Journal of Advanced Zoology
ISSN: 0253-7214
Volume 44 Issue S-7 Year 2023 Page 1954-1965

Encryption In Forensic Science: A Concrete Analysis Of The Paradigm Using Bibliometric Data In Web Of Science From 1995 To 2022

Isaac Atta Senior Ampofo[1*], Francis Oppong-Twum[2], Desire Mawuko Komla Ayite[3], Emil Anthony Kobina Jnr[4], Eugene Louis Batie Badzongoly[5]

[1*]*University of Liverpool, Brownlow Hill, Liverpool, United Kingdom, ampofoisaac10@yahoo.com*
[2]*Department of Computer Science, University of CapeCoast, Ghana, francis.oppongtwum@ucc.edu.gh*
[3]*Department of Mathematics and ICT, Kibi Presbyterian College of Education, Kibi, Ghana, dmkayite@kpce.edu.gh*
[4]*Department of Computer Science, Takoradi Technical University, Ghana, anthonykemiljnr@gmail.com*
[5]*Department of Computer Science, Ghana Communication Technology, University, Accra, Ghana, ebadzongoly@gctu.edu.gh*

[*]***Corresponding Author:*** *Isaac Atta Senior Ampofo*
[*]*University of Liverpool, Brownlow Hill, Liverpool, United Kingdom, ampofoisaac10@yahoo.com*

Article History

Received: 26 March 2023
Revised: 12 July 2023
Accepted:29 July 2023

Abstract

The use of encryption technologies is becoming increasingly common at both organizational and individual levels for a variety of reasons. The need to protect the confidentiality of sensitive information is the factor that receives the most attention. Sadly, it is also often used by cybercriminals as a means of evading the reach of investigations by digital forensics. Most of the time, access to such info contained therein is restricted by indirect storage device encryption or the direct encryption of data. As a result, in 60% of these cases, the investigation team of the forensics and later the trial have little to no proof to use. But it is inconceivable to risk the advancements in information security made possible by encryption technology in favor of digital forensics. This study's goal is to give a thorough analysis of the research papers that make up the existing literature. The data utilized for the research was mined from the Web of Science in the encryption and forensic science areas in many fields of study by using bibliometric literature analysis via the viewer of VOS. The study presented the most prominent papers and revealed literature gaps for future studies.

Keywords: Encryption, Forensic, Bibliometric, VoS viewer

1. INTRODUCTION

Many nations have passed laws allowing wired interception or/and wireless communications, the disclosure and acquisition of communications-related data, and tool acquisition for accessing or decrypting encrypted electronic data because of concerns about terrorism and organized crime [1]. For instance, Section Three of the Regulation of Investigatory Powers Act (RIPA), which deals with terror suspects, came into effect in the UK in 2008 and permits police to request keys of encryption or be given encrypted text's clear text transcript that has been transmitted or stored across networks of mobile phones. Steganography, a technique used by criminals to conceal messages in files or documents so that others cannot read them, has been around for a while. However, steganography usage to conceal proof of illegal conduct, however, has become ineffective due to improvements in forensic techniques and detection steganography tools, where laptops may be inspected. The interest in deniable encryption techniques and methods has increased as police response to occurrences has shifted from reactive to proactive, along with risk management. By using an algorithm, encryption transforms useful data, called plaintext, into a hidden format, known as the ciphertext (cipher). A key is used by encryption algorithms to obfuscate data (encryption) and recover the plaintext (decryption). To defend data encrypted, the decryption key just needs to be kept secret because good current algorithms make it impossible to retrieve the plaintext from the ciphertext without knowing the key decryption. They also make it difficult to distinguish the ciphertext from random data, making it difficult to demonstrate the use of encryption [2], [3]. Due to these factors, encryption is one of the best ways to hide information and is being utilized by thieves to hide their data more frequently. Additionally, it is utilized by regular people and organizations to reduce the possibility that personally identifiable information will wind up in the wrong hands, such as when a laptop is stolen. [4]. This study tries to give a thorough review of the most recent forensic science studies on encryption. This article’s key objective is to present a survey of contemporary research strands and topics on encryption in forensic science and to show existing research, identify current trends, and establish the thematic evolution of these topics.

2. LITERATURE REVIEW

The pioneering study on encryption deniable was written by Canetti et al. [5]. To safeguard wired or wireless communications against passive eavesdropping, researchers have up to that time concentrated on encryption for semantic passive security. At the time, [5] thought that generally recognized cryptographic procedures fell short of offering the required level of safety in scenarios where a consumer was forced to disclose their keys of encryption due to stress or coercion. Their study was intended to present a deniable encryption idea, which would allow a user to create fictitious random selections that would make the text cipher appear to be a dissimilar cleartext’s encryption while concealing the true cleartext. Karsten [6] covers 2 deniable encryption methods: Deniability, a software based on a static, interleaved algorithm, and TrueCrypt, an open-source free deniable encryption suite. A secure deniable file system using TrueCrypt version 5.1a was the subject of more recent research by Czeskis et al. [7]. The paper describes how the deniability of TrueCrypt is compromised by the operating systems of Windows Vista, Google Desktop, and Microsoft Word, and then offers various solutions for overcoming the difficulties presented by current operating systems in retaining deniability. The paper's authors demonstrate that "deniability, even under a very weak model, is fundamentally problematic" and that the operating system's default processes can "leak significant information outside the deniable volume." To conceal the existence of encrypted files, Oler and Fray [8] examined deniable file system usage. They examined the most significant developments in the steganographic file systems field. Nonetheless, they believe that each system they looked at has significant flaws.

BestCrypt [9] is a commercial data encryption system that works on Linux and Windows platforms and offers plausible deniability through hidden container usage. Several cipher techniques and cryptographic hashes are supported by BestCrypt. GOST, SHA-256, and SHA-1 hash algorithms are all supported. Blowfish, AES, CAST, RC-6, GOST 2814789, Twofish, and Serpent are some examples of ciphers. As security expands, BestCrypt's modular design enables the integration of hardware or software for encryption developed by third parties. FreeOTFE [10] is a free transparent disk onthe-fly encryption tool that runs on Windows Mobile 2005/2003, Microsoft Windows Vista/XP/2000 platforms, and Windows Mobile 6. It is also compatible with PDAs, mobile phones, and other devices with the Windows Mobile operating system. More than one volume or virtual disk can be created with FreeOTFE, and anything written to them is encrypted automatically before being placed on the hard drive of the computer. File-based or partition-based encrypted volumes are both possible. Several cipher algorithms and cryptographic hashes are supported by FreeOTFE. Some examples of hash algorithms are MD4, MD2, SHA-1, MD5, RIPEMD-160, SHA-512, Whirlpool, and Tiger. AES 128, 192, and 256, Blowfish, 6 & CAST5, 3DES, DES, RC-6, MARS, Twofish, and Serpent are some of the ciphers available. FreeOTFE's modular architecture enables the development of third-party drivers that integrate new cipher/hash algorithms. Like FreeOTFE, TrueCrypt [11] is a software program for creating and managing an encrypted volume "on the fly." Decrypted data is only ever momentarily stored in RAM by TrueCrypt instead of being saved to disk. In the volume, data stored is still encrypted once it is mounted. The volume is dismounted upon restarting Windows, making the files on it encrypted and inaccessible. The following hash algorithms are supported by TrueCrypt: Whirlpool, RIPEMD-160, and SHA512. The following algorithms of cipher are supported by TrueCrypt: AES 256, Serpent, and Twofish, as well as combinations of these three. A hidden operating system and hidden volumes are two plausible deniability types that TrueCrypt provides. A filesystem for Linux operating systems called PhoneBookFS [12] provides encryption with features for plausible deniability. Supported encryption and hash techniques include 256-bit Blowfish and SHA-1, respectively. To make it impossible or difficult for a contender to ascertain the full compliance of a user with decryption requirements, encrypted volumes are used by PhoneBook with various levels of encryption and "chaffing." Rubberhose [13], the first successful deniable cryptography tool, is a free disk system of encryption that enables encrypted data concealment. Currently, Linux and NetBSD are the platforms on which Rubberhose runs. Rubberhose supports the following cipher algorithms: 3DES, DES, RC-6, IDEA, Blowfish, CAST, and Twofish. Rubberhose supports every symmetric algorithm from the most recent OpenSSL release, in addition to the built-in ciphers. Rubberhose's modular architecture makes it simple to include new algorithms.

By recording stub instruction combinations, anti-virus software employs signatures as one of its tools to identify known infections. However, this is challenging [14] since viruses frequently "evolve" or employ challenging polymorphic obfuscation tactics [15]. As a result, anti-virus software was developed to track API calls to analyze viral behavior. A phylogenetic tree is suggested by Wagener et al. [16] to detect behaviors of related malware centered on API calls and the systems they make. Malware can be recognized by the behavior of its API calls, but it might be challenging to detect algorithmic behavior using the same method. According to Rhee et al. [17], malware can be identified by profiling its data object access behavior. He uses the method to find rootkits and asserts that it produces no false positives on kernels that are not infected. Their work and ours share some minor parallels in that we do not investigate calls of API, but their focus is on creating better malware signatures, while ours is on recognizing certain algorithmic behavior and then extracting encryption keys. Regardless of the packaging method employed, a substantial amount of work has been done on automatically unpacking and recognizing malware. Omniunpack [18] and PolyUnpack [19] assume that packers exhibit behavior that is somewhat comparable, as evidenced, for instance, by a dynamic memory page execution that enables the entry point and unpacker identification. According to Lyda [20], packed executables should be distinguished based on the entropy degree in their code section. In contrast to packed code, which frequently seems random, code portions typically have low entropy. Potentially, code that alters the entropy of memory might be recognized using this technique, potentially permitting code section identification that uses cryptography. However, manual analysis would still be necessary to determine the precise procedure and extract the key.

The authors of [21] examine numerous methods for resolving issues using encrypted evidence and explain why they might not work. They outline many techniques for opening encrypted disks: swaying the suspect into giving up the main detecting data copies unencrypted. Locate passphrases or keys sophisticated password attacks utilizing application weaknesses surveillance using software or hardware Nevertheless, they add that "excellent product design and disciplined use can negate most of these strategies" [21]. As a result, we need to find other solutions. One method is to get an image of a disk while the system computer is still powered on and operational and the encrypted containers or disks are mounted. This method also has significant drawbacks, some of which are listed in [21]; for instance, it violates forensic computing concepts like repeatability and verifiability. A complete image of the decrypted data may occasionally be impossible or impractical to build [21]. Another option is to get the encryption keys back. A secured disk can be decrypted using some encryption software, such as BitLocker, by linking the drive to a forensic analysis machine read-only [22]. However, most encryption tools do not support it. Recently, several studies that discuss the potential for getting keys of encryption from the system's memory or from a live picture of the system’s volatile memory were released. According to van Someren and Shamir, keys have a greater entropy than the other memory contents, and this property can be utilized to search for the keys [23]. However, because other random data (such as compressed files) may be present in memory, the approach may produce false-positive findings [24]. The authors of [25] suggest that to extract the key master from a variable in a readily recognizable data structure, one or more of the data structures of the operating system needs to be parsed. This necessitates a thorough knowledge of the fundamental operating system. This approach’s drawback is that it requires access to the kernel and application source codes [21]. The method of linear scan for recovery of keys is provided in [21] as an alternate strategy. The authors discovered that the entire block, including the auxiliary and main keys, has an identifiable layout. Each block of 64 bytes was thought to be a potential location for the primary and auxiliary encryption keys in the software they designed, which slowly passes the full memory image. The first encrypted block volume is decrypted using these potential keys. The system has been decrypted successfully and the encryption keys have been located if the first block’s decrypted value is according to values that relate to the file system FAT16. While the method described in [25] covers TrueCrypt 4.2a created for Windows XP, this work solely interacts with version 4.1 of TrueCrypt. In contrast to the current TrueCrypt 7.0a version, which uses the encryption mode of XTS, those Truecrypt versions only support LWR (Liskov, Rivest, and Wagner) and CBC (Cipher Block Chaining) mode. Because so many encryption keys are utilized, it is necessary to note the significance of the encryption mode. The secondary and primary keys are the two encryption keys used by the XTS mode.

Additionally, the memory structure data parsing method and the linear scan are vulnerable to a dishonest attacker, as stated in [25]. It is likely to evade linear scanning and list-walking methods using a few basic strategies. The linear scan method's dependence on keys being stored in memory according to regular patterns is another drawback. Therefore, the current study offers research trends and future research in forensic science and encryption.

3. METHODOLOGY

The authors used Google Books Ngram Viewer to present a graphical representation of how often the terms “encryption” and “forensic” have been used in the literature.

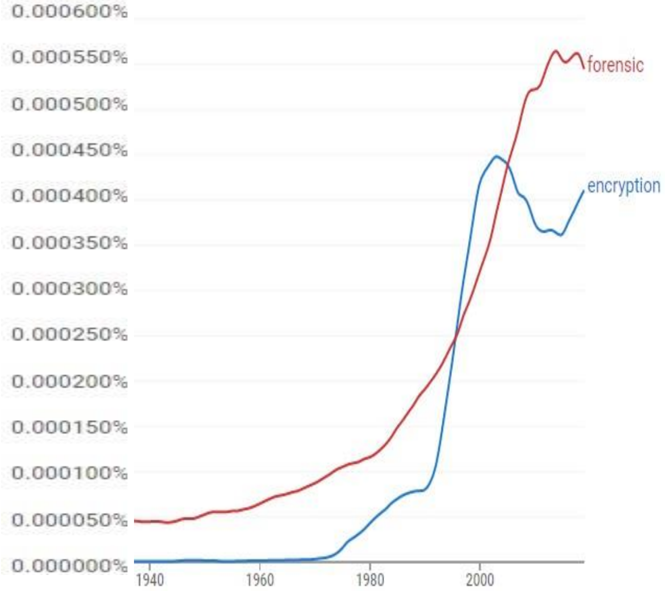

Fig 1. Graphical representation of “encryption” and “forensic” in literature

Fig. 1 shows that there is a point of intersection between 1995 and 2005 on encryption and forensics. From 1800 to 1980, encryption and forensics were not done. Hence, for more profound research, the authors searched for literature from 1995. The authors used the Web of Science database to extract bibliographic data because of its advantages over other bibliographic databases such as Scopus and PubMed. The literature on encryption in forensic science published from 1995-01-01 to 2022-07-07 was skimmed in the Web of Science collection database. Some of the search terms used to find the most relevant book included "encryption" and "forensic," which were used as keywords in all fields. A sizable number of research publications were written and published internationally, according to Web of Science sources. For the papers that satisfied the requirements, year of publication, author, language, journal, title, keywords, counts of citations, abstract, document type, and affiliation were all exported into TXT format. The recovery happened on July 7, 2022. With the use of the VOS viewer, themes, cooccurrence, co-citation, citation, bibliographic coupling, and co-authorship were analyzed (version 1.6.18). The many papers identified for the research were 656, and the times cited included were 14,719, with an average document per item of 22.44 and an h-index of 64, with 716 total link strength. See Table 1 for the top documents with the most citations, with an average of more than 200 per year.

Table 1. Top documents with highest citations

Documents	Citations	Average per year
Lest We Remember: Cold-Boot Attacks on Encryption Keys	496	35.43
A Privacy-Preserving and Copy-Deterrence Content-Based Image Retrieval Scheme in Cloud Computing	494	70.57
Separable Reversible Data Hiding in Encrypted Image	397	36.09
Toward Efficient Multi-Keyword Fuzzy Search Over Encrypted Outsourced Data With Accuracy Improvement	365	52.14
Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption	360	36
Privacy-Preserving Deep Learning via Additively Homomorphic Encryption	319	63.8

HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing	275	25
Attribute-Based Encryption With Verifiable Outsourced Decryption	248	24.8
Security issues in cloud environments: a survey	205	22.78

4. RESULTS AND DISCUSSIONS

Bibliometric analysis of publication country

In the period from 1995 to July 7th, 2022, 656 publications on encryption and forensic science were found in the Web of Science database. The number of original research articles and cited papers is included in the total publication count. The results revealed that all the publications were published in 66 countries (see Fig. 2).

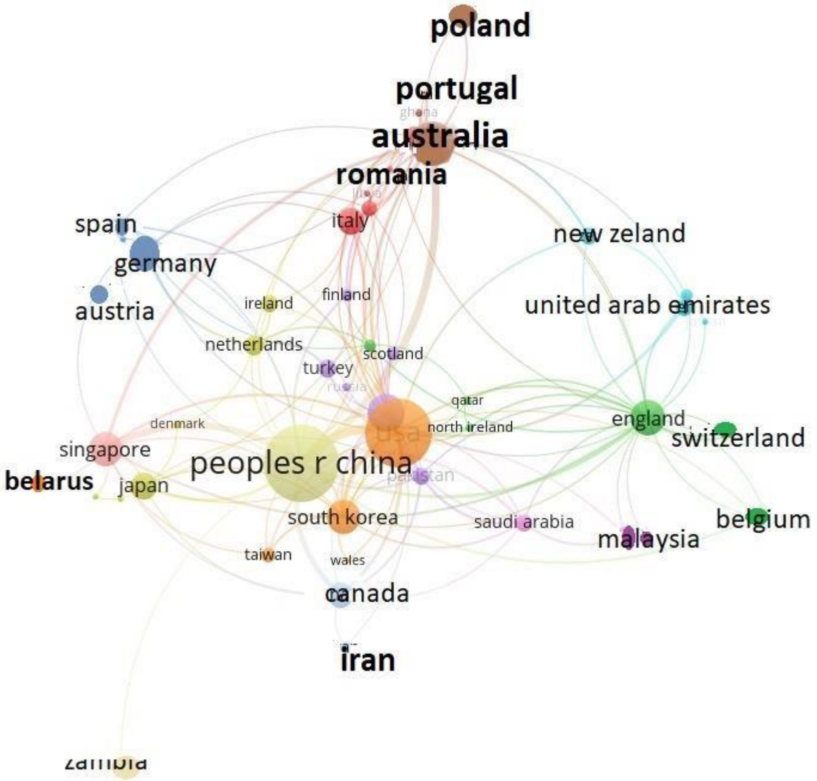

Fig 2. Network visualization for publications by country

The countries that appeared the most with the top total strength link were China, the United States of America (USA), and Australia. The other two countries that have predominantly contributed scholarly articles on encryption and forensic science are Singapore and England. Table 2 revealed that China had the highest total link strength of 150, representing 21% of the total link strength. China had the highest citations with 7619, representing 5.2% of the total citations. China also had the highest number of publications with 203, representing 31% of the total publications. See Table 2 for more details on nations with the top total strength link above ten.

Table 2. Highest nations with the top total strength link

Country	Documents	Citations	Total link strength
China	203	7619	150
USA	159	4831	98
Australia	67	2342	62
Singapore	39	1631	44
England	43	476	41
Canada	24	589	29
South Korea	41	492	25
Pakistan	11	77	18
Italy	26	780	17
Saudi Arabia	11	70	16
Netherlands	14	275	15

France	16	266	14
Germany	28	734	14
Japan	26	579	14
Greece	9	201	12
India	48	265	12

Bibliometric analysis of sources

The selected publications for the study were published in 244 sources (see Fig. 3).

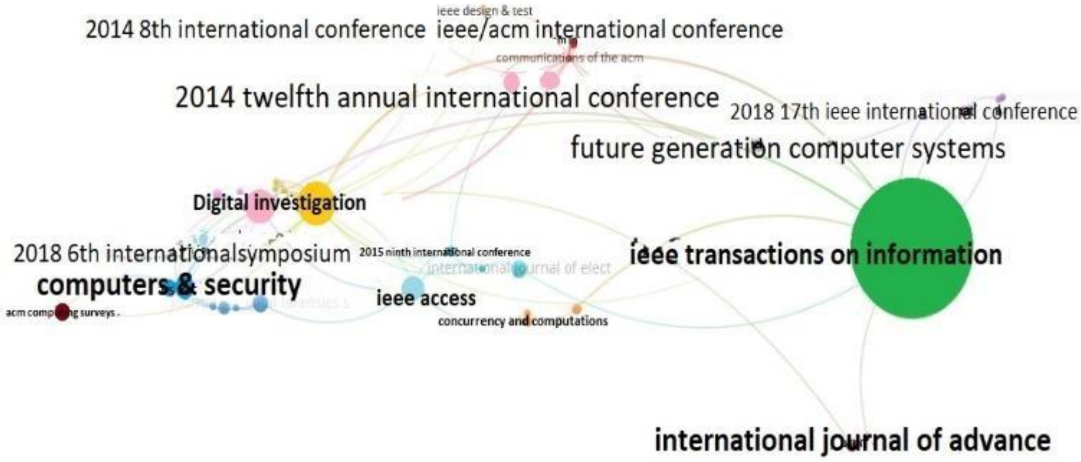
ieee design & test
2014 8th international conference
ieee/acm international conference
communications of the acm
2014 twelfth annual international conference
2018 17th ieee international conference
future generation computer systems
Digital investigation
2018 6th internationalsymposium
2015 ninth international conference
international journal of elect
ieee transactions on information
computers & security
ieee access
acm computing surveys
concurrency and computations
international journal of advance

Fig 3. Network visualization of source of publications

The results revealed that transactions of IEEE on security and information forensics had the highest publications with 304 documents representing 46.3%; the highest citations of 11898 representing 80.8%; and a total link strength of 43 representing 6% (see Table 3). Table 3 shows further information on the sources of the published documents with 10 or more total link strengths.

Table 3. Top five sources of publication

Source	Documents	Citations	Total link strength
Digital investigation	29	345	59
Forensic science international digital investigation	19	33	45
IEEE transactions on information forensics and security	304	11898	43
Communications of the ACM	1	496	22
Computers and security	5	50	10

Bibliometric analysis of research areas

Table 4 summarizes the findings of more than ten publications in the fields of encryption and forensic science. The results revealed that computer science had the highest publications with 594 documents representing 90.5%; 14344 times cited representing 97.5%; an average per item of 24.15; and an h-index of 63. This is followed by engineering with 413 documents representing 63%; 12425 times cited representing 84.4%; an average per item of 30.08; and h-index of 60. See Table 4 for further information.

Table 4. Top four research areas

Research area	Documents	Times cited	Average per item	h-index
Computer science	594	14344	24.15	63
Engineering	413	12425	30.08	60
Telecommunication	52	264	5.08	8
Optics	11	28	2.55	3

Bibliometric analysis of funding agencies

Table 5 presents the results of funding agencies for fifteen or more studies done on encryption and forensic science. The results revealed that the National Natural Science Foundation of China NSFc had the highest publications with 148 documents representing 22.6%; 6831 times cited representing 46.4%; an average per item of 46.16; and an h-index of 44. This is followed by the National Science Foundation (NSF) with 47 documents representing 7.2%; 2383 times cited representing 16.2%; an average per item of 50.7 and an h-index of 21. See Table 5 for further information.

Table 5. Top six funding agencies

Agency	Documents	Times cited	Average per item	h-index
National Natural Science Foundation of China Nsfc	148	6831	46.16	44
National Science Foundation Nsf	47	2383	50.7	21
Fundamental Research Funds for The Central Universities	23	962	41.83	13
National Key Research and Development Program Of China	20	298	14.9	7
Australian Research Council	18	678	37.67	12
European Commission	15	275	18.33	9

Bibliometric analysis of authors

Fig. 4 shows the results of authors with four or more publications. The total number of authors for the publications was 1804. Fig. 4 revealed that Susilo and Willy had the highest authorship.

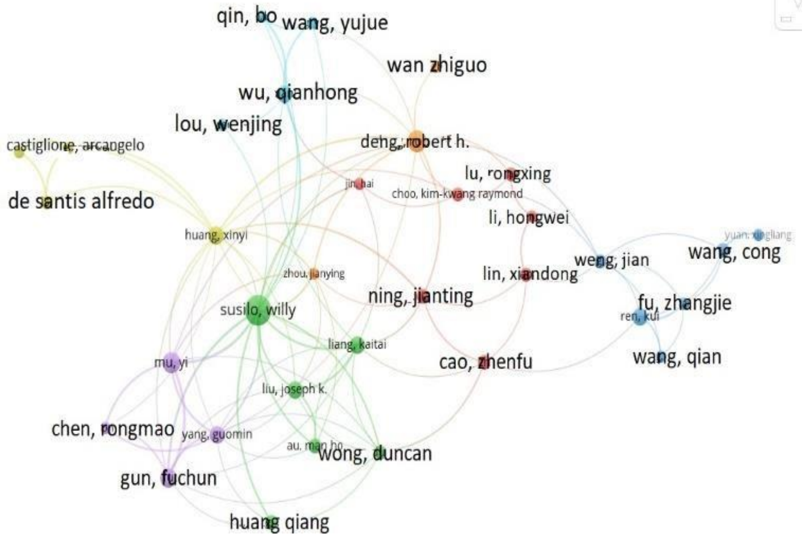

Fig 4. Network visualization of authors for documents published

Table 6 presents authors with more than twenty total link strengths. Table 6 shows that Susilo and Willy had the highest publications of 24, representing 3.7%; 928 citations, representing 6.3%; and 48 total link strength, representing 6.7%.

Table 1. Top authors

Author	Documents	Times cited	Total link strength
Susilo, Willy	24	928	48
Mu, Yi	12	606	31
Guo, Fuchun	10	466	28
Huang, Xinyi	9	207	24
Yang, Guomin	8	440	24

Bibliometric analysis of Top affiliation

Table 7 presents affiliations with more than fifteen publications on encryption and forensic science. The results revealed that the Chinese Academy of Sciences had the highest publications with 39 documents representing 5.9%; 1378 times cited representing 9.4%; an average per item of 35.33 and an h-index of 18. This is followed by the University of Wollongong with 31 documents representing 4.7%; 1254 times cited representing 8.5%; an average per item of 40.45; and an h-index of 20. See Table 7 for further information.

Table 2. Top affiliations

Affiliation	Documents	Times cited	Average per item	h-index
Chinese Academy of Sciences	39	1378	35.33	18
University of Wollongong	31	1254	40.45	20
Institute of Information Engineering CAS	24	965	40.21	14
City University of Hong Kong	17	668	39.29	9
Singapore Management University	16	916	57.25	10

Bibliometric analysis of Keywords

In the final analysis, keywords provided by the manuscript's authors and repeated more than three times in the Web of Science core collection were combined. The most common and pertinent keywords, out of 656 papers, are 2117. Keywords that appeared five or more times met the threshold. To prevent duplicates, the keywords were exported from VoSviewer and imported into a Google sheet to remove duplicates. After duplicates were removed from the keywords that met the threshold, the total number of keywords was reduced to 2046; 46 met the threshold. Fig. 5 shows that digital forensics was mentioned the most in the publications.

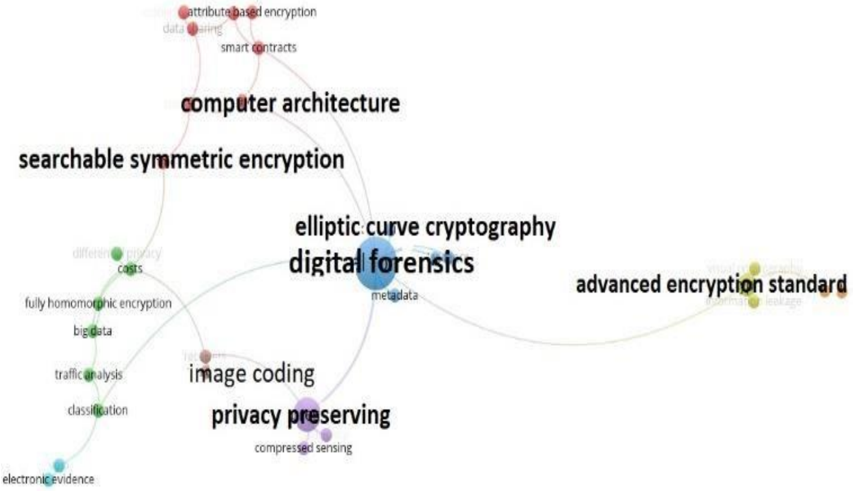

Fig 5. Network visualization of keywords

The "encryption" and "forensic" are majorly linked with privacy preservation, costs, advanced encryption standard, malware, and smart contracts. See Table 8 for keywords that had more than two total link strength.

Table 3. Top keywords

Keywords	Occurrence	Total link strength
Digital forensic	56	13
Privacy preservation	23	7
Costs	4	5
Advanced encryption standard	11	4
Malware	4	4
Smart contracts	4	4
Big data	4	3
Classification	4	3
Computer architecture	4	3
Data sharing	4	3
Dynamic analysis	4	3
Receivers	4	3
Revocation	4	3
Smartphone backup	4	3
Smartphone forensics	4	3
Tools	4	3
Transforms	4	3
Voip	4	3

Bibliometric analysis of citations

The analysis of article citations is the most widely used method of assaying the impact of authors and articles, since it identifies the key papers in the research area. Fig. 6 shows the visual representation of documents cited with authors.

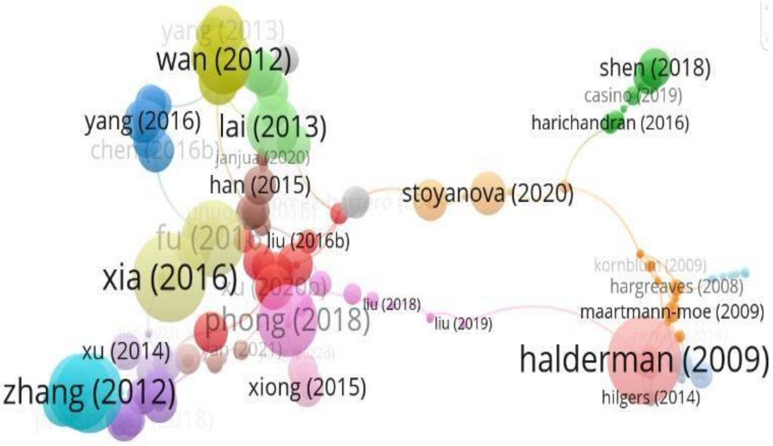

Fig 6. Network visualization of documents cited

Table 9 analyzes the structure of citations in the relevant area of research. It is possible to see which articles are most cited in this area, with "A Privacy-Preserving and Copy-Deterrence Content-Based Image Retrieval Scheme in Cloud Computing" being the reference publication, which has a total of 498 citations with an average per year of 71.14. This is followed by "Lest We Remember: Cold-Boot Attacks on Encryption Keys" being the second reference publication, which has a total of 498 citations with an average of 35.57 per year.

Table 4. Top documents cited

Documents	Authors	Average per year	Total
A Privacy-Preserving and Copy Deterrence Content-Based Image Retrieval Scheme in Cloud Computing	Xia et al. [26]	71.14	498
Lest We Remember: Cold-Boot Attacks on Encryption Keys	Halderman et al. [27]	35.57	498
Separable Reversible Data Hiding in Encrypted Image	Zhang, X.P. [28]	36.36	400
Toward Efficient Multi-Keyword Fuzzy Search Over Encrypted Outsourced Data With Accuracy Improvement	Fu et al. [29]	52	364
Reversible Data Hiding in Encrypted Images by Reserving Room	Ma et al. [30]	36.2	362
Before Encryption			
Privacy-Preserving Deep Learning via Additively Homomorphic Encryption	Phong et al. [31]	65.8	329
HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing	Wan et al. [32]	25	275
Attribute-Based Encryption With Verifiable Outsourced Decryption	Lai et al. [33]	24.9	249
Security issues in cloud environments: a survey	Fernandes et al. [34]	22.89	206
Optical Layer Security in Fiber-Optic Networks	Fok et al. [35]	16.25	195

Analysis of research opportunities

In a cloud computing environment, Xia et al. [26] introduced a copy-deterrence and privacy-preserving content-based picture retrieval technique. According to Xia et al. [26], the security of the image features against the Ciphertext-only Attack model, the security of the image contents against the Attack model of Chosen-plaintext, and the improvement of the efficiency of search from O (n) to O (ni) Future efforts, according to Xia et al. [26], should consider that their suggested watermarking method is not very reliable. Second, a small parameter will result in a constrained selection of watermarks. Researchers should work harder in the future to create watermarking algorithms that are more robust and capable of embedding data. New techniques were presented by Halderman et al. [27] for locating cryptographic keys in memory pictures and for fixing bit decay-related issues. According to Halderman et al. [27], there does not appear to be an easy cure for memory reminiscence attacks. But until architectures are updated to give running software a secure location to store secrets, it won't be possible to treat dynamic RAM (DRAM) as untrusted and avoid storing sensitive data there. A brand-new method for separable, reversible data hiding in encrypted images was put out by Zhang [28]. Zhang [28] demonstrated that if the receiver possessed the encryption and data-hiding key, he could recover the original content without making any mistakes and extract additional data. Zhang [28] suggested that future research should be done on a thorough mix of image encryption and data hiding compatible with lossy compression. The issue of multi-keyword fuzzy ranked search over cloud encrypted data was investigated by Fu et al. [29]. Founded on Wang et al.'s [38] method, Fu et al. [29] suggested a fuzzy multi-keyword ranked search technique. Fu et al. [29] summarized future work as follows:

- Fuzzy ranked search allows for dynamic updates. Although our technique in this paper can allow updates, we were unable to reach the optimal state due to the keyword weight. We'll provide a method to update and reflect the keyword weight.
- Semantic search: Specifically, we may extract the characteristics of a sentence, explain the relationship among attributes, and search using the attributes once the query of the user is a sentence.
- Multi-data owner scheme: Many works in the modern era were largely focused on the situations of single data owners and were thus ineffective for multi-data owners. Keep in mind that the multi-data owner method is more important in practice.
- Verification: In cloud computing, verification is a hot topic. A results verification search technique over encrypted cloud data was put out in reference [36]. Additionally, Wang et al. [37] introduced a brand-new Bloom filter-based verifiable auditing scheme for outsourced databases. We will find out more about them and develop a search strategy that can be verified for encrypted cloud data.

By reserving space before encrypting with a conventional RDH algorithm, Ma et al.'s [30] innovative approach makes it simple for the hider of the data to embed data reversibly in the encrypted image. The suggested method can achieve excellent performance without compromising perfect secrecy and can benefit from all conventional RDH techniques for plain images. Furthermore, the quality of annotated and decrypted photos can be substantially improved by using this unique method, which also achieves actual reversibility and distinct data extraction. A deep learning system that is privacy-preserving was introduced by Phong et al. [31] wherein several learning respondents use neural deep learning network-based on a merged dataset without disclosing their local data to a centralized server. Gradients sharing, even partly across a cloud parameter server, as in [38], might leak info, according to Phong et al. [31]. After that, Phong et al. [31] suggested a brand-new technique that uses homomorphic encryption additively to shield the gradients from the observant server. As well as maintaining privacy, their system has the advantage of maintaining deep learning accuracy. By adding a hierarchical user structure to ciphertext-policy attribute-set-based encryption (ASBE), Wan et al. [32] introduced hierarchical attribute-set-based encryption (HASBE). Wan et al. [32] implemented their plan and demonstrated its effectiveness and adaptability in handling access control for data outsourced in cloud computing through extensive trials. was taken into consideration as a new need for ABE with outsourced decryption. Informally, verifiability ensures that a user may quickly determine whether the transformation was carried out properly [39]. A concrete ABE method with verifiable outsourced decryption was developed by Lai et al. [33], who also demonstrated its security and verifiability. They don't use arbitrary oracles in their plan. They implemented their plan and ran trials in a simulated outsourcing scenario to determine how feasible it was. As predicted, the approach significantly decreased the amount of calculation time needed for devices with low resources to retrieve plaintext. Fernandes et al. [34] conducted a thorough evaluation of the literature on cloud security challenges by surveying the publications in the field. Second, a small parameter will result in a constrained selection of watermarks. Researchers should work harder in the future to create watermarking algorithms that are more robust and capable of embedding data. New techniques were presented by Halderman et al. [27] for locating cryptographic keys in memory pictures and for fixing bit decay-related issues. According to Halderman et al. [27], there does not appear to be an easy cure for memory reminiscence attacks. But until architectures are updated to give running software a secure location to store secrets, it won't be possible to treat dynamic RAM (DRAM) as untrusted and avoid storing sensitive data there. By utilizing an orthogonal coding and resilient optical ring topology for obscurity, Fok et al. [35] go on to address the usage of optical code-division multiple access (OCDMA) coding to improve the optical network's secrecy and availability. OCDMA's distinctive coding technique gives the signal the potential to be authenticated. As a result, scholars can continue to study this subject in the future.

5. CONCLUSION

To better understand the historical overview, the trends, and contributions of the literature, bibliometric analysis of forensic science and encryption literature is offered in this study. In the current study, the volume and impact of 656 publications on the academic topics of encryption and forensic science were statistically examined using a bibliometric technique. The study specifically sought to ascertain the distribution of keywords in publications on forensic science and encryption from 1995 to July 7, 2022; the total number of papers published; the national network; authorship patterns; the author; the sources of the publications; affiliation; funding agencies; and citation trends. Based on specific search queries about encryption and forensic science, research documents were gathered from the Web of Science database and examined. It is evident that China has the most publications and has the most effect in terms of the total link strength and the number of citations when comparing the geographical distribution of the literature to other nations like Australia and the United States of America. The most frequently occurring keywords were "Digital forensic", "Privacy preservation", "Costs", "Advanced encryption standard", "Malware", "Smart contracts", "Big data" and "Computer architecture" (see TABLE VIII). These keywords occurred more than three times. This study has some restrictions due to the built-in limitations of the database we used. This indicates that even though Web of Science is one of the biggest databases, some publications are still excluded from its coverage. Additionally, the scope of this research was restricted to forensic science and associated fields of study. The fact that no search query is flawlessly error-free is also crucial. Future researchers can focus on the National Science Foundation (NSF), Chinese National Foundation of Natural Science (CNFN), Chinese National Development Program and Key Research, Research Fundamental Funds for the Central Universities, Research Australian Council, and European Commission for funding in studies related to encryption and forensic science. Future researchers can rely on the Chinese Sciences Academy, University of Wollongong, Institute of Information Engineering CAS, City University of Hong Kong, and Singapore Management University for publications and for updating knowledge.

References

1. Regulation of Investigatory Powers Act, Chapter 23, www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1, 2000.
2. C. Tan, L. Zhang, L. Bao, “A Deep Exploration of BitLocker Encryption and Security Analysis,” In 2020 IEEE 20th International Conference on Communication Technology (ICCT) (pp. 1070-1074), IEEE, 2020.
3. H. Al Shehhi, I. Asad, F. Iqbal, “A forensic analysis framework for recovering encryption keys and BB10 backup decryption,” In 2014 Twelfth Annual International Conference on Privacy, Security and Trust (pp. 172178). IEEE, 2014.
4. E. Casey, G. J. Stellatos, “The Impact of Full Disk Encryption on Digital Forensics,” New York: ACM, 2008.
5. R. Canetti, C. Dwork, M. Naor, R. Ostrovsky, “Deniable encryption,” In Advances in Cryptology—CRYPTO'97: 17th Annual International Cryptology Conference Santa Barbara, California, USA August 17–21, 1997 Proceedings 17 (pp. 90-104). Springer Berlin Heidelberg, 1997.
6. Karstens, N.: Deniable Encryption. pp. 1-10. www.karstens.us/DeniableEncryption.pdf, 2006.
7. A. Czeskis, D. J. S. Hilaire, K. Koscher, S. D. Gribble, T. Kohno, B. Schneier, “Defeating Encrypted and Deniable File Systems: TrueCrypt v5. 1a and the Case of the Tattling OS and Applications,” In HotSec, 2008.
8. B. Oler, I. El Fray, “Deniable File System - Application of Deniable Storage to Protection of Private Keys,” CISIM '07’. 6th International Conference on 28-30 June, pp. 225-229, (2007).
9. BestCrypt for Windows, www.jetico.com/bcrypt8.htm (Accessed July. 2022)
10. FreeOTFE, www.freeotfe.org/docs/description.htm (Accessed July. 2022)
11. TrueCrypt, www.truecrypt.org/ (Accessed July. 2022)
12. PhoneBookFS online manual, www.freenet.org.nz/phonebook/manual.html (Accessed July. 2022)
13. Rubberhose, http://iq.org/~proff/rubberhose.org/ (Accessed July. 2022)
14. A. Stepan, “Improving proactive detection of packed malware,” Virus Bulletin, 2006.
15. A.H. Sung, J. Xu, P. Chavez, S. Mukkamala, “Static analyzer of vicious executables (save),” in ACSAC ’04: Proceedings of the 20th Annual Computer Security Applications Conference, IEEE Computer Society, pp. 326-334, 2004.
16. G. Wagener, R. State, A. Dulaunoy, “Malware behaviour analysis,” Journal in Computer Virology, pp. 279-287, 2008.

17. J. Rhee, Z. Lin, D. Xu, "Characterizing kernel malware behavior with kernel data access patterns," in Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, New York, pp. 207-216, 2011.
18. L. Martignoni, M. Christodorescu, S. Jha, "OmniUnpack: Fast,Generic, and Safe Unpacking of Malware," in 23rd Annual Computer Security Applications Conference (ACSAC), 2007.
19. P. Royal, M. Halpin, D. Dagon, R. Edmonds, W. Lee, "PolyUnpack: Automating the Hidden-Code Extraction of UnpackExecuting Malware," in 22nd Annual Computer Security Applications Conference, pp. 289-300, 2006.
20. R. Lyda, J. Hamrock, "Using Entropy Analysis to Find Encrypted and Packed Malware," IEEE Security and Privacy, 5(2), pp. 40-45, 2007.
21. C.H. Hargreaves, H. Chivers, Recovery of encryption keys from memory using a linear scan. Third International Conference on Availability, Reliability and Security, ares, pp. 1369-1376, 2008.
22. E. Casey, G.J. Stellatos, "The impact of full disk encryption on digital forensics," ACM SIGOPS Operating Systems Review, vol. 42, no. 3, pp. 93-98, 2008.
23. A. Shamir, N. Someren, "Playing «hideandseek» with stored keys," Lecture Notes in Computer Science, vol. 1648. Pp. 118-124. http://citeseer.ist.psu.edu/vansomeren98playing.html, 1999.
24. J.A. Halderman S.D. Schoen, N. Heninger, W. Clarkson, W. Paul, J.A. Calandrino, A.J. Feldman, J. Appelbaum, E.W. "Felten, Last we remember: cold-boot attacks on encryption keys," http://citp.princeton.edu/pub/coldboot.pdf, 2008.
25. A. Walters, N. Petroni, Volatools: Integrating Volatile Memory Forensics into the Digital Investigation Process. http://www.komoku.com/forensics/basic/bh-fed-07-walterspaper.pdf, 2007.
26. Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, Ren, K. "A privacy preserving and copy-deterrence content-based image retrieval scheme in cloud computing," IEEE transactions on information forensics and security, 11(11), pp. 2594-2608, 2016.
27. J.A. Halderman, S.D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, E. W. Felten, "Lest we remember: cold-boot attacks on encryption keys," Communications of the ACM, 52(5), pp. 91-98, 2009.
28. X. Zhang, "Separable reversible data hiding in encrypted image," IEEE transactions on information forensics and security, 7(2), pp. 826-832, 2012.
29. Z. Fu, X. Wu, C. Guan, X. Sun, K. Ren, "Toward efficient multikeyword fuzzy search over encrypted outsourced data with accuracy improvement," IEEE Transactions on Information Forensics and Security, 11(12), pp. 2706-2716, (2016).
30. K. Ma, W. Zhang, X. Zhao, N. Yu, F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," IEEE Transactions on information forensics and security, 8(3), pp. 553-562, 2013.
31. LT. Phong, Y. Aono, T. Hayashi, L. Wang, S. Moriai, "Privacypreserving deep learning via additively homomorphic encryption," IEEE Transactions on Information Forensics and Security, 13(5), pp. 13331345, 2018.
32. Z. Wan, R.H. Deng, "HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing," IEEE transactions on information forensics and security, 7(2), pp. 743-754, 2011.
33. J. Lai, R.H. Deng, C. Guan, J. Weng, "Attribute-based encryption with verifiable outsourced decryption," IEEE Transactions on information forensics and security, 8(8), pp. 1343-1354, 2013.
34. D.A. Fernandes, L.F. Soares, J.V. Gomes, M.M. Freire, P.R. Inácio, "Security issues in cloud environments: a survey," International Journal of Information Security, 13(2), pp. 113-170, 2014.
35. M.P. Fok, Z. Wang, Y. Deng, P.R. "Prucnal, Optical layer security in fiber-optic networks," IEEE Transactions on Information Forensics and Security, 6(3), pp. 725-736, 2011.
36. J. Wang, X. Chen, X. Huang, I. You, Y. Xiang, "Verifiable auditing for outsourced database in cloud computing," IEEE Trans. Comput., 64(11), pp. 3293–3303, 2015.
37. W. Zhang, Y. Lin, Q. Gu, "Catch you if you misbehave: Ranked keyword search results verification in cloud computing," IEEE Transactions on Cloud Computing, 6(1), pp. 74-86, 2015.
38. B. Wang, S. Yu, W. Lou, Y. T. Hou, "Privacy-preserving multikeyword fuzzy search over encrypted data in the cloud," in Proc. IEEE INFOCOM, pp. 2112–2120 (2014).
39. R. Shokri, V. Shmatikov, "Privacy-preserving deep learning," in Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur., pp. 1310– 1321, 2015.