Florida International University

FIU Digital Commons

2024

Forensic analysis of images

Isabel Fernández Corcobado

Alejandro Maestre Gasteazi

Unai Tapia

FIU GLOBAL FORENSIC AND JUSTICE CENTER
2024 Global Forensic Science Symposium
Tue 04 Jun - Fri 07 Jun, 2024
11200 SW 8th Street, Miami, FL 33199 United States

ASOCIACIÓN ESPAÑOLA DE IMAGEN CIENTÍFICA Y FORENSE · ISFO · PROBATIA Forensic Science · COLEGIO DE BIÓLOGOS

FORENSIC ANALYSIS OF IMAGES

Maestre Gasteazi, A.[1,3], Muriel Tapia, U.[1,3], Fernández Corcobado, I.C.[1,2,4]
[1] Spanish Association of Scientific and Forensic Imaging (AEICF), [2] Innovative Science Forensics Office (ISFO),
[3] Probatia Forensic Science, [4] Official College of Biologists of the Community of Madrid (COBCM), Spain

BACKGROUND 01

The Spanish Association of Scientific and Forensic Image works on the application of **new techniques of 'Forensic Analysis of Images' based on Data Science and BlockChain technology in the scientific and forensic environment,** establishing the methodology and good practices in this field, to improve the processes of investigation or review of cases and in particular those dealing with missing persons.

It involves optimization of workflows with evidence characterized by multimedia files and the specialization of forensic expert practice, since currently this dynamic is excessively slow and inefficient. **It translates into the speeding up of investigations and inquiries, which are especially decisive in the first hours, especially for cases aimed at locating people.** The particular usefulness of **these techniques serves to guarantee the veracity and origin of the files on which the investigations are developed,** of any of the cases to which the criminal justice system is applicable.

We present a model case, in which we appreciated the improvements during the research for image analysis and the advantages resulting from the application of our methodology in question.

This model is based on data from the previous FERNÁNDEZ CORCOBADO, I.C, Forensic thermomicrobiology. Forensic Approach to Time of Death Diagnosis (https://www.eurekalert.org/news-releases/726775, http://hdl.handle.net/10481/2047) research, where the main conclusions were the following:

- A distinction can be made between the living state and the cadaver state based on the count of the microorganism *Propionibacterium acnes* on human skin.
- The criminological cause of death - accidental or caused - can be distinguished on the basis of the growth parameters of *P. a*: number of generations, growth speed and generation time.
- A distinction can be made between existence and phases of decomposition, shorter or longer than 12 hours, depending on the growth parameters of *P.acnes*.
- For the sample of cadavers with a death certificate, 97% of the variance of the variable 'hours elapsed since discovery' can be predicted with the growth parameters of *P. acnes* : 'number of *P. acnes* generations per individual' and 'P. acnes growth speed per individual'.
- There is a relationship between the growth parameters of *P. acnes* and the temperatures in the corpse recorded by infrared thermography, although the correspondence between the temperature of the cadaveric remains and the time elapsed since death is slight and does not allow a greater approximation to the diagnosis of the time of death.
- However, there is a strong correspondence between the growth parameters of P. acnes on cadaveric remains, with respect to the time elapsed since death, which allows a greater approximation to the calculation for the diagnosis of the time of death, applicable to criminal investigations.

KEYWORDS: IMAGE, ANALYSIS, OPTIMIZATION

OBJECTIVES 02

To improve forensic techniques to acquire and analyze digital evidences, to investigate and prevent crime.

& FUTURE DEVELOPMENTS

ANTHROPOMETRIC FACIAL RECOGNITION IMAGE ANALYSIS
FAKE IMAGE ANALYSIS

2D & 3D MODELS FROM DRONE/SATELLITE CAPTURED IMAGES APPLIED TO FORENSIC EXPERTISE: LOCATION OF BURIALS

IMAGE BASED DOCUMENT EXAMINATION

OUTCOMES 04

©FERNÁNDEZ CORCOBADO, I.C, INSTITUTE OF LEGAL MEDICINE OF GRANADA, SPAIN, 2006
2006-08-22 11:24:07   -40 - +120   e=0.78   °C

FORENSIC THERMOGRAPHY
TIME OF DEATH DIAGNOSIS IMAGE ANALYSIS BASED

WHEN **FORENSIC IMAGE ANALYSIS** IS APPLIED, IT IS OBTAINED THAT:

THE SCATTER GRAPHICS INDICATE THAT **THERE IS A HIGH CORRELATION BETWEEN THE VARIABLES THAT REPRESENT THE TIME ELAPSED SINCE THE FINDING OF A BODY AND THE CAUSE OF DEATH (ACCIDENTAL OR CAUSED), REGARDING THE VALUES CORRESPONDING TO THE RGB CHANNELS OF THE PIXELS** THAT FORM THE DIGITAL IMAGE OF THE BODY..

A STRONG CORRELATION IS EVEN OBSERVED BETWEEN THE GROWTH PARAMETERS OF PROPIONBACTERIUM ACNES 'GROWTH SPEED' AND GENERATION TIME ALSO WITH RESPECT TO RGB CHANNELS.

CONCLUSIONS 05

IT IS POSSIBLE TO MAKE AN APPROACH TO THE DIAGNOSIS OF THE DATE OF DEATH THROUGH THE FORENSIC ANALYSIS OF DIGITAL IMAGES

Probatia is a digital evidence analysis tool designed to facilitate and optimize the work of forensic investigators on the processing of electronic evidence, such as digital images for Forensic Analysis of Images.

Features:

1. Identification, acquisition and preservation of electronic evidence in accordance with the UNE-EN ISO/IEC 27037:2016 standard, which guarantees the integrity and authenticity of the evidence.
2. Automatic analysis of digital evidence and multimedia files, based on scientific methods and standardized procedures, for faster and more efficient analysis.
3. Collaborative analysis system that is based on a database of highly qualified experts.
4. Presentation of expert reports for the interpretation and use of the results by the judicial authorities.
5. Chain of custody with blockchain technology, which guarantees the integrity and authenticity of digital evidence, as well as traceability at all times during the analysis process.
6. User management and information compartmentalization to ensure the security and privacy of all data.

References:
¹ https://probatia.com/
² https://aibase.com/products/image54f/
³ https://www.eurekalert.org/news-releases/726775

DEFINITIONS

Digital Evidence is all information in digital format of any nature, identifiable and capable of being treated in a differentiated manner, and generated, treated and managed and/or stored in a way that ensures its reliability, completeness and probative value.

Chain of Custody: is the controlled traceability procedure that is applied to digital evidence, throughout its useful life. The chain of custody aims to preserve the integrity and authenticity of these, ensuring throughout this process that the relevant information is not altered.

The digital evidence management system must be able to solve the following challenges: • Integrity and authenticity of evidence; • Traceability; • Long-term preservation; • Evidence collection; • Reproducibility; • Jurisdiction and privacy • Technical capabilities; • Huge data volumes: • Huge data volumes; • Data diversity; •Unstructure data.

For this model case, we first analyzed the images obtained from the previous research mentioned - on a sample of corpses with a death certificate -, using the open source software Image4 1.54f (http://imagej.org), specifically on the pixels of the areas of the bodies, that make up the study sample.

As each image pixel is an imaging unit defined by three RGB channels (red, green and blue) with intensity values between 0 and 255, for each one, this software quantifies the pixels and graph the images of the sample of corpses studied. In this case, were obtained scatter plots that relate the representative variables of the growth parameters of *P. acnes* with the pixel RGB canals values resulting from the analysis of both digital and thermographic images of the corpses sample.

The advantage of using Probatia secure automated platform is evident given the large number of images to be processed during forensic analysis.

To analyze digital evidences Probatia team focus on its intrinsic properties - intangible electronic format; volatility; destructibility; partial and intrusive about legal rights-; the difficulty of managing the chain of custody to preserve the integrity and authenticity of relevant information; to process large volumes of data.

They follow **4 steps,** using the secure **'PROBATIA FORENSIC SCIENCE '** platform to automate it.

METHODS 03

PROBATIA FORENSIC SCIENCE METHODOLOGY:

1 - WORKFLOW PLANNING BLOCKCHAIN TECHNOLOGY BASED
Compartmentalizing information and management of user permissions is essential to ensure the security and privacy of data on any platform, especially in the case of applications related to forensic investigations and digital evidence. PROBATIA Key Functions: 1.1 Set user roles; 1.2 **Role-based access control (RBAC);** 1.3 Object-level access: 1.4 **"Least privilege" permission policy;** Auditing and tracking; Periodic access reviews

Securing the scene: Protecting to avoid modifications or destruction of digital evidence / Identify who manages the capture devices: employees; external personnel, suppliers, etc. / Classify storage devices: hard drives, memory cards, Smartphone, etc. / Photographic and visual recording of scene and evidence elements.
Capturing evidence: By recording and storing forensic images, directories and files / Classify according to file type, giving preference to visual and multimedia content / Capture of evidence published on the web. Timestamped record of all media content, as well as a screenshot. / Capture of e-mails through access of an account with username and password / Tolomatic reception of evidence / Integration with other forensic tools / Facilitate integration with other forensic tools and data analysis software, allowing investigators to leverage the capabilities of these tools to conduct more advanced and comprehensive analysis of evidence. This could include the ability to import or export data between your platform and other digital forensics tools.
Chain of custody: Acquisition of all evidence is recorded through Blockchain technology.
Preservation of evidence: All evidence is stored securely, as well as protecting its access to any user outside the case. Registering in an unalterable way the date of registration, as well as all the users who have had access to the visualization and / or download of the evidence. Allow researchers to add notes or labels to evidence to facilitate its organization and follow-up during the investigation.
It also allows you to register the capture and / or storage devices. Thus allowing to faithfully identify the origin of each and every one of the evidence gained.

DEVICE

PHASES OF INVESTIGATION WORK

PROCEEDINGS	EVIDENCE ANALYSIS	REPORTING
- Acquisition of evidence according to **ISO/IEC 27037:2016** standard, allowing us to act in the least intrusive way possible, respecting the originality of the evidence through **BlockChain** technology. - Creating a forensic image of the storage drive(s)	Automatic analysis of computer and multimedia evidence through the use of **Artificial Intelligence** and **Big Data**	- Streamlines the presentation of expert reports showing in an orderly and detailed manner all the evidence with **HASH signatures** and time stamps to guarantee the correct Chain of Custody - STANDARD UNE 19/010:2015 Drafting of expert reports

All evidence is identified, collected, preserved, analyzed and presented ensuring the chain of custody

PHASE 1: LOGGING LOCATIONS, DEVICES AND FILES	PHASE 2: MANAGEMENT, CLASSIFICATION AND ANALYSIS OF EVIDENCE	PHASE 3: ADJUSTING REPORTING OPTIONS
- Location and description of the scene - Identification of the operators of the capture devices - Classification of devices found: hard drives, memory cards, smartphones - Logging device disk images or files obtained from logical extraction Hash signature and time stamp of all evidence through blockchain registration	- Search and classification of evidence according to the criteria of the investigation - Analysis of automatic authentication of multimedia files - Advanced batch metadata analysis of individual files **IMAGE ANALYSIS**	- Drafting of reports adjusted to scientific methodology - Presentation of evidence with HASH signature and timestamp certificates - Reports adapted to different models according to current legislation

PHOTOGRAMMETRIC ANALYSIS · BIOMETRIC IDENTIFICATION · CAMERA BALISTIC
CONVOLUTION TECHNIQUES · FREQUENCY ELIMINATION TECHS · QUALITY IMPROVEMENT

2 - PATTERNS IDENTIFICATION
that support or invalidate the integrity and veracity of the developed images, both in their binary structure and in their pixel matrix. Digital images are data; hence, many tools originally developed for data science can be applied to the systematic treatment of them. Machine learning models, for example can be trained to extract information from the content of the images, which up until recently, was only possible through visual examination. This is a rather time-intensive task, and the likelihood of human error increases with the volume of image files to assess. These models can quickly find images that contain relevant information to be then personally analyzed by the investigator. Some examples include: identifying photographs or scans of paper documents, security footage files or images that depict children. Facial recognition algorithms powered by machine learning can also flag all images portraying a predefined individual. Some models have shown good accuracy in distinguishing between groups of pixels from different camera images and models, a feat beyond the most skilled human visual examiners. An automated triage system combining these technologies with other tools designed to identify possible flaws in the integrity of digital image files (metadata, compression levels, noise levels) can help professionals focus their attention on images that are likely to be the most useful. This becomes increasingly relevant in cases containing large amounts of images from hard drives, mobile phones or OSINT scrapping.

3 - CRIMINALISTICS TECHNIQUES FOR IMAGE
Document examination / Graphistics
The forensic handwriting expert needs having the documents to be analyzed in their original paper support. The clients often provide the documentation, sometimes documents are submitted to the Court, allowing the 'in situ' examination, but without taking it to the professional office. Both sets of documents must equally comply with the Chain of Custody.
A fundamental task of the forensic handwriting expert is taking photograph of all the documentation to be analyzed, using different technical equipment in order to carry out computer based studies, analysis, and comparisons.
One of those technical devices is the HS3B [2], which takes photographs at different wavelength and from various angles of incidence. These photographs are stored on an internal SD card and data (images) are transferred to the professional's computer. Throughout this process, the chain of custody must be maintained.
The photographic capture taking from the document must be completely recorded and verified, since the obtained images can subsequently undergo digital processing. However, the images obtained initially must not be altered. Therefore, it's of utmost importance to guarantee the integrity of the obtained image, including its content (not only its metadata), as these will need to be included in the expert report that's issued.
Time of Death Diagnosis Image Analysis based: tested through Forensic Thermography and Microbiological Time of Death Diagnosis [3] analysis (see 'OUTCOMES').
4 - OTHER APPLICATIONS IN DEVELOPMENT, DERIVED FROM DIGITAL IMAGE ANALISIS
Anthropometric Facial Recognition Image Analysis based
Analysis of Evidence or Interior/Exterior Scenarios by Photogrammetry and/or mobile phone, scanner, drone or satellite captured.

ASOCIACIÓN ESPAÑOLA DE IMAGEN CIENTÍFICA Y FORENSE
HTTPS://IMAGENCIENTIFICA.ES/

Contact info:
isabel.fernandez@imagencientifica.es, alejandro.maestre@imagencientifica.es, unai.tapia@imagencientifica.es