Western European Journal of Modern Experiments and Scientific Methods
Volume 2, Issue 7, July, 2024
https://westerneuropeanstudies.com/index.php/1
ISSN (E): 2942-1896 Open Access| Peer Reviewed

MODERN METHODS OF INVESTIGATION AGAINST FORGERY OF ELECTRONIC DOCUMENTS

Sabirova Muhabbat Akramovna
Ministry of Internal Affairs of the Republic of Uzbekistan
Main forensic center
Senior expert of the Main Expert Forensic Center

Abstract: This article examines the main problems associated with forgery of electronic documents and the importance of implementing reliable investigative methods to solve this problem. It explores the various modern techniques and tools available to investigate the forgery of electronic documents, and by understanding and using these advanced investigative techniques, authorities and organizations can effectively protect the integrity and authenticity of electronic documents.
Key words: electronic documents, forgery, modern technologies, protection, techniques, manipulation.

Introduction.
Forgery of electronic documents is a serious problem today that can have negative consequences. As technology advances, so do the ways in which malicious individuals can create and manipulate electronic files for fraudulent purposes. In order to combat this threat, modern methods of anti-forgery verification of electronic documents have been developed. These methods use advanced technology and forensic methods to identify, prevent and prosecute those involved in the forgery of electronic documents.

Literature Analysis And Research Methodology
Digital forensics is an important tool in the investigation of forgery of electronic documents. Digital forensics experts use specialized software and techniques to analyze evidence of tampering or manipulation of digital devices and storage media. By examining metadata, file timestamps, and other digital artifacts, forensic experts can reconstruct the chain of events involved in the creation and alteration of electronic documents.[2]
Metadata contains valuable information about the history and provenance of electronic documents. Researchers can analyze metadata to determine when a document was created, modified, or accessed. Inconsistencies in metadata timestamps or inconsistencies in file properties can indicate potential forgery or tampering. Blockchain technology offers a secure and immutable way to store and verify electronic documents. By using Blockchain's decentralized and immutable ledger, organizations can create a transparent record of document transactions. Any changes made to a document stored on the blockchain are recorded and can be traced back to the source, making it difficult to alter forged documents without detection. Digital signatures use cryptographic algorithms to verify the identity of the signer and ensure the integrity of electronic documents. [1]
By digitally signing a document, the signer creates a unique cryptographic hash that can be verified to confirm the authenticity of the document. Digital signatures provide a strong layer

Western European Journal of Modern Experiments and Scientific Methods
Volume 2, Issue 7, July, 2024
https://westerneuropeanstudies.com/index.php/1
ISSN (E): 2942-1896 Open Access| Peer Reviewed

of security against forgery and unauthorized modification. Special document analysis tools and software can be used to check electronic documents for signs of forgery. These tools analyze document properties such as fonts, formatting, and content and identify inconsistencies or changes that may indicate a breach. Document analysis tools play a crucial role in uncovering hidden traces of forgery and ensuring the integrity of electronic documents. Cryptographic hash functions create unique digital fingerprints of electronic documents based on their content. By generating a hash value for a document, investigators can create a digital fingerprint that uniquely identifies the file. Changes to the document result in a different hash value, which allows investigators to detect any unauthorized changes or forgery attempts.[3]

Discussion And Results

Blockchain technology helps prevent counterfeiting of electronic documents by providing a secure and tamper-proof system for verifying the authenticity and integrity of digital records. One of the main characteristics of blockchain is immutability, which means that once a transaction or record is added to the block and confirmed by the network, it cannot be changed or deleted. This feature ensures that electronic documents stored on the blockchain are tamper-proof and resistant to unauthorized changes. Blockchain works on a network of decentralized nodes that jointly confirm and record transactions. This distributed architecture eliminates the need for a central authority or intermediary, reducing the risk of a single failure and unauthorized modification. Decentralization increases the security and reliability of electronic documents stored on the blockchain. Blockchain uses cryptographic hash functions to create a unique digital fingerprint (hash) for each block of data. Any change in the content of the document results in a different hash value and alerts users to possible corruption. By comparing hash values, users can verify the integrity of electronic documents and identify unauthorized changes. Smart contracts are self-executing contracts encoded on the blockchain that automatically enforce predetermined rules and conditions. [4]

Organizations can use smart contracts to create digital contracts, validate documents, and automate verification processes. Smart contracts increase transparency, reduce human error, and ensure the integrity of electronic documents in the blockchain ecosystem. Blockchain technology allows users to timestamp electronic documents and establish proof of existence at a particular point in time. By pinning document hashes to the blockchain, users can demonstrate the creation and authenticity of records, providing a reliable audit trail for legal and regulatory purposes. Time stamps increase the reliability and evidentiary value of electronic documents. Blockchain networks can be configured with permissioned access controls that allow authorized parties to view and inspect electronic documents while limiting unauthorized access. Audit trails stored on the blockchain record every transaction and interaction, providing traceability and accountability for document changes. Authorized access increases data security and privacy in document management. Blockchain networks rely on consensus mechanisms such as proof-of-work or proof-of-stake to validate transactions and ensure agreement between network participants. By cross-verifying document transactions across multiple nodes, blockchain technology establishes consensus on the correctness and authenticity of electronic documents, reducing the risk of forgery and fraud.[5]

Conclusion.

In summary, modern anti-forgery investigative techniques combine technological innovation, forensics, and analytical rigor to combat fraudulent activity in the digital realm. Using advanced technologies such as digital forensics, blockchain, digital signature, and document

Western European Journal of Modern Experiments and Scientific Methods
Volume 2, Issue 7, July, 2024
https://westerneuropeanstudies.com/index.php/1
ISSN (E): 2942-1896 Open Access| Peer Reviewed

analysis tools, investigators can improve their ability to identify, prevent, and prosecute individuals involved in electronic document forgery. These methods play a crucial role in protecting the integrity and authenticity of electronic documents today.

References.

1. 1.Kriminalistika. Darslik 1-jild. -T.: O'zbekiston Respublikasi Milliy gvardiyasi Harbiy-texnik instituti, 2018.-447 b.[1]
2. 2.Kriminalistika. Darslik 2-jild. -T.: O'zbekiston Respublikasi Milliy gvardiyasi Harbiy-texnik instituti, 2018. -365 b;[2]
3. 3.Mamatkulov T.B., Astanov I. va boshqa. Kriminalistika: Darslik. - T.: O'zbekiston Respublikasi IIV Akademiyasi, 2015. -B. 498;[3]
4. M.F.Ergashev, M.H.Obidov, Sh.P Alaev. Tergovchi.Qo'llanma. T: "G'afur G'ulom matbaa ijodiy uyushmasi;[4]
5. 5.I.R.Astanov. Jinoyat ishlari bo'yicha maxsus bilimlardan foydalanishning protsessual va kriminalistik jihatlari. Monografiya. T:2018-yil;[5]
6. Approaches for Forgery Detection of Documents in Digital Forensics: A Review | SpringerLink