NAME-KUNAL DNYANESHWAR MUNGASE ROLL NO.-FP1126

SUBJECT-DIGITAL IMAGE PROCESSING:-ACTIVITY:2 CLASS-F.Y. M.SC. – CYBER SECURITY

HOW DIGITAL IMAGE PROCESSING HELPS IN DIGITAL FORENSICS 🔍

EVER WONDERED HOW INVESTIGATORS CATCH CRIMINALS USING JUST PIXELS AND CODE? WELCOME TO THE FASCINATING WORLD OF DIGITAL IMAGE FORENSICS!

IN TODAY'S DIGITAL AGE, IMAGES TELL STORIES—BUT NOT ALL OF THEM ARE TRUE. FROM DEEPFAKES TO DOCTORED EVIDENCE, THE ABILITY TO VERIFY IMAGE AUTHENTICITY HAS BECOME CRUCIAL. DIGITAL IMAGE PROCESSING IS THE SUPERHERO THAT HELPS FORENSIC EXPERTS SEPARATE FACT FROM FICTION, ONE PIXEL AT A TIME.

WHAT IS DIGITAL IMAGE FORENSICS? 🎯

DIGITAL IMAGE FORENSICS IS LIKE BEING A DETECTIVE FOR PICTURES. IT'S THE SCIENCE OF VERIFYING WHETHER AN IMAGE IS AUTHENTIC OR HAS BEEN TAMPERED WITH. THINK OF IT AS A TRUTH-SERUM FOR DIGITAL PHOTOS—IT EXAMINES EVERY TINY DETAIL TO UNCOVER HIDDEN SECRETS.

UNLIKE TRADITIONAL FORENSICS THAT DEALS WITH FINGERPRINTS AND DNA, DIGITAL FORENSICS WORKS WITH PIXELS, METADATA, AND COMPRESSION ARTIFACTS. IT'S THE INTERSECTION WHERE TECHNOLOGY MEETS JUSTICE.

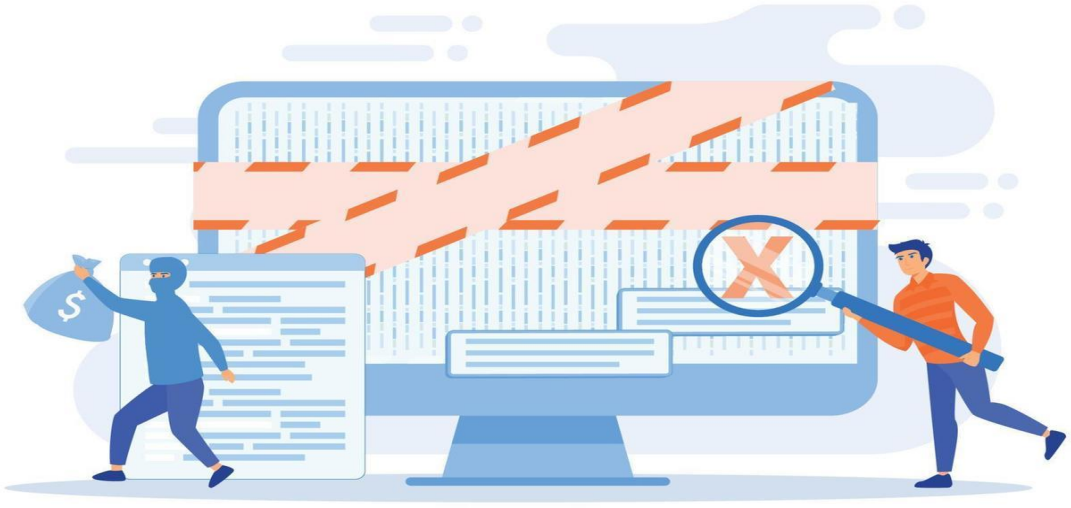


ILLUSTRATION OF DIGITAL FORENSICS FEATURING CYBERCRIME DETECTION AND INVESTIGATION USING DIGITAL TOOLS

WHY DOES THIS MATTER? IN LEGAL PROCEEDINGS, JOURNALISM, MEDICAL DIAGNOSES, AND SECURITY INVESTIGATIONS, THE AUTHENTICITY OF IMAGES CAN LITERALLY CHANGE LIVES. A SINGLE MANIPULATED PHOTO CAN SEND AN INNOCENT PERSON TO JAIL OR LET A CRIMINAL WALK FREE.

THE MAGIC BEHIND IMAGE PROCESSING IN FORENSICS ✨

DIGITAL IMAGE PROCESSING USES SOPHISTICATED ALGORITHMS AND AI TO ANALYZE IMAGES IN WAYS HUMAN EYES NEVER COULD. HERE'S HOW IT WORKS:

1. METADATA EXAMINATION: THE IMAGE'S DIGITAL FINGERPRINT 📋

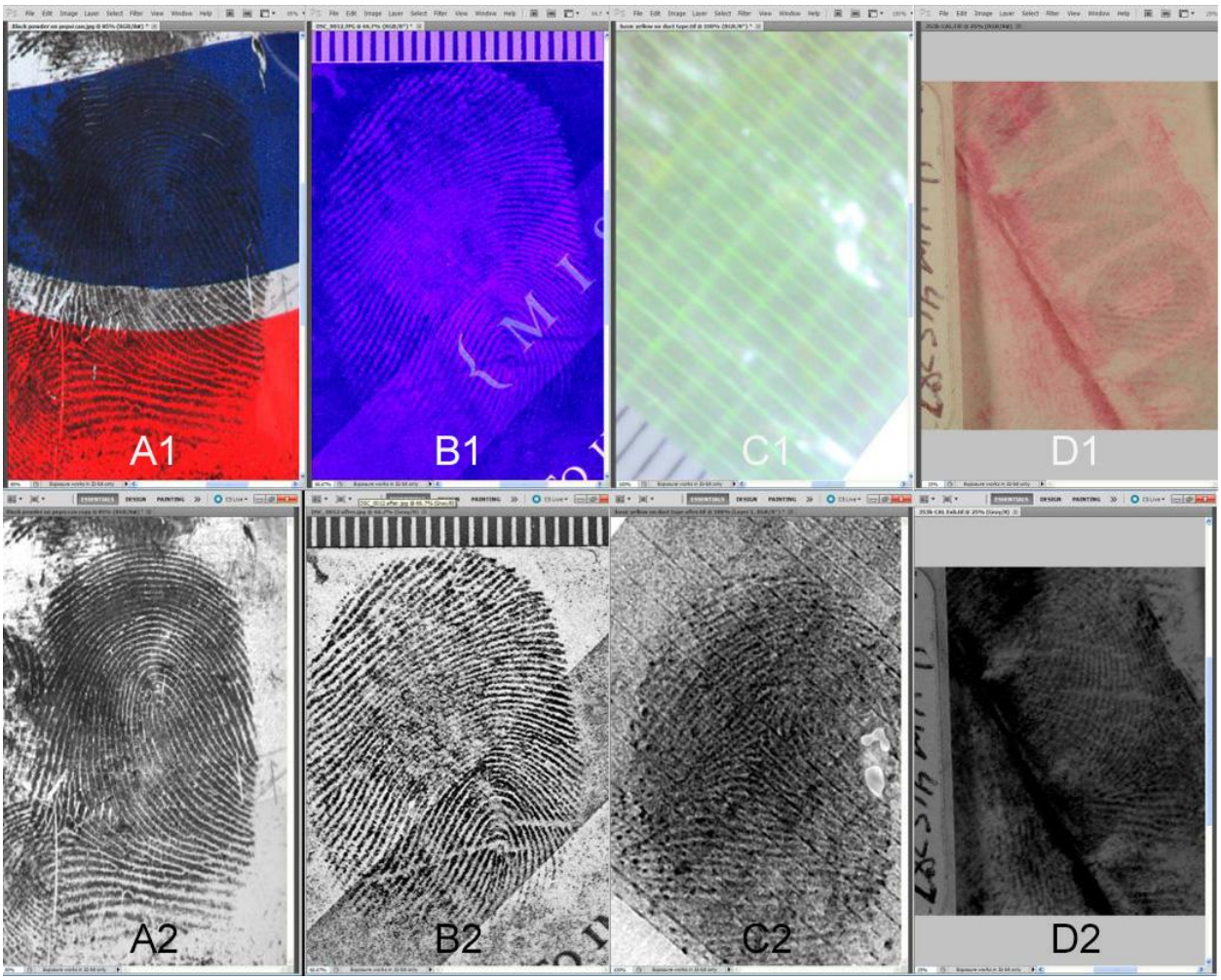
EVERY DIGITAL IMAGE CARRIES HIDDEN INFORMATION CALLED METADATA (EXIF DATA). THIS INCLUDES DATE AND TIME THE PHOTO WAS TAKEN, CAMERA MODEL AND SETTINGS, GPS LOCATION COORDINATES, AND SOFTWARE USED FOR EDITING.

FORENSIC EXPERTS EXAMINE THIS METADATA LIKE READING A DIARY. INCONSISTENCIES—LIKE A PHOTO SUPPOSEDLY TAKEN IN 2020 BUT SHOWING METADATA FROM 2018—IMMEDIATELY RAISE RED FLAGS. IF TIMESTAMPS DON'T MATCH, OR IF EDITING SOFTWARE TRACES APPEAR WHERE THEY SHOULDN'T, INVESTIGATORS KNOW SOMETHING'S FISHY.

2. PIXEL-LEVEL ANALYSIS: ZOOMING INTO THE TRUTH 🔬

THIS IS WHERE THINGS GET SERIOUSLY TECHNICAL. FORENSIC TOOLS ANALYZE INDIVIDUAL PIXELS TO DETECT LIGHTING INCONSISTENCIES, COMPRESSION ARTIFACTS, COPY-MOVE FORGERY, AND NOISE PATTERNS.

MODERN TOOLS CAN EVEN IDENTIFY WHICH SPECIFIC CAMERA TOOK A PHOTO BY ANALYZING ITS UNIQUE "NOISE FINGERPRINT"—LIKE A CAMERA'S DNA. EVERY CAMERA LEAVES A DISTINCTIVE NOISE IN THE PRODUCED IMAGES, ALLOWING FORENSIC EXPERTS TO CREATE A CAMERA REFERENCE PATTERN (CRP) FILE THAT CAN TRACE IMAGES BACK TO SPECIFIC CAMERA EXEMPLARS, EVEN WHEN IMAGES HAVE BEEN MILDLY COMPRESSED, ROTATED, OR CROPPED.



FINGERPRINT IMAGES BEFORE AND AFTER DIGITAL ENHANCEMENT SHOWING IMPROVED CLARITY FOR FORENSIC ANALYSIS

3. STEGANOGRAPHY DETECTION: UNCOVERING HIDDEN MESSAGES 🕵️

STEGANOGRAPHY IS THE ART OF HIDING SECRET MESSAGES INSIDE IMAGES. CRIMINALS MIGHT HIDE ILLEGAL INFORMATION IN INNOCENT-LOOKING PHOTOS. DIGITAL FORENSICS USES AI-POWERED TOOLS LIKE ALETHEIA AND STEGEXPOSE TO DETECT THESE HIDDEN PAYLOADS BY ANALYZING STATISTICAL PATTERNS AND IMAGE FEATURES LIKE PSNR (PEAK SIGNAL-TO-NOISE RATIO) AND MSE (MEAN SQUARE ERROR).

REAL-WORLD APPLICATIONS: WHERE DIGITAL IMAGE FORENSICS SAVES THE DAY 🦸

LAW ENFORCEMENT & CRIMINAL INVESTIGATIONS 👮

POLICE USE IMAGE FORENSICS TO VERIFY SURVEILLANCE FOOTAGE AUTHENTICITY, DETECT MANIPULATED EVIDENCE, ENHANCE BLURRY IMAGES TO IDENTIFY SUSPECTS, AND TRACE THE ORIGIN OF CRIMINAL PHOTOS.

MEDICAL IMAGING 🏥

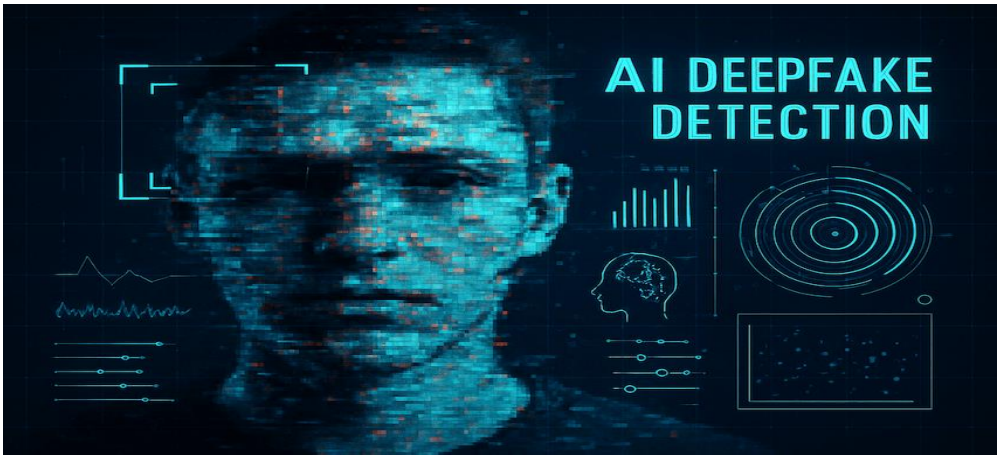
IN HEALTHCARE, IMAGE AUTHENTICITY IS LIFE-OR-DEATH. MEDICAL IMAGE AUTHENTICATION USES ADVANCED TECHNIQUES LIKE WAVELET PACKET ANALYSIS AND ENERGY ENTROPY TO ENSURE DIAGNOSTIC IMAGES HAVEN'T BEEN ALTERED. THIS PREVENTS INSURANCE FRAUD WITH FAKE MEDICAL IMAGES, ENSURES DIAGNOSTIC ACCURACY THROUGH WATERMARKING TECHNIQUES, AND PROTECTS PATIENT PRIVACY WITH EMBEDDED AUTHENTICATION.

JOURNALISM & MEDIA VERIFICATION 📰

IN THE ERA OF FAKE NEWS, JOURNALISTS RELY ON FORENSIC TOOLS TO VERIFY SOURCE AUTHENTICITY OF VIRAL IMAGES, DETECT DEEPFAKES AND AI-GENERATED CONTENT, FACT-CHECK VISUAL CLAIMS, AND MAINTAIN JOURNALISTIC INTEGRITY.

SOCIAL MEDIA & CYBERSECURITY 🌐

PLATFORMS USE IMAGE FORENSICS TO IDENTIFY DEEPFAKE VIDEOS, DETECT MISINFORMATION CAMPAIGNS, PROTECT USER IDENTITY FROM MORPHING ATTACKS, AND COMBAT REVENGE PORN AND IMAGE-BASED HARASSMENT.



AI DEEPFAKE DETECTION CONCEPT ILLUSTRATING DIGITAL FORENSIC TECHNOLOGY WITH HIGH-TECH VISUALS

THE CUTTING-EDGE TECHNIQUES USED TODAY 🚀

AI AND MACHINE LEARNING REVOLUTION

2025 HAS BROUGHT INCREDIBLE ADVANCEMENTS IN FORENSIC TECHNOLOGY. DEEP LEARNING MODELS CAN DETECT MANIPULATIONS WITH EXCEPTIONAL ACCURACY, AUTOMATED ANOMALY DETECTION INSTANTLY FLAGS SUSPICIOUS PATTERNS HUMANS MIGHT MISS, AND SPECIALIZED FILTERS IDENTIFY FACES GENERATED BY GENERATIVE ADVERSARIAL NETWORKS.

AI AND MACHINE LEARNING ARE AT THE FOREFRONT OF THE DIGITAL FORENSICS REVOLUTION. THESE TECHNOLOGIES DRAMATICALLY ENHANCE INVESTIGATORS' ABILITY TO PROCESS AND ANALYZE LARGE VOLUMES OF DATA QUICKLY AND EFFICIENTLY. AI ALGORITHMS HELP INVESTIGATORS UNCOVER PATTERNS IN SEEMINGLY UNRELATED DATA, SPOT NEW CYBERATTACK STRATEGIES, AND PREDICT THE BEHAVIOR OF SUSPECTS BASED ON DIGITAL FOOTPRINTS.

BLOCKCHAIN AUTHENTICATION

SOME ORGANIZATIONS NOW USE BLOCKCHAIN TECHNOLOGY TO CREATE IMMUTABLE RECORDS OF IMAGE AUTHENTICITY. ONCE AN IMAGE IS REGISTERED ON THE BLOCKCHAIN, ANY TAMPERING BECOMES IMMEDIATELY DETECTABLE—LIKE A DIGITAL SEAL THAT CAN'T BE BROKEN.

DIGITAL WATERMARKING

FRAGILE WATERMARKS EMBEDDED IN IMAGES ACT LIKE SECURITY SEALS. IF SOMEONE TRIES TO TAMPER WITH THE IMAGE, THE WATERMARK BREAKS, IMMEDIATELY ALERTING INVESTIGATORS. THIS TECHNIQUE INTEGRATES SCHUR DECOMPOSITION AND DISCRETE WAVELET TRANSFORM (DWT) FOR WATERMARK EMBEDDING, ENSURING ROBUSTNESS AGAINST ATTACKS. IT'S ESPECIALLY CRUCIAL FOR MEDICAL IMAGES AND LEGAL DOCUMENTATION.

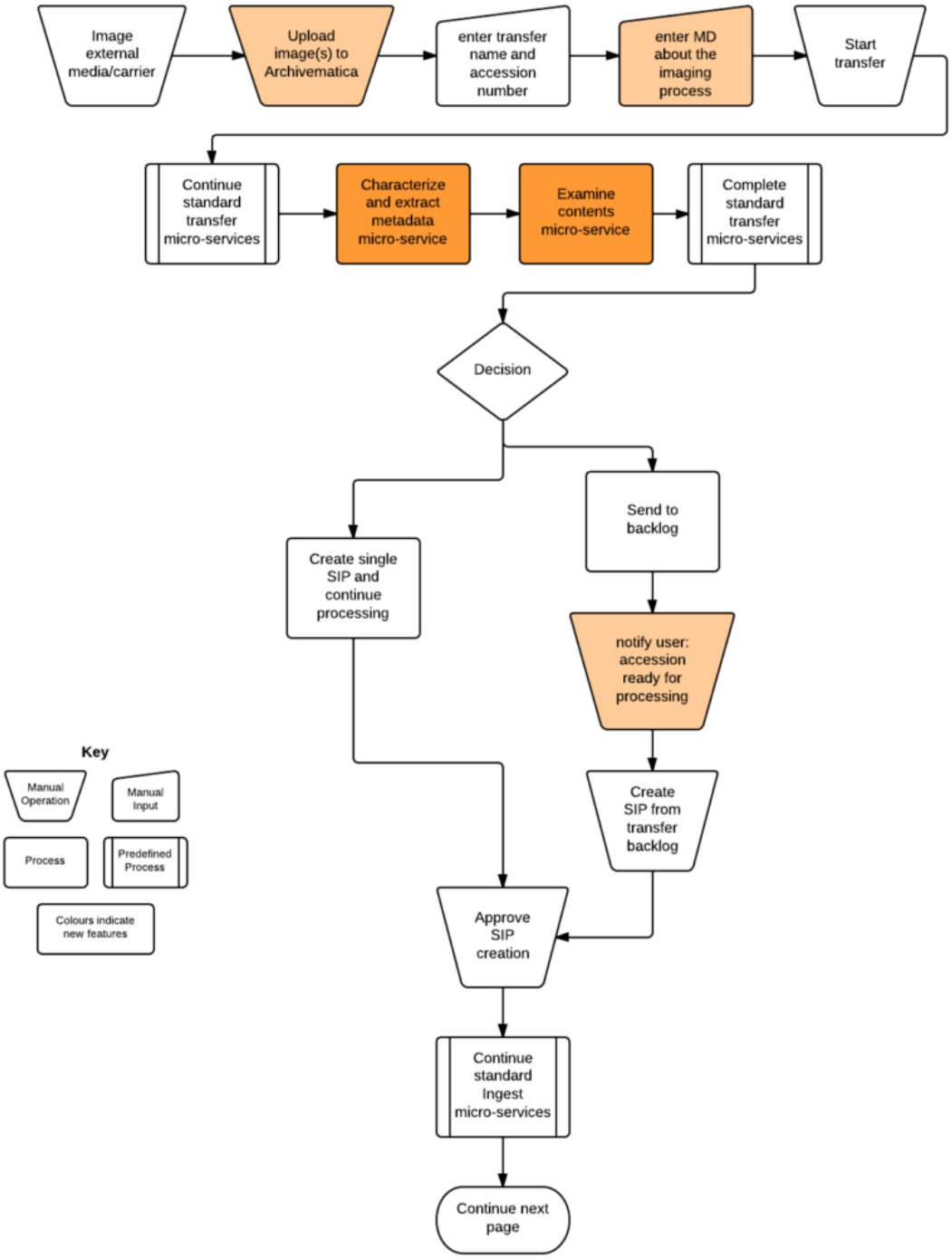


Image external media/carrier
Upload image(s) to Archivematica
enter transfer name and accession number
enter MD about the imaging process
Start transfer
Continue standard transfer micro-services
Characterize and extract metadata micro-service
Examine contents micro-service
Complete standard transfer micro-services
Decision
Send to backlog
Create single SIP and continue processing
notify user: accession ready for processing
Create SIP from transfer backlog
Approve SIP creation
Continue standard Ingest micro-services
Continue next page
Key
Manual Operation
Manual Input
Process
Predefined Process
Colours indicate new features

WORKFLOW DIAGRAM SHOWING DIGITAL IMAGE INGEST AND PROCESSING STEPS IN A DIGITAL FORENSICS ENVIRONMENT USING ARCHIVEMATICA

POPULAR FORENSIC TOOLS USED BY PROFESSIONALS 🛠️

FTK IMAGER

A FREE, POWERFUL TOOL FOR CREATING FORENSIC IMAGES AND PREVIEWING DIGITAL EVIDENCE WITHOUT ALTERING ORIGINAL DATA. IT'S THE SWISS ARMY KNIFE OF DIGITAL FORENSICS. FTK IMAGER CAN CREATE PERFECT COPIES (FORENSIC IMAGES) OF COMPUTER DATA WITHOUT MAKING CHANGES TO THE ORIGINAL EVIDENCE, INCLUDING FILE SLACK AND UNALLOCATED SPACE.

AMPED AUTHENTICATE

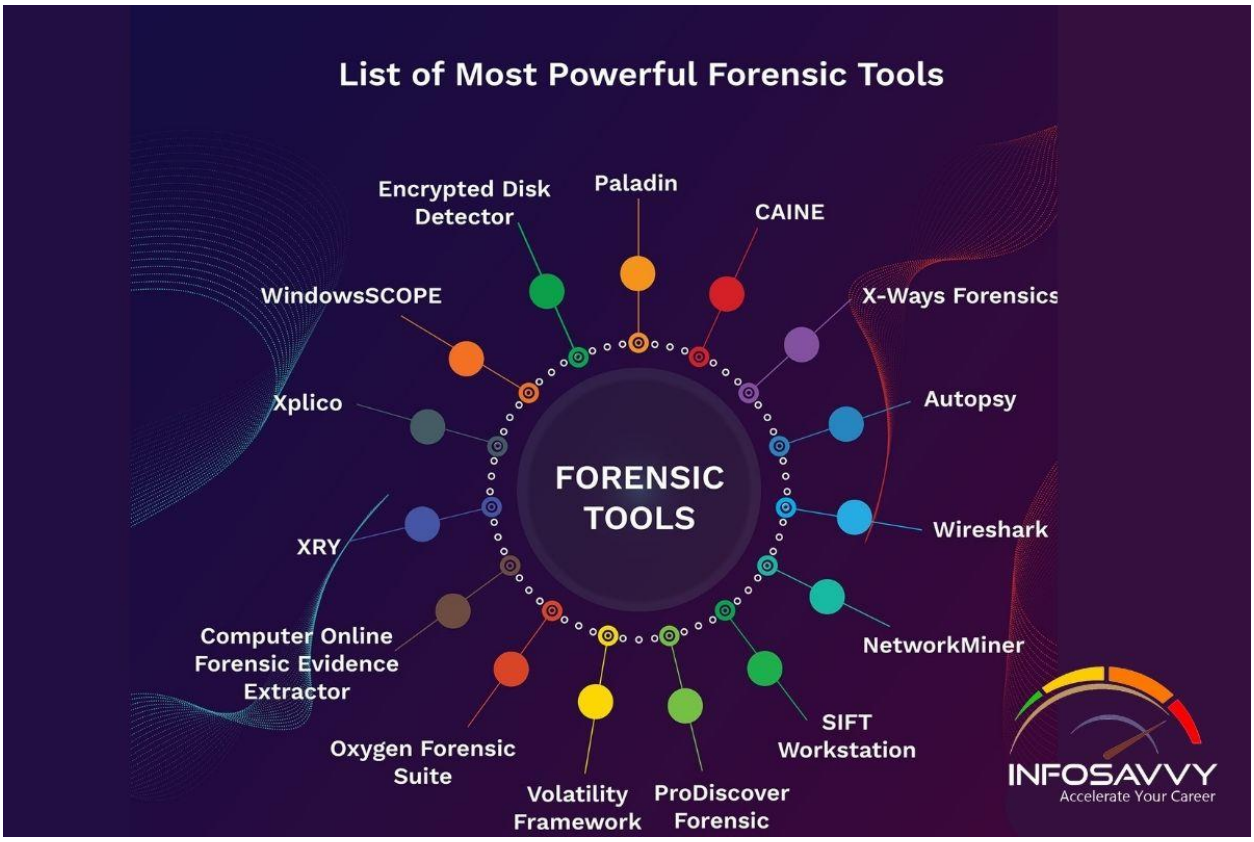
THE MOST COMPLETE SOFTWARE FOR PHOTO, VIDEO, AND DEEPFAKE FORENSICS. IT PERFORMS ADVANCED AUTHENTICATION, DETECTS MANIPULATIONS, AND IDENTIFIES SOURCE DEVICES THROUGH SENSOR ANALYSIS. THE SOFTWARE INCLUDES OVER 40 TOOLS AND FILTERS THAT AID IN THE ENTIRE AUTHENTICATION WORKFLOW, FROM INTEGRITY ANALYSIS TO CONTENT TAMPERING ANALYSIS AND DEEPFAKE DETECTION.

AUTOPSY & THE SLEUTH KIT

OPEN-SOURCE DIGITAL FORENSIC PLATFORMS USED BY LAW ENFORCEMENT WORLDWIDE FOR ANALYZING DIGITAL EVIDENCE.

ALETHEIA & STEGEXPOSE

SPECIALIZED TOOLS FOR DETECTING STEGANOGRAPHY—HIDDEN MESSAGES CONCEALED WITHIN IMAGES. ALETHEIA OFFERS A NOVEL APPROACH BY IMPLEMENTING STATE-OF-THE-ART MACHINE LEARNING TECHNIQUES FOR STEGANALYSIS.



CIRCULAR INFOGRAPHIC LISTING POWERFUL FORENSIC TOOLS USED IN DIGITAL INVESTIGATIONS, SUCH AS PALADIN, CAINE, AND WIRESHARK

THE CHALLENGES FORENSIC EXPERTS FACE 😰

DESPITE AMAZING TECHNOLOGICAL ADVANCES, DIGITAL FORENSICS ISN'T WITHOUT OBSTACLES. COMPUTATIONAL COMPLEXITY REQUIRES MASSIVE PROCESSING POWER FOR AI MODELS. HACKERS DEVELOP ADVERSARIAL ATTACKS AND TECHNIQUES TO BYPASS FORENSIC DETECTION. ANALYZING MILLIONS OF IMAGES IN REAL-TIME PRESENTS SCALABILITY ISSUES. PRIVACY CONCERNS REQUIRE BALANCING SECURITY NEEDS WITH INDIVIDUAL PRIVACY RIGHTS. AND AS DETECTION IMPROVES, SO DO DEEPFAKE MANIPULATION TECHNIQUES.

THE FUTURE IS HERE: WHAT'S COMING NEXT? 🔮

THE DIGITAL FORENSICS LANDSCAPE IS EVOLVING RAPIDLY. QUANTUM CRYPTOGRAPHY PROMISES NEXT-GENERATION SECURITY FOR IMAGE AUTHENTICATION. EXPLAINABLE AI (XAI) WILL PROVIDE TRANSPARENT FORENSIC DECISION-MAKING THAT EXPERTS CAN UNDERSTAND AND EXPLAIN IN COURT. REAL-TIME DETECTION WILL ENABLE INSTANT VERIFICATION AS IMAGES ARE CAPTURED. IOT FORENSICS WILL ANALYZE IMAGES FROM SMART HOME DEVICES, WEARABLES, AND CONNECTED CAMERAS. AND 5G INTEGRATION WILL ALLOW TRACING COMMUNICATIONS THROUGH HIGH-SPEED NETWORKS.

WHY THIS MATTERS TO YOU 💡

YOU MIGHT THINK FORENSIC IMAGE ANALYSIS ONLY MATTERS TO LAW ENFORCEMENT, BUT IT AFFECTS EVERYONE. YOUR SOCIAL MEDIA PHOTOS COULD BE USED WITHOUT PERMISSION. YOUR MEDICAL RECORDS NEED PROTECTION FROM TAMPERING. YOUR NEWS CONSUMPTION SHOULD BE BASED ON VERIFIED IMAGES. YOUR LEGAL RIGHTS MIGHT DEPEND ON AUTHENTIC VISUAL EVIDENCE.

UNDERSTANDING DIGITAL IMAGE FORENSICS EMPOWERS YOU TO BE MORE CRITICAL OF THE IMAGES YOU SEE AND SHARE ONLINE.

ILLUSTRATION OF DIGITAL FORENSIC INVESTIGATION SHOWING A PERSON ANALYZING DATA ON A LAPTOP WITH SECURITY SHIELD AND MAGNIFYING GLASS

THE BOTTOM LINE 🎯

DIGITAL IMAGE PROCESSING HAS REVOLUTIONIZED FORENSIC SCIENCE, TRANSFORMING IT FROM A MANUAL, TIME-CONSUMING PROCESS INTO A HIGH-TECH, AI-POWERED DISCIPLINE. IT'S THE INVISIBLE GUARDIAN PROTECTING TRUTH IN OUR INCREASINGLY DIGITAL WORLD.

FROM DETECTING MEDICAL FRAUD TO CATCHING CRIMINALS, FROM VERIFYING NEWS TO PROTECTING YOUR IDENTITY—DIGITAL IMAGE FORENSICS IS EVERYWHERE, WORKING SILENTLY BEHIND THE SCENES.

THE NEXT TIME YOU SEE A VIRAL IMAGE ONLINE, REMEMBER: SOMEWHERE, THERE'S TECHNOLOGY CAPABLE OF TELLING WHETHER IT'S REAL OR FAKE. AND THAT TECHNOLOGY IS CONSTANTLY EVOLVING, STAYING ONE STEP AHEAD OF THOSE WHO TRY TO DECEIVE.

THE FUTURE OF TRUTH LIES IN PIXELS, ALGORITHMS, AND THE BRILLIANT MINDS WHO KEEP PUSHING FORENSIC SCIENCE FORWARD. AND HONESTLY? THAT'S PRETTY EXCITING! 🚀

WANT TO LEARN MORE? 🧩

DIGITAL IMAGE FORENSICS IS A RAPIDLY GROWING FIELD WITH ENDLESS OPPORTUNITIES. WHETHER YOU'RE INTERESTED IN CYBERSECURITY, LAW ENFORCEMENT, JOURNALISM, OR JUST FASCINATED BY TECHNOLOGY, THIS FIELD WELCOMES CURIOUS MINDS.

THE TRUTH IS OUT THERE—HIDDEN IN PIXELS, WAITING TO BE DISCOVERED. ARE YOU READY TO FIND IT? 🔍✨