی فرمانروایان برمی‌گردد، و تا زمان حال که کارت شناسایی جعلی هم جزء آن است ادامه دارد. در سرتاسر تاریخ تبهکاران و یاغیان برای گریختن از اسیر شدن، به شکلی اسناد را جعل می‌کردند. هم‌اکنون اکثر کشورها احتیاج دارند که در مورد هویت واقعی شهروندانشان و همچنین گردشگران خارجی اطلاعاتی کسب کنند. انتظار می‌رود هر فرد سندی را همراه داشته باشد که نشان دهد آنها چه کسانی هستند، کجا زندگی می‌کنند، سنشان چقدر است، حق و حقوقشان مشخص شود و موارد بسیاری دیگر مثل مهارت‌ها و حزب سیاسی آنها مشخص شود.

برای جوابگویی به این احتیاجات، کشورهای زیادی برای شهروندان خود کارت شناسایی صادر می‌کنند. ایالات متحده کارت شناسایی صادر نمی‌کند، زیرا آمریکاییان زیادی اعتقاد دارند که داشتن کارت شناسایی استاندارد به دولت قدرت زیادی برای دخالت در زندگی خصوصی افراد می‌دهد و این امر هیچ‌گاه توسعه پیدا نکرده است (Steven K et al, ۲۰۰۹).

به هر حال فقدان کارت مقبول و معتبر در دنیا مجموعه‌ای متفاوت از مدارک پلاستیکی را به وجود می‌آورد. گواهینامه‌های رانندگی، به صورت بالفعل کارت‌های شناسایی هستند، اما ۵۰ نوع مختلف از آن وجود دارد - در ایالات متحده هر ایالت یک نوع متفاوت گواهینامه رانندگی صادر می‌کند - با وجود این بسیاری از افراد اصلاً رانندگی نمی‌کنند و اطلاعات دیگری هم وجود دارد که دولت‌ها احتیاج به دانستن آنها دارند ولی در گواهینامه رانندگی وجود ندارد. برای به دست آوردن اطلاعات در موقعیت‌های متفاوت، کارت‌های ویزا، کارت سبزه و کارت امنیت اجتماعی وجود دارند که همه اینها برای اثبات محل اقامت، پرداخت مالیات و حق رأی دادن ضروری هستند. کارت‌های شناسایی برای احزاب و سازمان‌های خاص هم وجود دارد، مانند کارت‌های شناسایی سازمانی برای ورود اعضا به ساختمان سازمان، کارت دانشجویی، که به شما اجازه ورود به دانشگاه را می‌دهد و امکان استفاده از تخفیف‌های دانشجویی را فراهم می‌آورد و همچنین به عنوان کارت کتابخانه هم استفاده می‌شود.



پول و کارت شناسایی عمومی ترین اشکال اسناد رسمی هستند که شهروندان با آنها در ارتباط هستند، اما دولت ها، شرکت ها، ادارات دیگر و آژانس های بین المللی تولید دریایی از اوراق قانونی استفاده می کنند. مدرک تحصیلی، گواهینامه، تأییدیه تولد و مرگ، کاغذهای رهن و اجاره، وصیتنامه و حکم دادگاه و برگ ها و مدارک دیگری نیز وجود دارند که هر کدام از اینها می توانند مورد جعل قرار گیرند.

بهترین مدارک برای جاعلان اسناد رسمی از نوع اینترنتی است، زیرا هیچ نیازی به چاپ آنها و به دست مردم دادن نیست چون در این صورت ممکن است متوجه جعلی بودن آن بشوند، ولی آنها تنها یک کپی از فایل اصلی می گیرند و مقداری تغییر در آن می دهند. اینترنت آنقدر وسیع است که کنترل آن برای پلیس فوق العاده مشکل است و تقریباً پلیس هیچ وقت متوجه جعلیات نمی شود. کالاها به شکل روزمره از صندوق های اداره پست بارگیری می شود و پول هم با یک کلیک موشواره<sup>۱</sup> انتقال داده می شود. گاهی اوقات فضای وبی که به نظر بسیار دقیق می رسد، ممکن است شروعی برای کلاهبرداری باشد. با نسخه دزدیده شده ای از فتوشاپ مورد اعتماد، کلاهبرداری موفقیت آمیز دور از انتظار نیست.

عکس در موقعیت های نامناسب صحنه های جرم نیاز به ویرایش با استفاده از نرم افزار فتوشاپ دارند. تصاویر ممکن است نیاز به وضوح بیشتر یا اصلاح رنگ زمینه داشته باشند. در برخی از موارد هنگام ویرایش تصویر، ممکن است شخص اصلاح کننده برای انجام کمی تغییرات بیشتر وسوسه شود. تصمیم اشتباه ممکن است منجر به قضاوت نادرست در مورد عکس شود.

### کاربرد جنایی نرم افزارهای ویرایش تصویر

اولین گام برای گرفتن عکس های دیجیتالی که به عنوان مدرک نیز مورد قبول باشند، انجام فرایندی مناسب برای انتقال عکس دیجیتال از دوربین به دادگاه است، که مستلزم فرایند اجرایی استاندارد (SOP) است، چیزی که هر نیروی خوب پلیس باید آن را داشته باشد (A.).

1. Mouse

Swaminathan et al. (۲۰۰۷). SOP شیوه‌ای سریع برای سند کردن و ذخیره حالت عکس بعد از انتقال از دوربین است. ساده ترین راه این است که فردی را برای اداره این تصاویر ذخیره شده بگماریم نه اینکه هر عکاس پلیس خودش بخواد عکس‌ها را ذخیره و نگهداری کند. شخص منصوب شده باید فایل‌ها را مستقیماً روی CD یا DVD کپی کند و آنها را در جای امن ذخیره کند. گام دوم این است که عکس‌ها به فرد دیگری غیر از عکاس تحویل داده شود و او عکس‌های ناقص را اصلاح و ویرایش کند. البته این شخص نباید هیچ میل شخصی و تعصبی را در این کار دخیل نماید، زیرا ممکن است مدارک را به دلخواه خود تغییر دهد که حتی روی تصمیم قضات نیز اثر گذار باشد. نرم افزارهای مختلفی برای محافظت از ایجاد تغییرات احتمالی در عکس‌ها توسط کسانی که عکس‌ها را دیده‌اند، وجود دارد.

وقتی مطمئن هستید که مدارک برای پرونده‌ای جمع آوری شده، عکسبرداری صورت گرفته و اصلاح شده است، باید فکر کنید که تصاویر به شما چه می‌گویند. گاهی اوقات حدس زدن ساده و آسان است؛ تعداد زیادی اثر انگشت مشخص، مدارک قوی یا عکس‌های فوق العاده خوب از صحنه جرم که تمام داستان را بیان می‌کنند، ولی گاهی اوقات اطلاعات در عکس‌های گرفته شده درست جلوی چشمان ماست، اما ما توانایی دیدن آن را نداریم. برخلاف فیلم‌ها، اثرات انگشت به آسانی ردیابی نمی‌شوند. کارآگاهان چند نسل پیش، ابزار تصویرگری محدودی در اختیار داشتند. چشم و ذهن ما براحتی قادر نخواهند بود تمام اطلاعاتی را که توسط یک عکس فراهم شده است پردازش کنند، بنابراین ما به کمک نیاز داریم. البته این کمک را براحتی نمی‌توان قبول کرد. اصلی ترین چالش برای مدارک ویرایش شده این است که بیشتر به صورت احساسی با آنها برخورد می‌شود تا منطقی. شما به عکس‌های «واقعی» نگاه می‌کنید و چیز خاصی نمی‌بینید، ولی وقتی به تصاویری که از لحاظ کیفی اصلاح شده‌اند می‌نگرید، ناگهان همه چیز آشکار می‌شود. قبل از اعمال تغییرات در تصاویر، جریان رسیدگی طولانی تری در مورد پرونده‌ها باید طی شود، ولی ما در عصر طلایی دسترسی به مدارک تصویری زندگی می‌کنیم و هم اکنون به نقطه‌ای رسیده‌ایم که محققان ذهنشان را به برخی از سخت ترین و گیج کننده ترین جرم‌ها دوخته‌اند و نرم‌افزارهایی را خلق کرده‌اند که آنچنان روی تصاویر زوم

می‌کنند که تصاویر را به شکل واضح می‌توان دید.

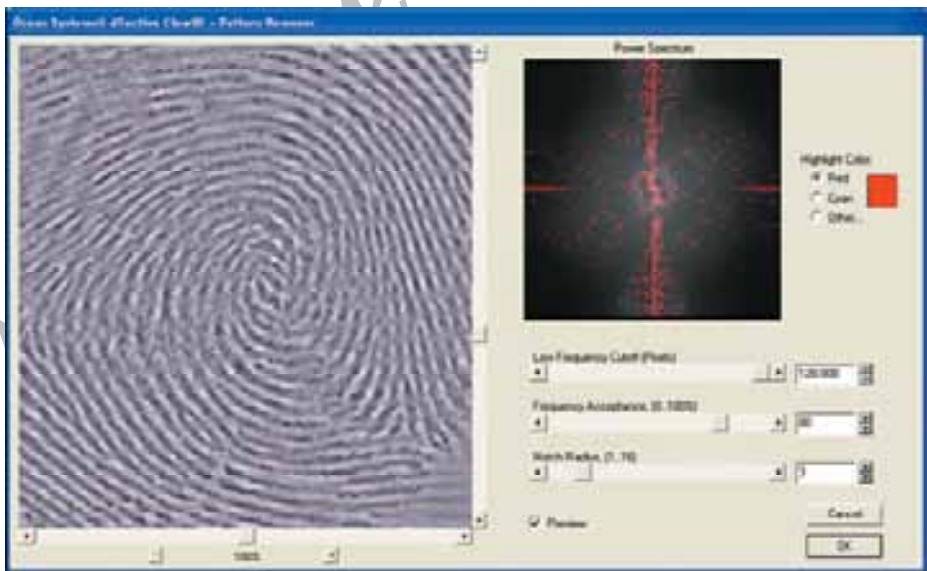
یکی از موفقترین تقاطع برنامه نویسی، تصویرگری و جرایم، برداشتن پیش زمینه از تصاویر است (Online ۲۰۰۹ C.Hass). فرض کنید ردپایی روی مقداری گرد و خاک روی کف پوش چوبی یا اثر انگشتی روی صندلی وجود دارد. شما از این صحنه‌ها عکس می‌گیرید، اما اطلاعات تصویری بیشتری در پس این آثار وجود دارد که تشخیص آنها را بسیار مشکل می‌نماید. آیا بهتر نیست که زمینه‌های ناخواسته از عکس حذف شود؟ با نرم افزار شناخت زمینه دقیقاً همان کاری را که می‌خواهید می‌توانید انجام دهید. جادوی پشت جرایم اثر انگشت الگوریتمی قوی به نام انتقال فوریه سریع است (FFT). ریاضیات FFT خارج از دامنه بحث این مطالب است، اما مفهوم آن بسیار ساده است. حرکت نور و صوت موج شکل است و اگر آنها به صورت پارازیت نباشند، دارای زمینه‌ای هستند. زمینه ویژه را شناسایی کنید، در این صورت می‌توانید آن را بی‌اثر کنید. هر چه که باقی می‌ماند اطلاعات بی نظیری است که به دنبال آن بوده‌اید. FFT برای گرفتن پارازیت در گوشی استفاده می‌شود، همچنین وقتی که شما عکسی را از یک مجله یا کتاب اسکن می‌کنید باز هم این ریاضیات است که برای حذف کردن زمینه‌های نامطلوب به شما کمک می‌کند. تعداد رو به رشدی از نرم افزارهای بهبود و تقویت تصاویر اثر انگشت و جزییات جنایی دیگر، مثل Foray's More Hits و Ocean Sys-tem's ClearID ([www.oceansystems.com/detective/clearid](http://www.oceansystems.com/detective/clearid)) در دسترس هستند که هر دوی آنها بخش کوچکی از نرم افزارهای جرایم تصویری هستند. متأسفانه این برنامه‌ها تنها در سیستم‌های ویندوز اجرا می‌شوند. اگر از سیستم عامل مکینتاش استفاده می‌کنید برای استفاده بهتر از FFT نیاز به رایانه اینتل دو ال کر با نرم افزار فتوشاپ CS۲ دارید که در محیط ویندوز اجرا می‌شود.

فرض کنید اثر انگشتی روی زمینه ناخواسته داریم و می‌خواهیم با نرم افزار ClearID زمینه‌های ناخواسته را از تصویر حذف کنیم (شکل ۵)



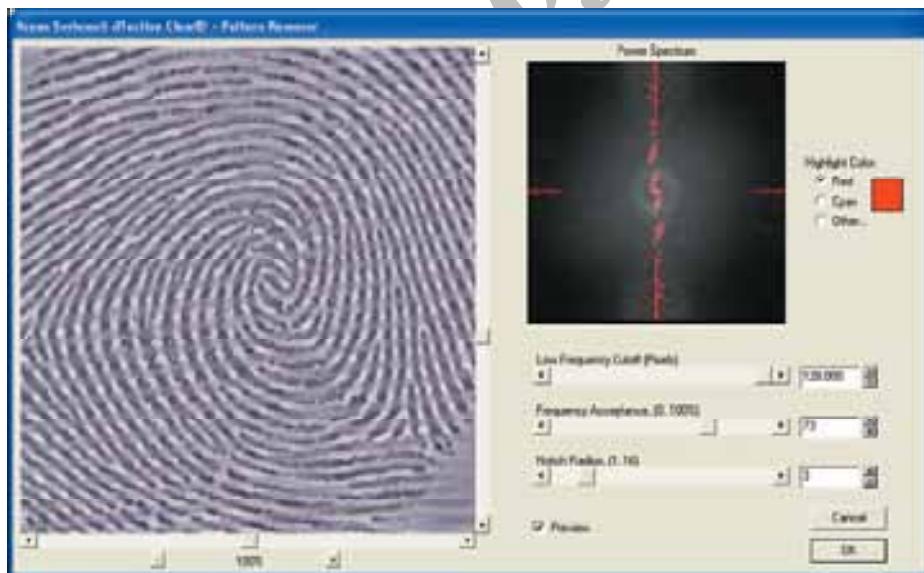
شکل ۵: نمونه‌ای از اثر انگشت که توسط زمینه‌ای مزاحم احاطه شده است.

در شکل بعدی بینیم که چگونه ردیاب پیش زمینه، تصویر را از زمینه‌های نامطلوب حذف می‌کند.

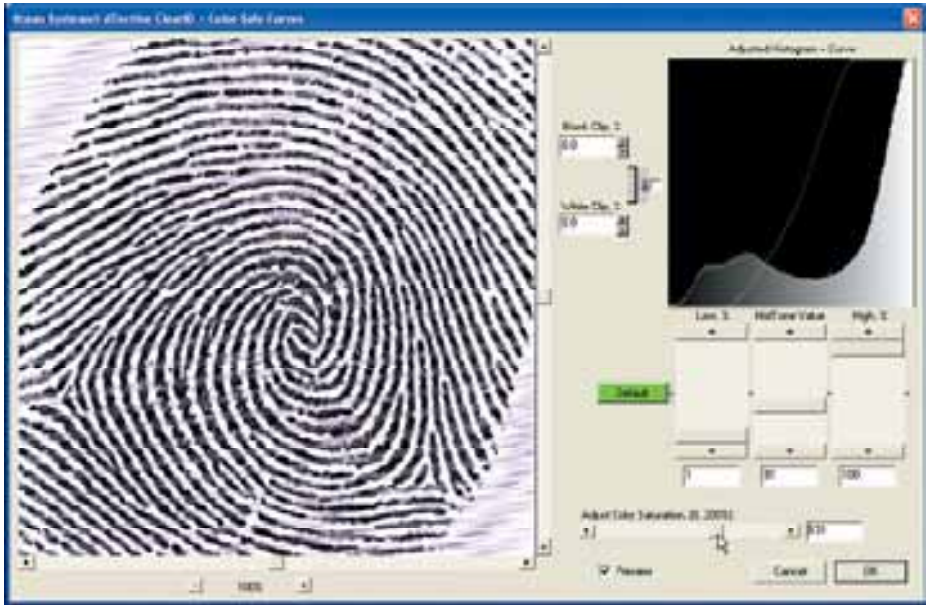


شکل ۶: حذف پیش زمینه ناخواسته

گزینه Slider در پنجره Filter این امکان را فراهم می‌کند که رابطه بین زمینه و اثر انگشت را به بهترین شکل ممکن درآورد و از پاک کردن سهوی اطلاعات تصویری مهم نیز جلوگیری می‌شود. تصویر Power Spectrum در قسمت بالا سمت راست بسامد طرح تصویری است. نقطه‌های قرمز نشان دهنده تکرار طرح است. آخرین Slider که در شکل ۷ مشاهده می‌شود که نقطه‌های قرمز را بزرگتر یا کوچکتر نشان داده است، که این فهمیدن تصویر را آسانتر می‌نماید و شما را در تعدیل تصویر مطمئنتر می‌کند. وقتی تغییرات را اعمال کردید، Script نتایج را در لایه‌ای جداگانه نشان می‌دهد که بتوانید تغییر را به تنهایی ببینید. هنگامی که بیشتر زمینه نامطلوب را حذف کردید، می‌توانید از فیلترهای دیگر در برنامه ClearID برای بهبود وضوح تصویر استفاده کنید و فاصله بین خطوط را تمیزتر کنید به طوری که در شکل ۸ نشان داده شده است.



شکل ۷



شکل ۸: اعمال فیلتر

آخرین عمل برای ایجاد اثر انگشتی مطلوب در فتوشاپ صورت می‌گیرد. با اعمال گزینه Channel Mixer می‌توانید نقطه‌های قرمز را به مونو کروم تغییر دهید (شکل ۹ سمت چپ) و بیشتر زمینه باقیمانده حذف می‌شود. نتیجه نهایی (شکل ۹ سمت راست) اثر انگشتی به اندازه کافی مطلوب و عاری از زمینه‌های نامطلوب است که برای تشخیص هویت مورد استفاده قرار می‌گیرد.

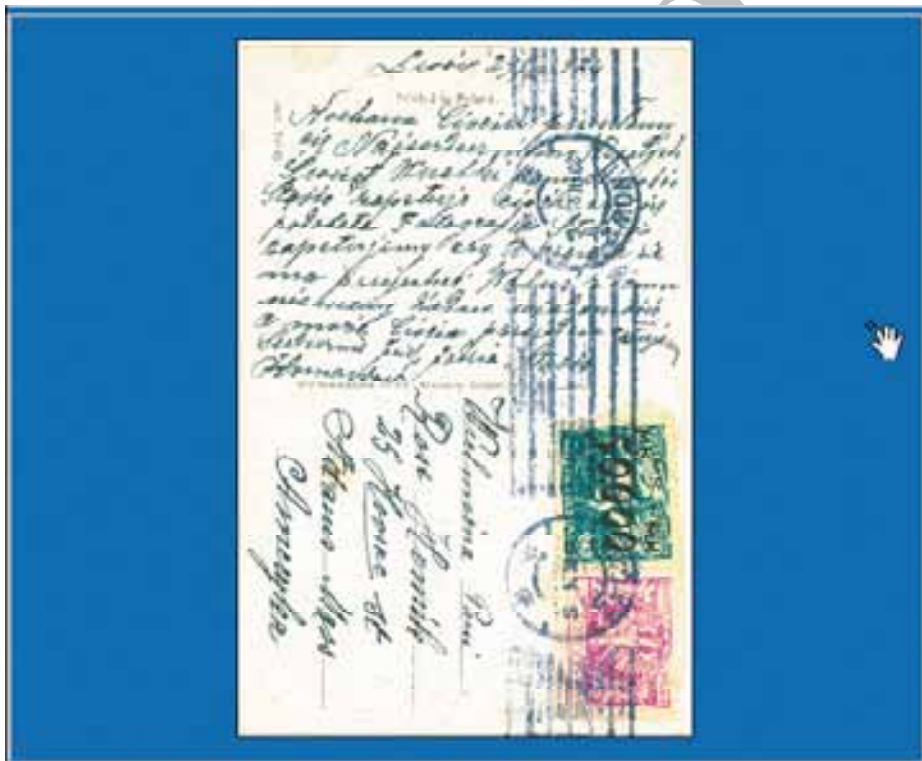


شکل ۹

### جدا کردن متن از زمینه نامطلوب

گاهی اوقات نوشته‌ها یا اسنادی وجود دارند که متن آنها با مهر یا نوشته‌های دیگر در هم آمیخته شده است و چشم انسان به تنهایی قادر به خواندن مطالب نوشته شده نیست. در این مورد نرم افزار Deconvolution برای جداسازی متونی که عمیقاً به هم آمیخته شده اند، استفاده می‌شود (Luo Weiqi: ۱۶۶: ۲۰۰۷). این نرم افزار تداخل رنگ‌های صورت گرفته را جدا می‌نماید و در جرایم تصویری بهترین کمک کار است. این نرم افزار دو رنگی را که ممکن است ما یکسان ببینیم از یکدیگر تمیز می‌دهد، برای مثال یک کارت پستال قدیمی که سرنخ‌هایی را از راز خانوادگی دارد در نظر بگیرید (شکل ۱۰). متن کارت پستال با جوهر

مشکی نوشته شده و بصورت ناتمام رها شده است که بیشتر آن نامفهوم است. به دلیل اینکه خط نوشتاری مشکی، قدیمی و از زبان دیگری است ممکن نیست بتوانیم حدس بزنیم که چه چیزی ممکن است در متن از بین رفته باشد.



شکل ۱۰

در گزینه Color deconvolution، رنگ‌های نامطلوب را با انتخاب نمونه‌ای از آن مشخص می‌کنید (شکل ۱۱). این فرایند را برای مشخص کردن رنگ دلخواه که ممکن است نمونه‌ای از متن باشد تکرار می‌کنید. در نهایت رنگ زمینه را که در این مورد زرد کم‌رنگ است مشخص می‌کنید.





شکل ۱۱

به کادر نگاه کنید، شما دو سایه سیاه در کادرهای رنگی مطلوب و نامطلوب می بینید، اما فیلتر، این دو سایه سیاه را به شکل دو رنگ متفاوت ترکیب شده، تشخیص می دهد. وقتی که گزینه Remove را انتخاب می کنید، پیکسل هایی را در دامنه رنگی نامرئی نامطلوب ایجاد می کند و با انتخاب گزینه Preview یا پیش نمایش می توانید نتایج را مشاهده کنید و می بینید که متن برای خواندن مطلوب است (شکل ۱۲).



شکل ۱۲

## جعل در مقالات علمی

با توجه به قدرت نرم افزار فتوشاپ در تصویرگری، متأسفانه جعل در مقالات علمی هم به کرات توسط این نرم افزار برای داده سازی مشاهده شده است. گاهی شناسایی این گونه جعلیات غیر ممکن است و گاهی نیز بر حسب اتفاق شناسایی می شوند. مهمترین نمونه در این زمینه مربوط به چاپ مقاله‌ای از محقق کره‌ای در مورد سلول‌های بنیادی رویانی انسان است، که توانسته است آنها را کلون کند. جعل تصویر در این مقاله آنچنان ماهرانه انجام شده بود که این مقاله در معتبرترین مجله علمی دنیا -science- به چاپ رسید. او حتی بعد از این مقاله، مقالات دیگری را نیز به چاپ رساند که همگی بر اساس جعل تصویر انجام شده بودند. هیچ کس متوجه این فریبکاری نشد تا اینکه یکی از همکارانش این واقعیت را افشا کرد. اثر خوبی که این واقعه بر جامعه علمی داشت این بود که در مجلات معتبر دنیا هیئت‌هایی در این زمینه برای جلوگیری از این اقدامات تشکیل شد. یکی از مجلات معتبر علمی بیان کرده است که حدود ۲۰ درصد از مقالات ارسالی برای این نشریه، اشکالات عمده‌ای از این قبیل داشته‌اند. به نظر می‌رسد جامعه علمی برای نمونه‌هایی بیشتر از شاهکارهای! فتوشاپ در مقالات علمی باید خودش را آماده کند. مطمئناً جامعه علمی ما هم از بحث جعل سازی تصویری و داده سازی مصون نخواهد بود و متأسفانه هیچ اقدامی هم در این زمینه انجام نمی‌شود. مشکلات احتمالی این مقالات گریبانگیر محققان و دانشجویانی خواهد بود که موضوع این مقالات را به عنوان بخشی از کارهای علمی خود انتخاب می‌کنند. بحث در این زمینه بسیار گسترده است و نمونه‌هایی از جعل فتوشاپ در مقالات بعدی ذکر خواهد شد.

## پرونده‌های حل شده به وسیله فتوشاپ

### پرونده ۱:

در هر دوره‌ای ممکن است دادگاه‌ها مدارکی را که منجر به آزاد شدن مظنون بی گناهی می‌شود، نادیده بگیرند. هر جا که فناوری جدیدی در دادگاه ظاهر می‌شود، طرفین دادگاه می‌توانند ادعا کنند که این فناوری دارای نقص است. قضات با دلیل بیان می‌کنند که در مورد

فناوری‌های جدید باید محافظه کار بود - زیرا محکوم کردن فردی بی گناه وحشتناک است -  
تبرئه کردن یک فرد جنایتکار نیز به همان اندازه مخرب است. در مورد پرونده کانکتیکت  
سوینتون، سرانجام پس از چند سال فناوری به کمک قاضی آمد و او با مدرک قوی، مجرم را  
محکوم و تنبیه کرد (Simon Bramble ۱۶: ۲۰۰۱).

در سال ۱۹۹۱ جسد کارلا تری در یک سطل زباله پلاستیکی در کنار جاده‌ای خلوت در  
ساحل برفی پیدا شد که با پارچه‌ای پیچیده شده بود. کبودی‌های روی گردنش نشان دهنده  
این بود که او را خفه کرده‌اند و همچنین نشانه‌هایی از گاز گرفتگی روی سینه اش وجود داشت.  
محل گاز گرفتگی در فرد زنده بسرعت التیام می‌یابد اگر بافت پوست شکسته نشده باشد. ظاهر  
جسد نشان دهنده این بود که قبل از مرگ با قاتل درگیری داشته است.

آلفرد سوینتن در شب قتل تری در قهوه خانه‌ای نزدیک محل قتل او بود و پلیس برای مظنون  
شدن به او دلیل داشت. آنها او را به بازداشتگاه بردند و از دندان‌هایش قالبگیری کردند. متأسفانه  
علامت‌های گاز گرفتگی را بسختی می‌توان به دندان‌های فرد خاصی مرتبط ساخت، زیرا رد  
دندان‌ها کاملاً ظاهر نمی‌شود و نمی‌توان همخوانی دقیقی را آشکار نمود. علیرغم برخی مدارک  
تصادفی و برخی اظهارات خود محکومی توسط سوینتن، مدارک کافی برای محکومیت وجود  
نداشت و دادگاه نتوانست وی را محکوم کند. سال‌ها گذشت و پرونده از آب و تاب افتاد.

در سال ۱۹۹۸ یخ پرونده شکسته شد، باربارا ویلیامز نرم افزار جدیدی را برای تصویرگری  
خلق کرده بود (Dongho W. ۲۰۰۸). ([www.imagecontent.com](http://www.imagecontent.com)). این نرم افزار  
مورد توجه دکتر کنستانتین کارازولاس دندان شناس جنایی که برای آزمایشگاه علوم جنایی  
پلیس ایالات کانکتیکت کار می‌کرد قرار گرفت. یکی از مشکلات شناسایی و تشخیص محل  
گاز گرفتگی یا دیگر جزییات جرم این است که دوربین در تشخیص وضوح تصویر بسیار بهتر از  
چشم انسانی است و در تفسیر کردن بهتر عمل می‌کند. کارازولاس بسرعت متوجه شد که این  
ابزار می‌تواند نتیجه پرونده تری را روشن کند. با وارد کردن عکس‌های اصلی از کالبد شکافی  
به رایانه، او توانست تشخیصی را بدهد که سال‌ها از انجام آن در مانده بود. سوینتن سرانجام به  
دادگاه احضار شد و بر اساس مدارک جدیدی که از محل گاز گرفتگی تهیه شده بود، محکوم

شد. وکیلش عکس‌های دیجیتالی اصلاح و تقویت شده را قبول نداشت. با تصمیم عالی، دادگاه مقبولیت تصاویر دیجیتال را با تعیین اینکه آنها استانداردهای لازم برای واقعی بودن و بدون تغییر یافتگی دارند، پذیرفت. این تصمیم قاضی راه جدیدی را برای پذیرفتن تصاویر دیجیتال در دادگاه باز کرد. ترکیب فتوشاپ با نرم افزار ویلیامز تأیید شد و سوپنتن هم اکنون در حال سپری کردن محکومیت ۶ ساله اش در زندان است. دکتر کارازولاس ترکیبی از فتوشاپ و نرم افزار ویلیامز را برای کمک به حل چندین مسئله جنایی دیگر، از قتل گرفته تا کودک آزاری به شکل موفق به کار گرفته است.

## پرونده ۲:

در مورد قضیه هیلمون کارآگاهان با معمای عجیبی روبرو بودند. سلاح، قاتل و جسد همه در دسترس بودند (Bredius et al. ۱۹۳۷، ۲۱). مشکل آنها تعیین هویت جسد بود (شکل ۱۳). حدود ۱۳۰ سال طول کشید تا هویت جسد به کمک نرم افزار فتوشاپ مشخص شود.



شکل ۱۳

در سال ۱۸۷۹، جان هیلمون همسرش سالی را در شهر لارنس ایالت کانزاس ترک کرد. او در جستجوی محلی برای ایجاد مزرعه‌ای جدید بود و جان براون به او کمک می‌کرد. قبل از ترک خانه، هیلمون مبلغی پول را برای بیمه عمر خودش هزینه کرد و خود را بیمه کرد... که در آن زمان، این کار تا حدودی غیر معمول بود. دو هفته بعد، تفنگ شکاری براون به طور تصادفی درست روی سر شریکش شلیک شد و فوراً او را از پای درآورد.

وقتی بیوه عزادارش به دنبال گرفتن پول بیمه مردن شوهرش بود، شرکت بیمه موتوال لایف به این جریان مشکوک شد. در نظر آنان این عمل از قبل طراحی شده بود. شاید هیلمون و براون برای تقسیم کردن پول بیمه، نفر سومی به نام فردریک والترز - شخص گمشده‌ای که هم سن و سال هیلمون بود - را کشته بودند. قبل از آزمایش‌های خونی، اثر انگشت یا نمونه DNA، تشخیص هویت با چشم انجام می‌شد. متأسفانه بیشتر افراد حافظه ضعیفی برای به خاطر سپردن چهره‌ها دارند، حقیقتی که اغلب شاهدان عینی را برای شناخت دچار اشتباه می‌کند. برخی از افرادی که هیلمون را ملاقات کرده بودند و جسد را دیدند مطمئن نبودند که او هیلمون باشد (شکل ۱۴).



شکل ۱۴: عکس سمت راست متعلق به هیلمون و سمت چپ والترز است که شباهت این دو قابل تأمل است.

شهادت زن هیلمون، از آنجا که مبلغ زیادی پول به دست می‌آورد مشکوک بود، بنابراین شرکت بیمه از پرداخت پول خودداری کرد. سالی هیلمون در سال ۱۸۸۲ تحت تعقیب قانونی قرار گرفت. براون در دادگاه داستان خود را تغییر داد و قسم خورد برای پول والترز را کشته است. او قبل از اتمام دادرسی حرفش را پس گرفت و ادعا کرد که شرکت بیمه تهدید کرده بود برای قتل هیلمون از او استفاده کنند. شواهد و مدارک متناقض منجر به سردرگمی هیئت منصفه شد و دادرسی جدیدی در سال ۱۸۸۵ شروع شد. این دادرسی هم به همان روش اولی خاتمه یافت و دادرسی سوم در سال ۱۸۸۸ شروع شد. در دادرسی سوم، سالی هیلمون برنده شد، ولی ماجرا تمام نشده بود زیرا شرکت بیمه درخواست استیناف کرد و پرونده به دادگاه عالی رفت. در سال ۱۸۹۹ بعد از دو دادرسی دیگر، سرانجام دو طرف به این نزاع پایان دادند.

معما بعد از همه دادرسی‌ها همچنان حل نشده باقی ماند؛ آیا جسد دفن شده واقعاً هیلمون بود؟ در بهار سال ۲۰۰۵، میمی و سن استاد دانشگاه کلرادو این معما را به همکارش دنیس گرون استاد انسان شناس منتقل کرد. ون گرون به عکس‌های هیلمون، والترز و جسد نگاه کرد. هیلمون بینی منحنی‌واری داشت، با فرو رفتگی عمیقی بین چشمان، به طوری که در عکس دوم مشخص است. این یک ویژگی مشخص است که به‌عنوان بخشی از ساختار جسد در مجموعه باقی می‌ماند. او مطمئن بود که اگر بتواند جسد را مورد آزمایش قرار دهد، می‌تواند روش‌های جنایی استاندارد برای تطبیق دادن عکس‌های هیلمون و والترز با آن جعبه را استفاده کند. فرضیه او این بود که هر دو دارای صورت‌هایی هستند که برای تطبیق دادن با جسد به‌وسیله فتوشاپ به اندازه کافی متفاوت هستند و می‌توان یکی از آنها را به جسد نسبت داد (Cheng L. et al. ۲۰۰۹: ۱۲).

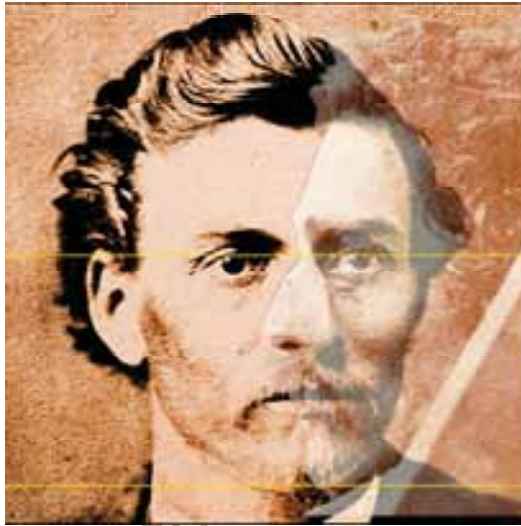
گاهی اوقات معماها در مقابل حل شدن از خود مقاومت نشان می‌دهند. وقتی و سن و ون گرون مجوز نبش قبر را دریافت کردند تابوت در وسط یک چشمه یافت شد. لاشه‌های استخوانی و دندانی کمی باقی مانده بود. آیا می‌توان با استفاده از DNA این معما را حل کرد؟ بله افرادی از نسل‌های هر دو جسد کاندیدا که برای کمک کردن مشتاق بودند وجود

داشت، ولی در اثر سال‌ها جاری شدن آب، همه DNAها شسته شده بودند. اما ون گرون تسلیم نشد. شاید آنها جسدی برای تشخیص هویت در دسترس نداشتند، ولی تعدادی عکس خوب و نرم‌افزار فتوشاپ وجود داشت. آیا او به جای تطبیق عکس با مجموعه می‌تواند از تصاویر جسد و مردانی که از نسل او هستند و اکنون در قید حیات به سر می‌برند استفاده کند؟ او با این روش نخواهد توانست تشخیص درستی بدهد، زیرا دو مرد وجود دارد که ممکن است جسد متعلق به آنها باشد. به دلیل شکل مشخص بینی هیلمون، ون گرون از طریق فرایند حذف کردن ممکن است قادر به تشخیص جسد باشد. در مرحله اول باید مطمئن می‌شد که مقایسه ۳ عنصر بدرستی انجام می‌شود. عکس دیگری از والترز وجود داشت؛ صورت رو به جلو و جهت دار مشابه عکس دوم هیلمون. تصاویر نیاز به مرتب کردن و تطبیق دادن در جهت مناسب داشتند. با فتوشاپ، تطبیق دو عکس در اندازه‌های مختلف نسبتاً آسان است. گام اول عمود کردن دو عکس است (یعنی چند زاویه‌ای که از خط عمود انحراف دارند را درست کنیم). آنها این کار را با استفاده از ابزار Measure برای کشیدن خط مستقیمی دور تا دور عکس انجام دادند و سپس با انتخاب گزینه‌های Image و سپس Rotate Canvas و در نهایت Arbitrary تصویر را به صورت عمود درآوردند. نمای جلو اطلاعات کافی را فراهم نمی‌کند، اما نمای جانبی به صورت واضح ساختار صورت و انحناهای مشخص بینی را نشان می‌دهد.

ون گرون می‌دانست که نواحی آناتومی مشخصی روی صورت وجود دارد که ممکن است برای مقایسه کردن با عکس‌ها به او کمک کند. او برای تعیین این مناطق، روی تصویر هر دو مرد، بالای استخوان بینی بین چشم‌ها را انتخاب کرد و حاشیه پایینتر گونه و خط‌های افقی را رسم کرد و همین کار را برای نمای جانبی چرخیده شده جسد انجام داد و توانست جسد را با تصویرهای هر کدام از مردان، به صورت جداگانه تطبیق دهد.

وقتی تصاویر والترز و جسد روی هم منطبق شدند، مسئله به سرعت حل شد و مشخص شد هیچ ارتباط فیزیکی بین آن دو وجود ندارد. بینی‌ها در اندازه‌های متفاوت بود، خط پیشانی همخوانی نداشت و بینی والترز ساختار منحنی وار نداشت. ولی در مورد تطابق بین جسد و

هیلمون نمی توان همین مسائل را بیان کرد، از خط رستنگاه مو گرفته تا چانه همخوانی بسیار کامل بود (شکل ۱۵).



شکل ۱۵

کار ون گرون با فتوشاپ نمونه‌ای کلاسیک از تحقیقات علمی در زمینه تصاویر دیجیتال جنایی است. او و وسن به صورت قطعی والترز را به عنوان مردی که در تابوت بود حذف کردند و ثابت کردند که باور سرسختانه زن هیلمون درست بوده است.

### نتیجه گیری

با توجه به کاربرد خاص و با اهمیت نرم افزار فتوشاپ در امور جنایی، وجود متخصصان این نرم افزار در بین کارآگاهان امری ضروری به نظر می رسد. نمونه‌های بیان شده در مورد استفاده از فتوشاپ در این مقاله نشان می دهد که این نرم افزار می تواند چه اندازه مخرب و چه اندازه سازنده باشد. استفاده مطلوب از این نرم افزار کمک شایانی به کارآگاهان در کشف جرم خواهد نمود، همان گونه که در مورد پرونده هیلمون توضیح داده شد. همان طور افراد تبهکار از



تصاویر دیجیتال و نرم‌افزارهای ویرایش تصویر برای رسیدن به اهداف خود استفاده می‌کنند، کارآگاهان جنایی هم باید قادر به تشخیص این تغییرات در تصاویر باشند و مجرمان مورد نظر را تحت پیگرد قانونی قرار دهند و همچنین بتوانند از این نرم‌افزارها برای کشف جرم استفاده کنند. از تصاویر دیجیتال در دادگاه‌ها هم ممکن است به‌عنوان مدرک جرم یا مدرک برائت استفاده شود. درک ناصحیح از تصاویر دیجیتال ممکن است منجر به محکومیت فرد بی‌گناه و تبرئه یک جنایتکار خطرناک شود. مقوله جعل تصویری در مقالات علمی هم یکی از موضوعاتی است که دامنگیر همه کشورها شده است و کشور ما هم از این قاعده مستثنا نیست. در برخی کشورها محکومیت‌هایی برای این‌گونه جعلیات علمی در نظر گرفته می‌شود، ولی متأسفانه در کشور ما هیچ اقدامی در مورد فریبکاران علمی نشده است.

## منابع

- 1- A. Swaminathan, M. Wu, and K. J. R. Liu, "Non-intrusive component forensics of visual sensors using output images," IEEE Trans. Inf. Forensics Security, vol. 2, no. 1, pp. 91–106, Mar. 2007.
- 2- Bredius, Abraham. A New Vermeer, The Burlington Magazine for Connoisseurs, Vol, 71, No. 416, p. 210–211, Nov. 1937.
- 3- Cheng-Liang Lai, Yi-Shiang Chen, Proceedings of the Eighth International Conference on Machine Learning and Cybernetics, Baoding, 12-15 July 2009.
- 4- C. Hass, Impulseadventure – JPEG Quality and Quantization Tables for Digital Cameras, Photoshop 2009 [Online]. Available: <http://www.impulseadventure.com/photo/jpeg-quantization.html>
- 5- Douglas, K.S., Lyon, D.R. & Ogloff, J.R.P. "The Impact of Graphic Photographic Evidence on Mock Jurors' Decisions in a Murder Trial: Probative or Prejudicial?" Law and Human Behavior, Vol. 21, No. 5, 1997
- 6- Luo Weiqi, Qu Zhenhua, Pan Feng, Huang Jiwu, Front. Comput. Sci. China 2007, 1(2): 166–179.

- 7- P. S. Hiremath, Jagadeesh Pujari, International Conference on Computational Intelligence and Multimedia Applications 2007.
- 8- Simon Bramble, 13th Interpol Forensic Science Symposium, Lyon, France, October 16-19 2001.
- 9- W. Sabrina Lin, Steven K. Tjoa, H. Vicky Zhao and K. J. Ray Liu, Transactions on Information Forensics and Security, Vol. 4, No. 3, September 2009.
- 10- Witkowski, Jill. "Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images," 10 WASH. U. I. L. & POL'Y 267, 273 (2002).
- 11- Youngsoo Kim, Dowon Hong, Dongho Won, Advanced Software Engineering & Its Applications 2008.