

Artificial intelligence for cryptography: a systematic literature review of methods, applications, and challenges

Decky Hendarsyah

Institut Syariah Negeri Junjungan (ISNJ) Bengkalis, Riau, Indonesia

deckydb@gmail.com

DOI: <https://doi.org/10.65881/jistecs.v1i2.210>

ARTICLE INFO

History:

Received: 09-28-2026

Revised: 10-11-2026

Accepted: 10-12-2026

Published: 10-16-2026

Keywords:

artificial intelligence;
cryptography;
machine learning;
deep learning;
systematic literature
review.

ABSTRACT

Purpose: to identify, classify, and synthesize the application of artificial intelligence (AI) techniques in cryptography, including AI methods, cryptographic problems and applications, evaluation approaches, challenges, and emerging future research directions.

Method: this study employed a Systematic Literature Review (SLR) following the PRISMA framework. Studies were retrieved from Scopus and analyzed through screening, quality assessment, data extraction, and thematic synthesis based on five research questions.

Findings: neural networks, deep learning, and machine learning are the dominant AI techniques applied to cryptography, particularly in image encryption, privacy-preserving computation, healthcare, and IoT. Key challenges include computational overhead, methodological heterogeneity, reproducibility, and security validation, while emerging directions emphasize adaptive, privacy-preserving, and intelligent cryptographic systems.

Implications: provides an integrated framework for understanding AI applications in cryptography and identifies key methodological patterns, challenges, and research opportunities to guide the development of secure, efficient, and adaptive cryptographic systems.

Originality: lies in providing an integrated synthesis that systematically connects AI techniques, cryptographic applications, evaluation approaches, challenges, and emerging research directions within a unified framework.



Open access article under CC-BY-SA license.



Introduction

The rapid expansion of digital transformation has fundamentally changed the way information is generated, exchanged, processed, and stored (Yaqub & Alsabban, 2023). The proliferation of cloud computing, Internet of Things (IoT), mobile and distributed systems, artificial intelligence (AI), and other data-intensive technologies has

created increasingly interconnected digital environments in which sensitive information must be protected against sophisticated and continuously evolving cyber threats (Prangon & Wu, 2024; Trigka & Dritsas, 2025). In this context, cryptography remains a fundamental foundation of information security because cryptographic mechanisms provide essential protection for confidentiality, integrity, authentication, privacy, and secure communication (Z. Wang & Tabassum, 2024). However, the growing complexity of digital infrastructures and the increasing volume and diversity of security threats have created new demands for cryptographic mechanisms that are not only mathematically secure but also efficient, adaptive, scalable, and able to respond to dynamic security environments (Eren et al., 2025).

At the same time, artificial intelligence has developed rapidly and shown considerable potential for solving complex computational and decision-making problems (Huang et al., 2025). Machine learning (ML), deep learning (DL), neural networks, reinforcement learning, and other AI-based techniques can learn patterns from data, identify anomalies, optimize parameters, and support adaptive decision-making (Mohamed, 2025). These capabilities have increasingly attracted attention in cybersecurity and cryptographic research. Recent studies have explored AI for cryptographic attack detection, cryptanalysis, side-channel analysis, cryptographic design, and security optimization. For example, recent systematic research has examined machine learning techniques for detecting cryptographic attacks, while other studies have investigated AI's potential to influence or threaten conventional cryptographic mechanisms (Adere et al., 2026; Taherdoost et al., 2025). The interaction between these two fields therefore represents an emerging interdisciplinary research area in which AI can function both as a tool for strengthening cryptographic security and as a potential source of new security threats (Taherdoost et al., 2025).

The bidirectional relationship between AI and cryptography further complicates the phenomenon. On one hand, AI techniques can potentially enhance cryptographic systems by supporting cryptanalysis, identifying vulnerabilities, optimizing cryptographic parameters, improving attack detection, and developing adaptive security mechanisms (Abdewi et al., 2026). Recent research has also explored AI in quantum cryptography, suggesting that AI may improve the efficiency and robustness of cryptographic systems in emerging technological environments (Radanliev, 2024). On the other hand, AI can also become a tool for discovering cryptographic weaknesses and improving the efficiency of attacks against cryptographic implementations. Recent systematic research on machine learning and cryptographic attacks illustrates this dual role, reporting the application of several learning techniques to attack detection and vulnerability analysis (Khaleel et al., 2024). Consequently, AI and cryptography should not be considered as two independent research domains; rather, their interaction creates both opportunities and risks that require systematic investigation (Taherdoost et al., 2025).

The existing literature demonstrates substantial research activity at this intersection, but it also reveals considerable fragmentation. Some studies focus primarily on applying machine learning to cryptographic attack detection, while others investigate AI-assisted cryptanalysis and cryptographic design (Biswas & Raj, 2024). Other reviews examine the relationship between AI and quantum cryptography, while recent bibliometric research investigates cryptographic techniques for securing AI systems rather than applying AI to cryptography itself (Abdewi et al., 2026; Taherdoost et al., 2025). Broader cybersecurity reviews have also examined AI techniques across intrusion detection, malware classification, privacy preservation, and other security

applications (Achuthan et al., 2024). However, these studies generally treat cryptography as one component of a much wider cybersecurity landscape (Achuthan et al., 2024). This dispersion makes it difficult to build a consolidated understanding of which AI techniques are used for which cryptographic problems, how their effectiveness is evaluated, and what limitations consistently emerge across studies (Heidari et al., 2026; Taherdoost et al., 2025).

Another issue is the lack of a sufficiently integrated perspective on the evidence generated by these studies. Existing reviews tend to emphasize particular dimensions of the AI-cryptography relationship rather than examining the AI methodology, cryptographic task, application domain, evaluation strategy, security implications, and limitations of the proposed approaches simultaneously. For instance, a review focused on cryptographic attack detection may provide detailed comparisons of machine learning models but does not necessarily explain how AI is being used for cryptographic design, key generation, encryption optimization, or other cryptographic functions. Conversely, reviews addressing AI and quantum cryptography or cryptography-based AI security examine important emerging areas but represent different directions of interaction between the two fields (Adere et al., 2026). This fragmentation indicates the need for a broader, more systematic synthesis that connects these dimensions into a coherent research framework.

The research gap therefore lies not simply in the lack of studies on AI and cryptography, but in the limited integration and systematic classification of the existing evidence across the broader AI-cryptography research landscape. In particular, we still need to establish how different AI techniques are distributed across cryptographic problems, how researchers evaluate the resulting approaches, what technical and methodological limitations are repeatedly reported, and which research directions emerge from these limitations. Recent reviews with narrower scopes further reinforce the need for a review that systematically maps the broader relationship between AI techniques and cryptographic applications, rather than focusing on a single attack type, cryptographic paradigm, or application domain (Taherdoost et al., 2025). This study's novelty lies in developing an integrated analytical perspective that connects AI techniques, cryptographic problems, application domains, evaluation approaches, challenges, and emerging research directions within a single systematic framework. Rather than treating AI and cryptography as isolated topics or focusing exclusively on cryptographic attacks, this review maps the broader spectrum of interactions between AI methodologies and cryptographic mechanisms. The proposed framework aims to reveal patterns and relationships that may be obscured when the literature is examined through individual technological or application-specific perspectives.

This review draws its theoretical foundation from the intersection of cryptographic security theory and artificial intelligence and machine learning theory. From the cryptographic perspective, the analysis considers fundamental security objectives, including confidentiality, integrity, authentication, privacy, resistance to cryptanalysis, and computational security. From the AI perspective, the review considers learning paradigms and computational approaches such as supervised learning, unsupervised learning, deep learning, reinforcement learning, neural networks, and optimization-based methods. Combining these theoretical perspectives provides a basis for examining not only whether AI techniques are applied to cryptography, but also why particular AI approaches are selected, what cryptographic functions they support, and how their performance and security are assessed.

Based on these theoretical and empirical considerations, this study's primary objective is to systematically identify, classify, and synthesize research on applying artificial intelligence to cryptography. Specifically, the study aims to identify the AI techniques employed in cryptographic research, classify the cryptographic problems and application domains addressed, analyze the evaluation metrics and experimental approaches used to assess AI-based cryptographic solutions, identify recurring technical and methodological challenges, and synthesize emerging research directions. This objective matters because a systematic understanding of these dimensions can help distinguish established research patterns from emerging approaches and provide a stronger evidence base for future research in this interdisciplinary field.

This study matters because the relationship between intelligent computing and information security is becoming increasingly complex. As AI becomes more deeply integrated into digital infrastructure, cryptographic mechanisms must be considered not only as static mathematical primitives but also as components operating within adaptive, data-driven, and increasingly autonomous environments. At the same time, AI-based approaches must account for the security properties and constraints imposed by cryptographic systems. A systematic synthesis of this relationship is therefore important for researchers developing new algorithms, security architectures, and intelligent cryptographic mechanisms. It is also relevant for practitioners who need to understand the potential benefits, limitations, computational requirements, and security implications of incorporating AI into cryptographic environments.

This study's expected contribution is threefold. First, it provides a systematic taxonomy linking AI techniques with cryptographic tasks and application domains, thereby offering a structured representation of the existing research landscape. Second, it offers a comparative synthesis of evaluation strategies, performance considerations, security implications, and limitations, helping researchers identify methodological patterns and unresolved issues across studies. Third, it develops an evidence-based research agenda by identifying research gaps and emerging directions at the intersection of AI and cryptography. Through these contributions, the study is expected to provide a conceptual and empirical foundation for future investigations into intelligent cryptographic systems while helping researchers understand where current knowledge is relatively mature and where further systematic investigation is required.

Method

This study employs a Systematic Literature Review (SLR) methodology to identify, evaluate, classify, and synthesize existing research on the application of artificial intelligence (AI) in cryptography. The SLR provides a structured, reproducible process for identifying relevant studies, assessing their quality, extracting evidence, and synthesizing findings according to the research questions defined in this study. The review process consists of several sequential stages: (1) development of the SLR protocol, (2) database selection, (3) search strategy formulation, (4) application of inclusion and exclusion criteria, (5) study selection, (6) quality assessment, (7) data extraction, and (8) synthesis and reporting of the findings. The review protocol was developed before the detailed study selection process to minimize selection bias and ensure consistency throughout the review. The protocol defines the research scope, information sources, search string, eligibility criteria, quality assessment procedure, and data extraction strategy. The overall study selection and reporting process follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework.

The review followed these research questions: RQ1: What artificial intelligence techniques have been applied to cryptography? RQ2: What cryptographic problems and applications are addressed using AI techniques? RQ3: How are AI-based approaches evaluated in cryptographic research? RQ4: What are the major challenges and limitations of applying AI to cryptography? RQ5: What emerging research directions can be identified at the intersection of AI and cryptography? These questions move the analysis beyond a descriptive inventory of publications by examining relationships among methods, problems, applications, evaluation criteria, limitations, and future opportunities. These research questions guide study selection, quality assessment, data extraction, and evidence synthesis.

Scopus was selected as the primary bibliographic database for this systematic literature review. The selection of Scopus was motivated by its extensive coverage of peer-reviewed scientific publications across computer science, engineering, mathematics, cybersecurity, artificial intelligence, and information technology. The database also provides structured bibliographic information that facilitates systematic searching, filtering, citation analysis, and subsequent data extraction. Using a single well-defined database also provides a consistent search environment and enables the study to maintain a clearly reproducible search strategy. The search was conducted in Scopus, with search fields and filters defined according to the research objectives and eligibility criteria.

A structured search strategy was developed to identify publications addressing the intersection of artificial intelligence and cryptography. The search terms were derived from the study's main concepts: artificial intelligence techniques and cryptographic technologies. Synonyms and related terms were incorporated using Boolean operators to increase the coverage of potentially relevant studies. The search query used in Scopus was formulated as follows: ("artificial intelligence" OR "machine learning" OR "deep learning" OR "neural network*" OR "reinforcement learning") AND (cryptograph* OR "cryptographic algorithm*" OR encryption OR decryption OR "cryptographic security"). The wildcard operator * was used to capture variations of terms, particularly for words such as cryptography, cryptographic, and related forms. The Boolean operator OR was used to combine alternative terms representing similar concepts, whereas AND was used to ensure that the retrieved documents addressed both AI-related and cryptography-related concepts. The initial search retrieved 1,691 documents from Scopus. These documents formed the initial identification set and were then screened against predefined inclusion and exclusion criteria.

To ensure that the selected studies were relevant to the research objectives and sufficiently comparable for systematic analysis, explicit inclusion and exclusion criteria were established. The criteria were applied to the initial set of retrieved documents. The inclusion criteria were defined based on four principal characteristics: publication year, subject area, document type, and language. Studies were included if they met all criteria in Table 1.

Table 1 inclusion requirement

Criterion	Inclusion requirement
Publication year	2015–2025
Subject area	Computer Science, Engineering, and Mathematics
Document type	Article
Language	English

Studies that did not satisfy one or more of these requirements were excluded from the review. Accordingly, conference papers, book chapters, reviews, editorials, notes, errata, non-English publications, publications outside the specified subject areas, and publications outside the 2015–2025 period were excluded at this filtering stage. After applying the predefined Scopus filters, the initial 1,691 documents were reduced to 609 documents. These 609 publications formed the dataset for the subsequent study selection and screening process.

The study selection process was conducted systematically to determine which of the 609 filtered publications were sufficiently relevant to address the research questions. The selection process consisted of sequential screening stages designed to remove studies that did not directly provide evidence on AI applications in cryptography. First, the bibliographic records retrieved from Scopus were examined for potential duplicate records and inconsistencies. Duplicate records, where identified, were removed. Second, the titles and abstracts of the remaining publications were screened for relevance to the review's scope. Studies were considered potentially relevant when they addressed the application, development, evaluation, analysis, or security implications of AI techniques in cryptographic contexts. Third, the team subjected potentially relevant studies to full-text assessment. At this stage, the researchers evaluated whether each study met the predefined eligibility requirements and provided enough information to address at least one research question. Studies were excluded if their primary focus was unrelated to cryptography or AI techniques, or if they did not provide sufficient evidence relevant to the objectives of this review. The complete study selection process is reported using a PRISMA flow diagram, which presents the number of records identified, filtered, screened, assessed for eligibility, excluded, and finally included in the qualitative synthesis.

A quality assessment procedure was applied to evaluate the methodological and reporting quality of the studies selected for the final review. Quality assessment matters because inclusion in the selected literature does not necessarily mean a study has the same methodological strength or evidential value. The quality assessment criteria were developed to evaluate the clarity of the research objectives, methodological transparency, description of the AI technique, description of the cryptographic problem, evaluation methodology, and clarity of reported findings. Each selected study was assessed against a standardized set of questions. Table 2 presents the quality assessment questions used.

Table 2 quality assessment question

Code	Quality assessment question
QA1	Are the research objectives or research questions clearly stated?
QA2	Is the AI technique or methodology adequately described?
QA3	Is the cryptographic problem or application clearly defined?
QA4	Is the dataset, experimental environment, or evaluation setting adequately described?
QA5	Are the evaluation metrics or performance measures clearly reported?
QA6	Are the findings and conclusions adequately supported by the presented evidence?
QA7	Are the limitations or threats to validity discussed?

Each question can be evaluated using a three-point scale: Yes (1): the criterion is clearly satisfied. Partially (0.5): the criterion is partially satisfied. No (0): The criterion is not satisfied. The total quality score for each study can therefore range from 0 to 7. The quality assessment results characterize the methodological strength of the selected literature and support the interpretation of the synthesized findings. A standardized

data extraction form was developed to ensure consistency in collecting information from the selected studies. The extraction process aligned with the research questions and captured both bibliographic and substantive characteristics of each study. The information in Table 3 was extracted from each selected publication.

Table 3 extracted information

Data category	Extracted information
Bibliographic information	Author(s), publication year, title, journal, DOI
AI technique	Machine learning, deep learning, neural networks, reinforcement learning, etc.
Cryptographic area	Encryption, decryption, cryptanalysis, key generation, cryptographic algorithms, etc.
Application domain	Cybersecurity, IoT, cloud computing, communication systems, healthcare, etc.
Research objective	Main problem addressed by the study
Dataset	Dataset or experimental data used
Methodology	Proposed model, algorithm, framework, or approach
Evaluation metrics	Accuracy, precision, recall, F1-score, computational cost, execution time, entropy, security measures, etc.
Main findings	Principal findings reported by the study
Challenges	Technical, computational, security, or methodological limitations
Future directions	Research opportunities identified by the authors

The extracted information was then organized into a structured dataset to support descriptive analysis, thematic classification, approach comparison, and evidence synthesis. The data extraction process specifically supports the five research questions by linking each study to the AI techniques employed, cryptographic problems addressed, evaluation methods, reported limitations, and future research directions. After data extraction, the selected studies were synthesized using descriptive and thematic analysis. Descriptive analysis characterized the distribution of publications by publication year, AI technique, cryptographic application, research domain, and other relevant bibliographic characteristics.

Thematic synthesis was then conducted to identify recurring patterns and relationships among AI techniques, cryptographic problems, application domains, evaluation approaches, and reported challenges. The synthesis was organized by research question. For RQ1, studies were classified according to the AI techniques employed. For RQ2, studies were categorized according to the cryptographic problems and application domains addressed. For RQ3, the review analyzed the evaluation methods and performance metrics used in the literature. For RQ4, the review identified recurring technical, computational, methodological, and security-related limitations. Finally, RQ5 synthesized emerging research themes and future research directions based on trends and gaps identified across the selected studies. This analytical process enables the review to move beyond a simple descriptive summary and develop an integrated taxonomy of AI applications in cryptography.

The study selection process follows the PRISMA framework. The PRISMA flow diagram summarizes the progression of studies through four principal stages: identification, screening, eligibility, and inclusion. During the identification stage, the Scopus search retrieved 1,691 documents. After applying the predefined publication year, subject area, document type, and language criteria, 609 documents remained. These publications proceeded to the subsequent screening stage. The title and abstract screening was conducted to identify studies that were potentially relevant to the

research scope. Publications that did not address the intersection of artificial intelligence and cryptography were excluded. The remaining studies were then assessed through full-text screening based on the eligibility criteria and quality assessment procedure. Finally, studies satisfying the eligibility and quality requirements were included in the final qualitative synthesis. The PRISMA flow diagram reports the exact number of records removed at each subsequent stage after title/abstract screening and full-text assessment. This approach ensures that every exclusion decision is transparently documented and that the final sample can be traced back to the original Scopus search. Figure 1 presents the PRISMA flow diagram.

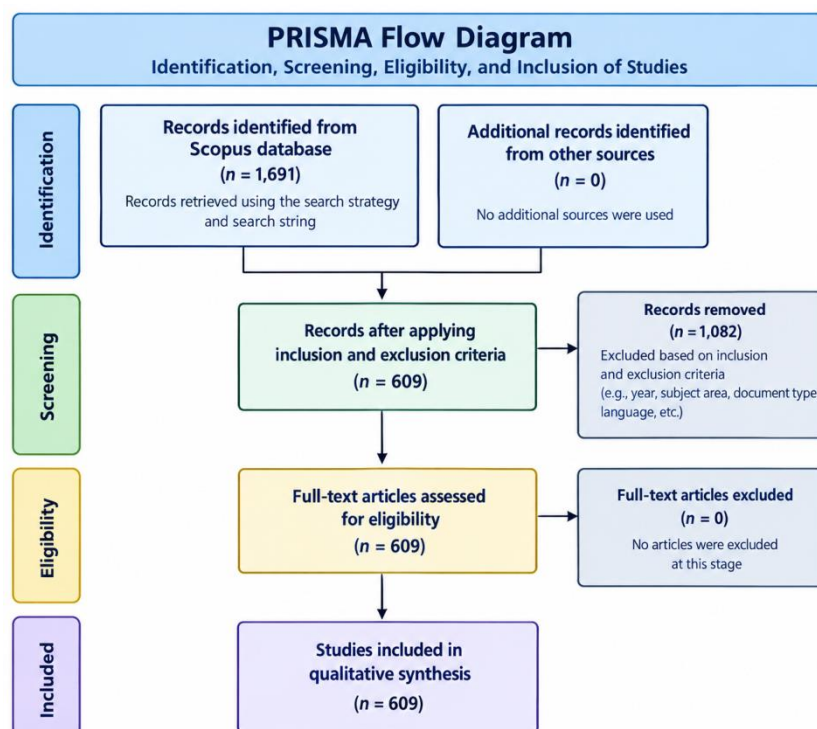


Figure 1 PRISMA flow diagram of the systematic literature review

Results and discussion

Document by years

Figure 2 illustrates the annual publication output on artificial intelligence for cryptography, based on documents indexed in Scopus from 2015 to 2025. The figure provides an overview of the development and growth of scholarly research on methods, applications, and challenges in integrating artificial intelligence and cryptography over the selected period. As shown in Figure 2, the number of publications increased steadily over the period, although growth was relatively modest in the early years. In 2015, only 6 documents were recorded, followed by 7 in 2016, 8 in 2017, and 10 in 2018. The number then increased more noticeably to 26 documents in 2019, 36 in 2020, and 44 in 2021. In 2022, the publication output reached 71 documents, indicating a further increase in research activity related to artificial intelligence and cryptography. A more substantial increase is evident from 2023 onward. The number of documents rose from 71 in 2022 to 102 in 2023 and 112 in 2024, before reaching a high of 187 documents in 2025. Overall, the figure demonstrates a clear upward trend in scholarly publications, particularly during the most recent years of the observation period. The substantial

increase in publications in 2025 indicates that research on artificial intelligence for cryptography has expanded considerably, reflecting growing scholarly attention to the methods, applications, and challenges associated with this interdisciplinary field.

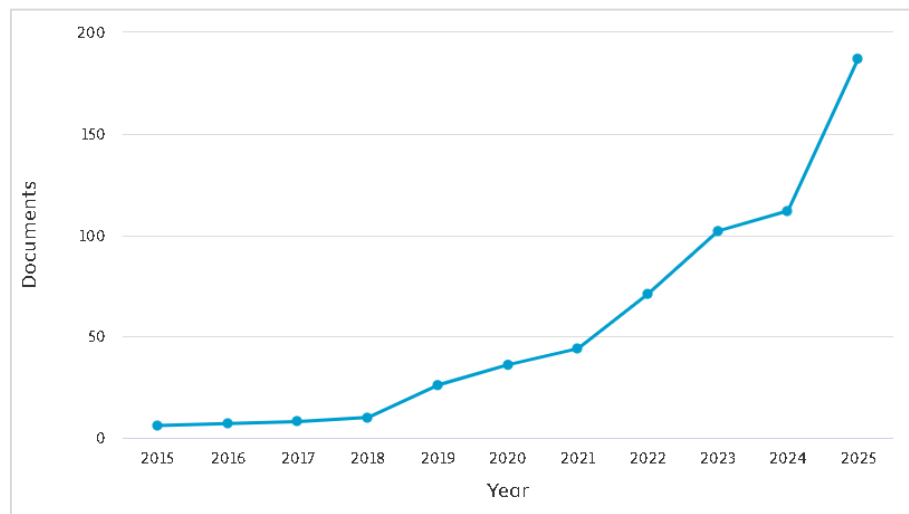


Figure 2 document by years

Source: Scopus, 2026

Document per year by source

Figure 3 shows the annual distribution of publications by source in artificial intelligence for cryptography, based on documents indexed in Scopus from 2016 to 2025. The figure shows publication patterns across the five most represented sources and how research output has developed over the period.

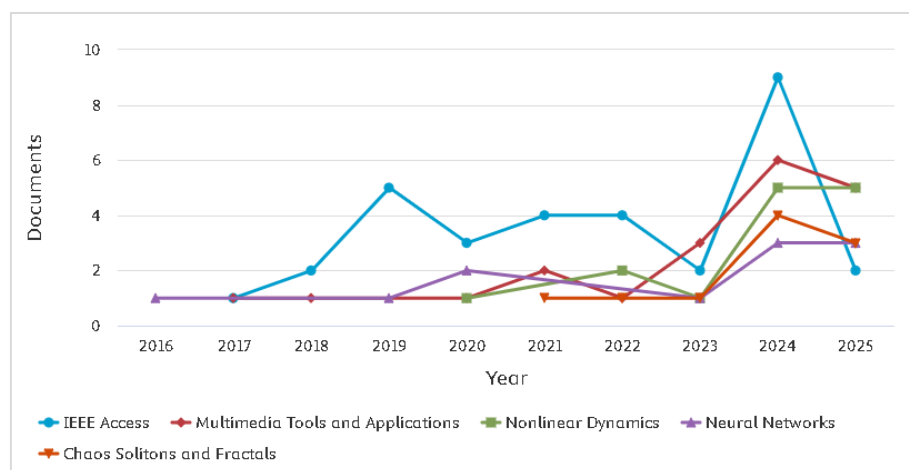


Figure 3 document per year by source

Source: Scopus, 2026

As shown in Figure 3, IEEE Access has the highest overall number of documents, with 32 publications, followed by Multimedia Tools and Applications with 20 documents. Nonlinear Dynamics contributed 14 documents, while Neural Networks and Chaos, Solitons & Fractals recorded 11 and 10 documents, respectively. In terms of annual distribution, IEEE Access shows publication activity throughout most of the period, with a noticeable increase from 2023 to 2024, when it published 9 documents. The other sources generally show lower and more variable publication volumes across

the years. The figure also indicates that publication activity across the five sources increased notably in 2024, when several sources reached their highest annual outputs. Multimedia Tools and Applications recorded 6 documents in 2024, while Nonlinear Dynamics published 5, Neural Networks published 3, and Chaos, Solitons & Fractals published 4. In 2025, publications in several sources decreased compared with 2024, although their overall presence shows their contribution to research at the intersection of artificial intelligence and cryptography.

Document by author

The distribution of publications by author provides an overview of the researchers who have contributed most prominently to the literature on artificial intelligence for cryptography. Figure 4 presents the ten authors with the most documents indexed in Scopus as of 2026. This distribution highlights the relative productivity of individual researchers and indicates their contribution to research development in this field.

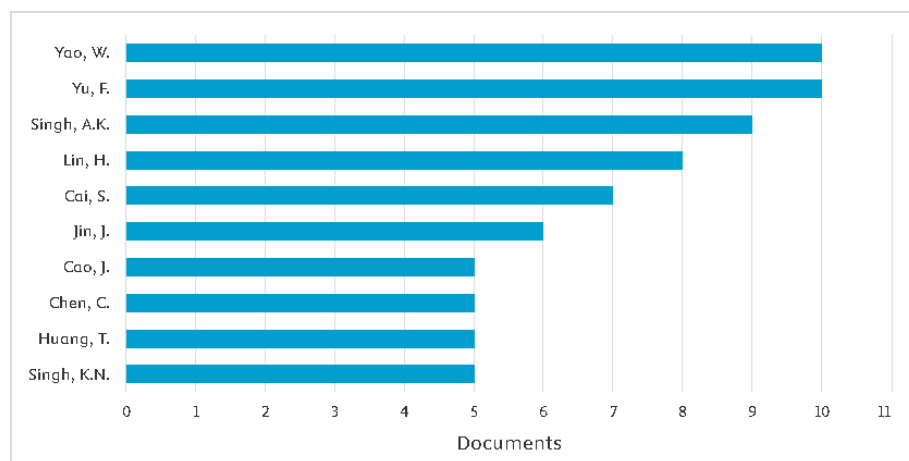


Figure 4 document by author
Source: Scopus, 2026

As shown in Figure 4, Yao, W. and Yu, F. have the most documents, with 10 publications each, followed by Singh, A.K. with 9 documents and Lin, H. with 8 documents. Cai, S. contributed 7 documents, while Jin, J. recorded 6 documents. Meanwhile, Cao, J., Chen, C., Huang, T., and Singh, K.N. each contributed 5 documents. Overall, the figure shows that publication output is concentrated among a relatively small group of authors, with document counts ranging from 5 to 10 among the ten most productive authors.

Document by affiliation

The analysis of institutional affiliations provides an overview of the organizations that have contributed to research on artificial intelligence for cryptography. Figure 5 illustrates the distribution of documents by institutional affiliation based on Scopus-indexed publications as of 2026. As shown in Figure 5, SRM Institute of Science and Technology has the most publications, with 17 documents, followed by the University of Electronic Science and Technology of China with 16 documents. Changsha University of Science and Technology and the Ministry of Education of the People's Republic of China each contributed 13 documents, while Hunan University recorded 12 documents. The National Institute of Technology Patna contributed 10 documents, whereas Vellore

Institute of Technology, Sichuan University, Hunan University of Science and Technology, and Princess Nourah Bint Abdulrahman University each recorded 9 documents. Overall, the figure shows that publications are distributed across institutions in several countries, with the highest document counts concentrated in China and India.

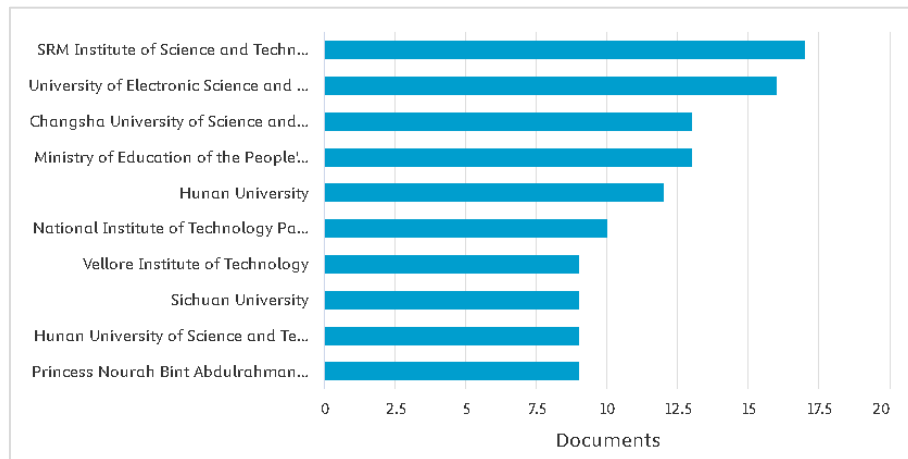


Figure 5 document by affiliation

Source: Scopus, 2026

Document by country

The analysis of publications by country provides an overview of the geographical distribution of research on artificial intelligence for cryptography. Figure 6 presents the distribution of Scopus-indexed documents by country or territory as of 2026, highlighting the countries with the highest publication output in this research area.

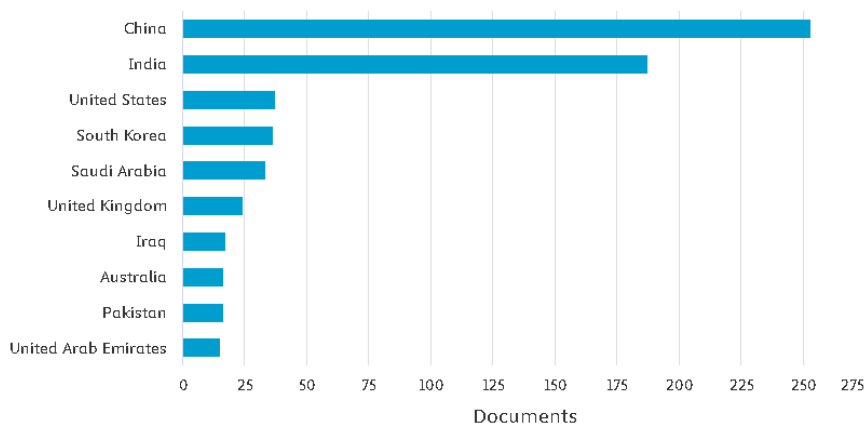


Figure 6 document by country

Source: Scopus, 2026

As shown in Figure 6, China has the most documents, with 253 publications, followed by India with 187. The United States and South Korea recorded 37 and 36 documents, respectively, while Saudi Arabia contributed 33 documents. The United Kingdom accounted for 24 documents, followed by Iraq with 17, Australia and Pakistan with 16 each, and the United Arab Emirates with 15 documents. Overall, the figure shows a substantial difference in publication output between the leading countries and the rest, with China and India accounting for the largest shares of the documents shown.

Document by citations

To identify the most influential publications in the field of artificial intelligence for cryptography, a citation analysis was conducted based on the number of citations received by individual documents indexed in Scopus. Table 4 presents the 20 most-cited documents, including their titles, authors, publication years, sources, and citation counts.

Table 4 document by citations

Nu.	Document title	Authors (Year)	Source	Citations
1	Privacy-Preserving Deep Learning via Additively Homomorphic Encryption	Phong et al. (2018)	IEEE Transactions on Information Forensics and Security	1,744
2	Privacy preserving machine learning with homomorphic encryption and federated learning	Fang & Qian (2021)	Future Internet	414
3	Privacy-Preserving Machine Learning With Fully Homomorphic Encryption for Deep Neural Network	Lee et al. (2022)	IEEE Access	407
4	Design and Analysis of Multiscroll Memristive Hopfield Neural Network With Adjustable Memductance and Application to Image Encryption	Lai et al. (2023)	IEEE Transactions on Neural Networks and Learning Systems	341
5	Lag synchronization of switched neural networks via neural activation function and applications in image encryption	Wen et al. (2015)	IEEE Transactions on Neural Networks and Learning Systems	322
6	DeepEDN: A Deep-Learning-Based Image Encryption and Decryption Network for Internet of Medical Things	Ding et al. (2021)	IEEE Internet of Things Journal	275
7	Impulsive Synchronization of Reaction-Diffusion Neural Networks With Mixed Delays and Its Application to Image Encryption	Chen et al. (2016)	IEEE Transactions on Neural Networks and Learning Systems	271
8	Double image encryption algorithm based on neural network and chaos	Man et al. (2021)	Chaos Solitons and Fractals	260
9	Chaos in fractional-order discrete neural networks with application to image encryption	L. Chen et al. (2020)	Neural Networks	255
10	An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach for Healthcare Systems Using Neural Network	Ali et al. (2022)	Sensors	246
11	A color image encryption algorithm based on Hopfield chaotic neural network	Wang & Li (2019)	Optics and Lasers in Engineering	226

Nu.	Document title	Authors (Year)	Source	Citations
12	Synchronization of Markovian jumping inertial neural networks and its applications in image encryption	Prakash et al. (2016)	Neural Networks	204
13	Constructing Multiscroll Memristive Neural Network with Local Activity Memristor and Application in Image Encryption	Lai et al. (2024)	IEEE Transactions on Cybernetics	194
14	DeepKeyGen: A Deep Learning-Based Stream Cipher Generator for Medical Image Encryption and Decryption	Ding et al. (2022)	IEEE Transactions on Neural Networks and Learning Systems	192
15	Homomorphic Encryption for Machine Learning in Medicine and Bioinformatics	Wood et al. (2021)	ACM Computing Surveys	184
16	Color-Gray Multi-Image Hybrid Compression-Encryption Scheme Based on BP Neural Network and Knight Tour	Gao et al. (2023)	IEEE Transactions on Cybernetics	181
17	Adaptive control for fractional order induced chaotic fuzzy cellular neural networks and its application to image encryption	Mani et al. (2019)	Information Sciences	181
18	A new fractional-order chaos system of Hopfield neural network and its application in image encryption	Xu et al. (2022)	Chaos Solitons and Fractals	171
19	Impulsive synchronization of unbounded delayed inertial neural networks with actuator saturation and sampled-data control and its application to image encryption	Li et al. (2021)	IEEE Transactions on Neural Networks and Learning Systems	169
20	High-dimensional memristive neural network and its application in commercial data encryption communication	C. Wang et al. (2024)	Expert Systems with Applications	163

Source: Scopus, 2026

Table 4 shows that the most-cited publication is “Privacy-Preserving Deep Learning via Additively Homomorphic Encryption” by Phong et al. (2018), published in IEEE Transactions on Information Forensics and Security, with 1,744 citations. This document is followed by “Privacy-preserving machine learning with homomorphic encryption and federated learning” by Fang & Qian (2021), with 414 citations, and “Privacy-Preserving Machine Learning With Fully Homomorphic Encryption for Deep Neural Network” by Lee et al. (2022), with 407 citations. The remaining publications received between 163 and 341 citations, indicating that the documents listed in the table have attracted substantial scholarly attention. The citation distribution also shows a considerable gap between the first-ranked publication and the other highly cited documents.

In terms of research themes, the highly cited documents mainly address the integration of artificial intelligence, neural networks, homomorphic encryption, privacy-

The network can be divided into several color-coded clusters: blue, yellow, green, red, purple, and light blue. The blue cluster centers on authors such as Yu, F., Lin, H., Yao, W., and Wang, C., while the yellow cluster includes Huang, Y., Jin, J., Chen, C., and Liu, L. The green cluster contains authors such as Zhang, Y., Zhou, L., Yang, X., Liu, J., and Wang, H., whereas the red cluster includes Wang, Y., Wang, Z., Wang, T., and related authors. The numerous cross-cluster links indicate collaboration among researchers from different groups and suggest a multidisciplinary, interconnected research environment. Overall, the figure shows that research on artificial intelligence for cryptography has developed through multiple collaborative communities, with several researchers serving as key links between groups.

Collaborative network between countries

To examine the international dimension of research on artificial intelligence for cryptography, Figure 8 presents the country-level collaboration network generated with VOSviewer. The visualization shows patterns of international co-authorship and identifies the countries that contribute to and connect different research communities in the field.

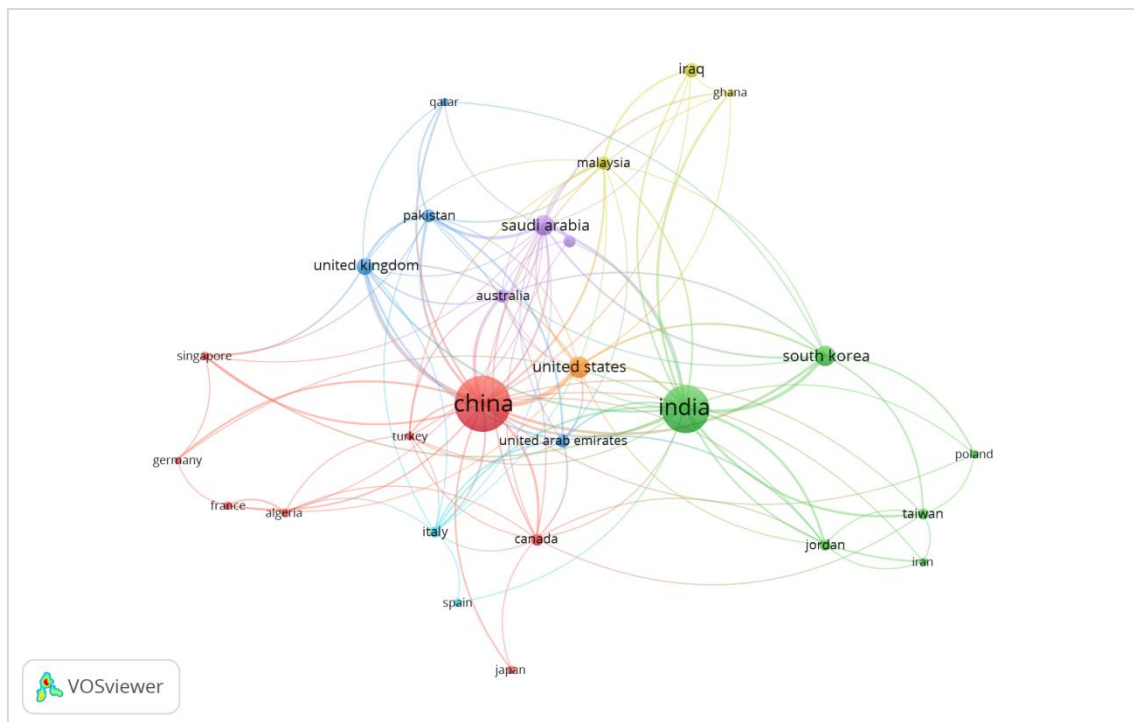


Figure 8 collaborative network between countries

Source: VOSviewer, 2026

Figure 8 demonstrates a highly interconnected international collaboration network involving researchers from numerous countries. Each node's size represents the relative level of research contribution or occurrence for that country, while the connecting lines indicate co-authorship relationships between countries. China and India appear as the most prominent nodes in the network, reflecting their substantial presence and extensive collaborative connections within the literature. Other countries, including the United States, United Kingdom, Australia, Saudi Arabia, Pakistan, Malaysia, South Korea, and the United Arab Emirates, are also visibly connected to multiple countries, indicating their participation in broader international research collaborations.

The dense concentration of links around China, India, and the United States further illustrates the interconnected nature of research activities in artificial intelligence and cryptography.

The network is organized into several color-coded clusters that reflect groups of countries with relatively strong collaboration patterns. The red cluster is strongly associated with China and includes Singapore, Germany, France, Algeria, Turkey, Canada, Japan, and Italy. The green cluster centers on India and includes South Korea, Poland, Taiwan, Jordan, and Iran. In contrast, the blue and purple clusters include countries such as the United Kingdom, Pakistan, Qatar, Saudi Arabia, and Australia. Malaysia, Iraq, and Ghana form part of another visible collaboration grouping. The numerous links between clusters indicate that international collaboration extends beyond geographically or regionally concentrated groups. Overall, Figure 8 suggests that research on artificial intelligence for cryptography is characterized by a broad international research landscape in which countries are connected through multiple cross-border collaborative relationships.

Research keyword network

To identify major research themes and conceptual relationships in artificial intelligence for cryptography, Figure 9 presents the research keyword network generated with VOSviewer. The visualization maps the co-occurrence relationships among frequently used keywords and highlights the thematic structure of the existing literature.

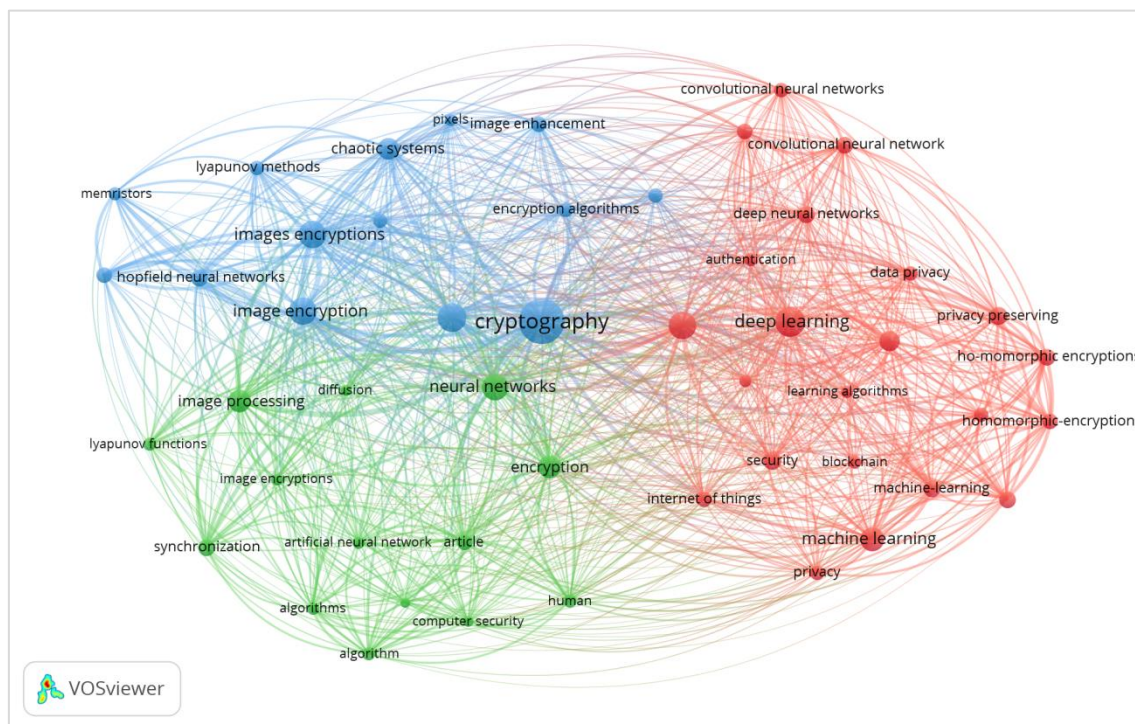


Figure 9 research keyword network

Source: VOSviewer, 2026

Figure 9 illustrates a dense and highly interconnected keyword network, indicating that research on artificial intelligence for cryptography encompasses several closely related themes. Each node's size reflects a keyword's frequency or prominence, while the links between nodes represent their co-occurrence in the analyzed

publications. Cryptography appears as a central and prominent keyword, connecting major themes across the network. Other highly visible terms include deep learning, machine learning, neural networks, image encryption, encryption, security, privacy, and convolutional neural networks. The network therefore shows that researchers study artificial intelligence techniques in relation to both fundamental cryptographic concepts and specific applications, particularly image encryption, security, privacy protection, and data processing.

The color-coded structure further reveals several thematic clusters. The blue cluster is strongly associated with image-oriented and computational techniques, including image encryption, Hopfield neural networks, chaotic systems, Lyapunov methods, pixel image enhancement, and encryption algorithms. The green cluster emphasizes broader encryption, neural-network, and cybersecurity topics, including neural networks, encryption, image processing, synchronization, algorithms, and computer security. In contrast, the red cluster is dominated by artificial intelligence and security-related themes such as deep learning, machine learning, convolutional neural networks, privacy, data privacy, authentication, blockchain, and homomorphic encryption. The substantial number of links connecting these clusters indicates strong thematic overlap. It suggests that current research increasingly integrates artificial intelligence methods with cryptographic mechanisms to address challenges involving security, privacy, encryption, and intelligent data processing.

AI techniques and methodological approaches in cryptography

The findings indicate that artificial intelligence techniques applied to cryptography encompass a broad range of approaches, with neural networks, deep learning, machine learning, and optimization-oriented computational methods representing the most visible methodological groups in the reviewed literature. The keyword co-occurrence analysis in Figure 9 shows that deep learning, machine learning, neural networks, and convolutional neural networks are strongly connected with cryptography, encryption, security, and image encryption. This pattern indicates that AI in cryptography is not limited to a single learning paradigm but involves several computational approaches adapted to different cryptographic requirements. Neural-network-based methods are particularly prominent in the literature, especially for image encryption, where neural architectures are combined with chaotic systems, synchronization mechanisms, and nonlinear dynamics. For example, Wen et al. (2015) investigated switched neural networks for image encryption, while Chen et al. (2016) applied reaction–diffusion neural networks to image encryption. Prakash et al. (2016) similarly examined Markovian jumping inertial neural networks and their application to image encryption. These studies show that researchers have explored neural networks not only as conventional predictive models but also as dynamic computational structures for constructing or supporting encryption mechanisms.

Deep learning represents another important AI approach identified in the literature. Unlike earlier neural-network studies that frequently relied on specific architectures and mathematical synchronization or chaotic properties, deep-learning approaches utilize multilayer representation learning to support more complex encryption and decryption processes. Ding et al. (2021), for instance, proposed DeepEDN, a deep-learning-based image encryption and decryption network for the Internet of Medical Things, demonstrating how deep learning can secure medical image transmission. Ding et al. (2022) subsequently introduced DeepKeyGen, which applied deep learning to generate stream-cipher components for medical image encryption and

decryption. The presence of these studies among the highly cited publications in Table 4 indicates substantial scholarly attention toward deep-learning-based cryptographic approaches. At the same time, the literature also shows that deep learning is strongly associated with privacy-preserving machine learning, not only encryption generation. Phong et al. (2018) investigated privacy-preserving deep learning using additively homomorphic encryption, while Lee et al. (2022) examined fully homomorphic encryption for deep neural networks. These studies highlight an important distinction within RQ1: AI can construct or improve cryptographic mechanisms, while cryptography can also secure AI computation and data. Therefore, deep learning occupies a bidirectional position in the AI-cryptography relationship.

The reviewed literature further indicates that AI applications in cryptography increasingly involve hybridization rather than isolated algorithms. Researchers frequently combine neural networks with chaos theory, memristive systems, fuzzy systems, synchronization mechanisms, and other nonlinear computational techniques to generate complex encryption behavior. For example, Wang & Li (2019) developed a color image encryption algorithm based on a Hopfield chaotic neural network, while Man et al. (2021) proposed a double image encryption algorithm combining neural networks and chaos. Chen et al. (2020) investigated fractional-order discrete neural networks for image encryption, and Lai et al. (2023, 2024) extended this direction through multiscroll memristive Hopfield and memristive neural networks for image encryption. These studies suggest that the role of AI in cryptography extends beyond conventional supervised or unsupervised learning and includes AI-inspired nonlinear computational structures capable of generating complex transformations. In parallel, machine learning has been incorporated into privacy-preserving architectures involving homomorphic encryption and federated learning, as Fang & Qian (2021) show, while Wood et al. (2021) reviewed homomorphic encryption for machine learning applications in medicine and bioinformatics. Thus, the synthesis for RQ1 shows that the AI-cryptography literature comprises several methodological streams, with neural networks and deep learning particularly prominent. In contrast, hybrid neural, chaotic, memristive, and privacy-preserving approaches reflect the field's tendency to combine learning mechanisms with cryptographic or nonlinear mathematical structures.

Cryptographic applications and problem domains addressed by AI

The findings indicate that artificial intelligence has been applied to a diverse range of cryptographic problems, with image encryption, privacy-preserving computation, secure data processing, cryptographic algorithm development, and encryption/decryption emerging as prominent application areas. The keyword network in Figure 9 supports this finding, showing strong associations among cryptography, image encryption, encryption, deep learning, neural networks, security, and privacy. Image encryption appears particularly prominent within the reviewed literature. This pattern also appears in the highly cited publications in Table 4, where numerous studies investigate neural-network-based or AI-assisted image encryption. Wen et al. (2015) applied switched neural networks to image encryption, while Chen et al. (2016) investigated reaction-diffusion neural networks for the same purpose. Prakash et al. (2016) further explored Markovian jumping inertial neural networks in image encryption. Subsequent studies expanded this direction through Hopfield chaotic neural networks (X.-Y. Wang & Li, 2019), fractional-order neural networks (L. Chen et al., 2020; Xu et al., 2022), and neural networks combined with chaotic systems (Man et al., 2021). These findings suggest that image encryption is an important application domain

because AI-based and nonlinear computational structures can be incorporated into the transformation and diffusion processes required to protect digital images. The continued appearance of image-encryption studies across different years also indicates that this application remains an active research area within the broader AI-cryptography landscape.

A major application domain is privacy-preserving artificial intelligence and secure computation, where cryptographic techniques protect AI models, training data, and computational processes. This differs from using AI to construct encryption mechanisms because the primary objective is to use cryptography as a security layer for AI-based computation. Phong et al. (2018), which received the highest citation count in the dataset, investigated privacy-preserving deep learning through additively homomorphic encryption. Similarly, Fang & Qian (2021) examined combining homomorphic encryption and federated learning for privacy-preserving machine learning, while Lee et al. (2022) investigated fully homomorphic encryption for deep neural networks. Wood et al. (2021) further examined the application of homomorphic encryption to machine learning in medicine and bioinformatics. These studies demonstrate that the relationship between AI and cryptography is bidirectional: AI can be incorporated into cryptographic mechanisms, while cryptographic techniques can simultaneously provide confidentiality and privacy protection for AI operations. The application domains also extend to sensitive environments such as healthcare, where privacy-preserving computation is particularly relevant because AI systems may process confidential medical information. Ali et al. (2022), for example, combined blockchain-enabled searchable encryption with neural networks in an industrial IoT-based healthcare system. Consequently, the literature shows that AI-cryptography research is not limited to developing encryption algorithms; it also encompasses broader secure-computing architectures designed to protect data and AI processes.

The synthesis identifies secure communication, IoT, medical systems, and other data-intensive digital environments as key application domains. The reviewed studies show that researchers increasingly investigate AI-based cryptographic mechanisms in contexts where large volumes of sensitive data must be securely stored, transmitted, or processed. Ding et al. (2021) developed a deep-learning-based image encryption and decryption network specifically for the Internet of Medical Things, illustrating how AI-based encryption can be integrated into distributed healthcare environments. Ding et al. (2022) subsequently focused on stream-cipher generation for medical image encryption and decryption, further demonstrating the application of AI within healthcare-oriented cryptographic systems. Wang et al. (2024) investigated a high-dimensional memristive neural network and its application to commercial data encryption communication, indicating that AI-inspired cryptographic mechanisms can also secure communication and commercial data environments. In addition, Ali et al. (2022) demonstrated the integration of neural networks, searchable encryption, blockchain, and industrial IoT for healthcare systems. Taken together, these findings indicate that AI in cryptography is increasingly moving from individual cryptographic algorithms to application-oriented security architectures. The literature therefore reveals two interconnected directions: AI is used to develop or enhance cryptographic mechanisms, while cryptographic technologies are integrated into AI-driven systems to protect sensitive information. This broad application spectrum shows that AI-cryptography research is closely tied to emerging environments such as IoT, healthcare, cloud and distributed computing, privacy-preserving machine learning, and secure communication, where conventional

static security mechanisms may need to operate alongside adaptive, data-driven computational technologies.

Evaluation methods and performance metrics of AI-based cryptographic approaches

The findings indicate that the evaluation of AI-based cryptographic approaches uses a combination of machine-learning performance metrics, cryptographic security measures, and computational performance indicators. This multidimensional evaluation is necessary because AI-based cryptographic systems must demonstrate not only an AI model's ability to perform a particular task but also the security and efficiency of the resulting cryptographic mechanism. The data-extraction framework developed in this study identifies accuracy, precision, recall, F1-score, computational cost, execution time, entropy, and security measures as important evaluation dimensions. The literature reviewed in Table 4 illustrates this diversity of evaluation objectives. Studies involving neural networks and deep learning for image encryption generally emphasize encryption quality and security. In contrast, studies involving privacy-preserving machine learning place greater emphasis on the effectiveness of the underlying AI model under encryption. For example, Phong et al. (2018); Fang & Qian (2021); and Lee et al. (2022) focus on privacy-preserving machine learning using homomorphic encryption, where preserving machine-learning functionality under encrypted computation is a key consideration. In contrast, studies such as Wang & Li (2019); Chen et al. (2020); Man et al. (2021); and Lai et al. (2023) investigate neural-network- and chaos-based image encryption, where evaluation focuses more closely on the security and statistical properties of encrypted images. This difference shows that evaluation practices are strongly influenced by the specific cryptographic problem and application domain each study addresses.

For image encryption, evaluation commonly emphasizes an algorithm's ability to transform the original image into a ciphertext that exhibits appropriate security characteristics while maintaining acceptable computational performance. Previous studies in the reviewed literature employ neural networks, chaotic systems, fractional-order systems, and memristive architectures to generate complex encryption transformations. For example, Wang & Li (2019) developed a color image encryption algorithm based on a Hopfield chaotic neural network, while Chen et al. (2020) examined a fractional-order discrete neural network for image encryption. Man et al. (2021) combined neural networks and chaos to develop a double-image encryption algorithm, and Xu et al. (2022) applied a fractional-order chaotic Hopfield neural network to image encryption. Lai et al. (2023, 2024) further explored multiscroll memristive neural networks for image encryption. Across this research direction, evaluation is concerned not simply with whether encryption can be performed, but with whether the resulting ciphertext demonstrates characteristics associated with resistance to statistical analysis and effective diffusion and confusion. Measures such as entropy, correlation, computational time, and other security-related indicators can therefore provide evidence regarding the behavior of an encryption mechanism. This is important because a model that produces encrypted images successfully does not automatically demonstrate cryptographic robustness. Consequently, evaluating AI-based image encryption must consider both the system's functional output and the security properties of the generated ciphertext.

A different evaluation perspective emerges in privacy-preserving machine learning and homomorphic encryption, where computational overhead and model

performance become particularly important. Phong et al. (2018) investigated deep learning under additively homomorphic encryption, while Fang & Qian (2021) examined privacy-preserving machine learning by combining homomorphic encryption and federated learning. Lee et al. (2022) similarly investigated fully homomorphic encryption for deep neural networks, and Wood et al. (2021) examined homomorphic encryption for machine learning in medical and bioinformatics applications. In these studies, evaluations must consider the trade-off between privacy protection, model performance, and computational efficiency. Encryption can increase computational complexity, communication requirements, and execution time, potentially affecting the practical deployment of AI models. Therefore, measures such as accuracy and other predictive-performance indicators should be considered alongside computational cost, execution time, and the overhead introduced by cryptographic operations. Overall, the synthesis for RQ3 indicates that no single evaluation metric is sufficient to assess AI-based cryptographic approaches. A comprehensive evaluation should consider AI effectiveness, cryptographic security, and computational efficiency simultaneously. This multidimensional perspective matters for future research because improvements in one dimension may introduce trade-offs in another; for example, stronger cryptographic protection may increase computational overhead, while a more complex AI architecture may improve encryption or prediction performance but require more computational resources. Thus, the evaluation approaches identified in the literature show the need for standardized, application-specific assessment frameworks that can evaluate the security, effectiveness, and practical feasibility of AI-based cryptographic systems simultaneously.

Technical, computational, methodological, and security challenges

The findings indicate that applying artificial intelligence to cryptography creates several technical and computational challenges because integrating learning algorithms with cryptographic mechanisms is complex. AI-based approaches, particularly deep learning, neural networks, and hybrid architectures, may require substantial computational resources for model training, parameter optimization, and encryption or decryption operations. This issue becomes more significant when AI-based cryptographic systems are deployed in resource-constrained environments such as IoT and edge devices. For example, studies by Ding et al. (2021) and Ding et al. (2022) demonstrate the application of deep learning to medical image encryption and stream-cipher generation. However, these approaches operate in environments where computational efficiency and secure data processing remain key considerations. Similarly, homomorphic encryption adds computational overhead because encrypted data must be processed without decryption. Phong et al. (2018); Fang & Qian (2021); Lee et al. (2022); and Wood et al. (2021) demonstrate the potential of homomorphic encryption for privacy-preserving AI. However, this research direction also highlights the computational complexity associated with performing machine-learning operations over encrypted data. Therefore, one recurring challenge in the literature is achieving an appropriate balance between cryptographic security, AI performance, and computational efficiency.

A challenge concerns methodological consistency and the difficulty of establishing comparable evidence across studies. The literature reviewed in this study encompasses substantially different AI techniques, cryptographic problems, datasets, experimental environments, and evaluation criteria. For image encryption, researchers may emphasize entropy, correlation, encryption quality, and computational time,

whereas privacy-preserving machine-learning studies may prioritize model accuracy, privacy protection, communication overhead, and execution cost. Studies such as Wang & Li (2019); Chen et al. (2020); Man et al. (2021); and Lai et al. (2023, 2024) employ different combinations of neural networks, chaotic systems, fractional-order models, and memristive architectures. Consequently, directly comparing their reported performance is difficult because improvements are often demonstrated under different experimental conditions. A related methodological issue is how datasets, parameter settings, experimental environments, and evaluation procedures are described and reproduced. This issue is particularly relevant to the quality assessment framework developed in the present study, which explicitly evaluates whether datasets or experimental environments, evaluation metrics, AI methodologies, cryptographic problems, and limitations are adequately reported. The diversity of methodological approaches therefore represents both a strength and a challenge: it demonstrates the breadth of research in the field. However, it makes it difficult to establish standardized benchmarks and determine whether one approach provides consistently reproducible improvements across different cryptographic applications.

Another challenge is ensuring security and distinguishing experimental effectiveness from cryptographic security. Using AI or neural networks in an encryption system does not inherently guarantee resistance to cryptanalysis or other attacks. Many studies in the reviewed literature investigate image encryption using neural networks, chaos, fractional-order systems, and memristive structures, including Wen et al. (2015); Chen et al. (2016); Chen et al. (2020); Man et al. (2021); and Lai et al. (2023, 2024). These approaches show how AI-related computational structures can contribute to complex encryption mechanisms. However, their security must be evaluated against appropriate cryptographic criteria, not solely by successful encryption or ciphertext statistical properties. The challenge grows more complex because AI systems can be vulnerable to attacks, while AI can also be used for cryptanalysis, vulnerability discovery, and attack detection. Radanliev (2024), for example, highlights the evolving relationship between artificial intelligence and quantum cryptography, illustrating that emerging computational technologies create both opportunities and security considerations for cryptographic systems. Similarly, the broader cybersecurity perspective discussed by Achuthan et al. (2024) emphasizes that AI introduces a range of security and privacy considerations across digital systems. Thus, the synthesis for RQ4 indicates that future AI-based cryptographic research must address three interconnected dimensions: technical scalability, methodological reproducibility, and cryptographic security assurance. Addressing these challenges requires evaluation frameworks that go beyond model performance and demonstrate whether AI-based cryptographic mechanisms remain secure, efficient, reproducible, and practical under realistic operational and adversarial conditions.

Emerging research directions and future opportunities

The reviewed literature suggests that one emerging research direction is developing more adaptive, efficient, and integrated AI-based cryptographic systems. The increasing publication output shown in Figure 2, particularly the substantial growth from 2023 to 2025, indicates expanding research activity at the intersection of artificial intelligence and cryptography. Methodologically, the literature has shifted from applying individual neural-network structures to more complex hybrid architectures involving deep learning, chaotic systems, memristive neural networks, and other nonlinear computational mechanisms. Studies by Lai et al. (2023, 2024), for example, demonstrate

continued development of multiscroll memristive neural networks for image encryption, while Ding et al. (2021, 2022) demonstrate the use of deep learning for medical image encryption and stream-cipher generation. These developments suggest that future research can further investigate AI architectures that simultaneously address security, computational efficiency, and adaptability. Rather than focusing exclusively on improving individual encryption mechanisms, future studies may increasingly examine integrated architectures in which AI dynamically supports cryptographic parameter selection, key management, encryption processes, attack detection, and security optimization. Such approaches are particularly relevant for IoT, edge computing, healthcare, and distributed environments where cryptographic systems must operate under changing conditions and resource constraints.

An important research direction is developing privacy-preserving AI through advanced cryptographic mechanisms, particularly homomorphic encryption, federated learning, and other privacy-enhancing technologies. The high citation counts of Phong et al. (2018); Fang & Qian (2021); Lee et al. (2022); and Wood et al. (2021) show strong scholarly interest in protecting AI computation and data through cryptographic techniques. These studies suggest that the future relationship between AI and cryptography will not be limited to using AI to develop encryption algorithms; instead, cryptography will increasingly serve as a security foundation for AI systems that process sensitive, distributed data. This direction is particularly relevant to healthcare, bioinformatics, IoT, and cloud-based machine learning, where data cannot always be transferred or processed in plaintext. Future research can therefore explore ways to reduce the computational and communication overhead of encrypted machine learning while maintaining meaningful privacy guarantees. Further research may also examine combinations of homomorphic encryption, federated learning, blockchain, and AI, extending the type of integrated architecture explored by Ali et al. (2022). The key research opportunity is to develop privacy-preserving AI systems that are not only theoretically secure but also computationally practical for real-world deployment.

An emerging direction concerns advanced cryptographic security in the context of evolving AI capabilities and emerging computing paradigms. The bidirectional relationship identified throughout this review indicates that AI can serve both as a mechanism for strengthening cryptographic systems and as a computational tool for analyzing or discovering cryptographic weaknesses. This creates a continuing need to investigate AI-assisted cryptanalysis, intelligent vulnerability assessment, adaptive attack detection, and automated security analysis alongside AI-enhanced cryptographic design. Radanliev (2024) further identifies the relationship between artificial intelligence and quantum cryptography as an emerging research area, suggesting that the interaction between AI and next-generation cryptographic technologies warrants continued investigation. Future research can consequently explore how AI techniques can support cryptographic systems designed for emerging computational environments while also examining whether advances in AI create new threats to existing cryptographic assumptions. In addition, the geographical and collaboration patterns shown in Figures 6 and 8 indicate a broad international research landscape, with substantial contributions from China, India, the United States, South Korea, Saudi Arabia, and other countries. This provides opportunities for greater cross-disciplinary and international collaboration to establish common datasets, standardized evaluation protocols, security benchmarks, and reproducible experimental environments. Overall, RQ5 suggests that future research will likely move toward intelligent, privacy-preserving, adaptive, and application-aware cryptographic systems while also

addressing the security implications of increasingly capable AI technologies. Developing standardized benchmarks and reproducible evaluation frameworks will be important for determining whether these emerging approaches provide consistent improvements across different cryptographic applications and operational environments.

Conclusions

This systematic literature review shows that the application of artificial intelligence in cryptography has become a broad and increasingly active interdisciplinary research area. The findings indicate that neural networks, deep learning, machine learning, and hybrid AI-based approaches are the main techniques used across the literature, with image encryption, privacy-preserving machine learning, secure data processing, healthcare, IoT, and secure communication as major application domains. The synthesis further shows that AI and cryptography have a bidirectional relationship: AI can support the development, optimization, and analysis of cryptographic mechanisms, while cryptographic techniques such as homomorphic encryption can protect AI models and data. Evaluating these approaches generally involves multiple dimensions, including AI performance, cryptographic security, statistical security properties, computational cost, and execution time. At the same time, recurring challenges include computational overhead, methodological heterogeneity, limited comparability between studies, reproducibility issues, and the need for stronger security validation. The increasing publication output, particularly during 2023–2025, further indicates growing research attention to this interdisciplinary field.

The study contributes by providing an integrated taxonomy linking AI techniques, cryptographic problems, application domains, evaluation approaches, challenges, and emerging research directions within a single systematic framework. This perspective extends beyond reviews that concentrate on individual areas such as cryptographic attacks, privacy-preserving machine learning, quantum cryptography, or broader AI-based cybersecurity. The findings provide researchers with a structured overview of methodological patterns and application trends while highlighting the importance of evaluating AI-based cryptographic systems through security, computational, and performance dimensions simultaneously. However, several limitations should be considered when interpreting the findings. First, the review relies primarily on the Scopus database, meaning that relevant publications indexed exclusively in other databases may not have been captured. Second, the review is restricted to English-language articles published between 2015 and 2025 and selected subject areas and document types, which may exclude relevant evidence from other languages, publication formats, or disciplines. Third, the substantial methodological diversity among the reviewed studies limits direct comparison of reported performance because studies frequently use different datasets, experimental environments, metrics, and security-testing procedures. Finally, citation and bibliometric patterns should not be interpreted as direct measures of the technical quality or security strength of individual approaches.

Future research should address these limitations by conducting multi-database systematic reviews that combine Scopus with sources such as Web of Science, IEEE Xplore, ACM Digital Library, ScienceDirect, and other relevant repositories, while explicitly documenting database overlap and duplicate removal. Future reviews could also extend the scope to additional publication languages, document types, and emerging research areas to obtain a more comprehensive evidence base. More importantly, empirical research should develop standardized datasets, evaluation metrics, security benchmarks, and reproducible experimental protocols that enable

meaningful comparison among AI-based cryptographic approaches. Future studies should also investigate the computational trade-offs associated with deep learning, homomorphic encryption, federated learning, and hybrid cryptographic architectures, particularly in resource-constrained IoT, edge, healthcare, and distributed environments. In addition, the field should pay greater attention to adversarial evaluation, cryptanalytic resistance, explainability, key-management security, and emerging technologies such as quantum-resistant cryptography. Such research would help move the field from fragmented experimental demonstrations toward reproducible, scalable, and rigorously validated intelligent cryptographic systems.

References

- Abdewi, M. A., Emara, F. A., Gouda, A. A., & Razek, M. A. (2026). AI-Based Cryptography: A Comprehensive Review of Adaptive Encryption, Neural Cryptanalysis, and Post-Quantum Resilience. *Engineering, Technology & Applied Science Research*, 16(2), 33790–33797. <https://doi.org/10.48084/etasr.16510>
- Achuthan, K., Ramanathan, S., Srinivas, S., & Raman, R. (2024). Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions. *Frontiers in Big Data*, 7. <https://doi.org/10.3389/fdata.2024.1497535>
- Adere, K., Hailu, S., Abebe, M., Kemal, A., Silassie, S. W., Tseghai, A., Haile, G., Tamirat, B., Bitew, W., Regassa, D., Gizachew, Z., & Alemu, W. (2026). A systematic review of artificial intelligence applications in Internet of Things, blockchain, and quantum cryptography. *Discover Artificial Intelligence*, 6(1), 270. <https://doi.org/10.1007/s44163-026-01029-1>
- Ali, A., Almaiah, M. A., Hajjej, F., Pasha, M. F., Fang, O. H., Khan, R., Teo, J., & Zakarya, M. (2022). An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach for Healthcare Systems Using Neural Network. *Sensors*, 22(2), 572. <https://doi.org/10.3390/s22020572>
- Biswas, S., & Raj, M. W. Z. (2024). Quantum-Resistant Cryptographic Protocols Integrated With AI For Securing Cloud And IoT Environments. *International Journal of Business and Economics Insights*, 04(04), 60–90. <https://doi.org/10.63125/dryw3b96>
- Chen, L., Yin, H., Huang, T., Yuan, L., Zheng, S., & Yin, L. (2020). Chaos in fractional-order discrete neural networks with application to image encryption. *Neural Networks*, 125, 174–184. <https://doi.org/10.1016/j.neunet.2020.02.008>
- Chen, W.-H., Luo, S., & Zheng, W. X. (2016). Impulsive Synchronization of Reaction-Diffusion Neural Networks With Mixed Delays and Its Application to Image Encryption. *IEEE Transactions on Neural Networks and Learning Systems*, 27(12), 2696–2710. <https://doi.org/10.1109/TNNLS.2015.2512849>
- Ding, Y., Tan, F., Qin, Z., Cao, M., Choo, K.-K. R., & Qin, Z. (2022). DeepKeyGen: A Deep Learning-Based Stream Cipher Generator for Medical Image Encryption and Decryption. *IEEE Transactions on Neural Networks and Learning Systems*, 33(9), 4915–4929. <https://doi.org/10.1109/TNNLS.2021.3062754>
- Ding, Y., Wu, G., Chen, D., Zhang, N., Gong, L., Cao, M., & Qin, Z. (2021). DeepEDN: A Deep-Learning-Based Image Encryption and Decryption Network for Internet of Medical Things. *IEEE Internet of Things Journal*, 8(3), 1504–1518. <https://doi.org/10.1109/JIOT.2020.3012452>
- Eren, H., Karaduman, Ö., & Gençoğlu, M. T. (2025). Security and Privacy in the Internet of Everything (IoE): A Review on Blockchain, Edge Computing, AI, and Quantum-Resilient Solutions. *Applied Sciences*, 15(15), 8704.

- <https://doi.org/10.3390/app15158704>
- Fang, H., & Qian, Q. (2021). Privacy Preserving Machine Learning with Homomorphic Encryption and Federated Learning. *Future Internet*, 13(4), 94. <https://doi.org/10.3390/fi13040094>
- Gao, X., Mou, J., Banerjee, S., & Zhang, Y. (2023). Color-Gray Multi-Image Hybrid Compression–Encryption Scheme Based on BP Neural Network and Knight Tour. *IEEE Transactions on Cybernetics*, 53(8), 5037–5047. <https://doi.org/10.1109/TCYB.2023.3267785>
- Heidari, A., Rastegar, S. H., & Khonsari, A. (2026). Artificial Intelligence-driven privacy preservation in the internet of vehicles: a comprehensive systematic literature review. *Journal of Big Data*, 13(1), 31. <https://doi.org/10.1186/s40537-025-01360-x>
- Huang, J., Xu, Y., Wang, Q., Wang, Q. (Cheems), Liang, X., Wang, F., Zhang, Z., Wei, W., Zhang, B., Huang, L., Chang, J., Ma, L., Ma, T., Liang, Y., Zhang, J., Guo, J., Jiang, X., Fan, X., An, Z., ... Fei, A. (2025). Foundation models and intelligent decision-making: Progress, challenges, and perspectives. *The Innovation*, 6(6), 100948. <https://doi.org/10.1016/j.xinn.2025.100948>
- Khaleel, Y. L., Habeeb, M. A., Albahri, A. S., Al-Quraishi, T., Albahri, O. S., & Alamoodi, A. H. (2024). Network and cybersecurity applications of defense in adversarial attacks: A state-of-the-art using machine learning and deep learning methods. *Journal of Intelligent Systems*, 33(1). <https://doi.org/10.1515/jisys-2024-0153>
- Lai, Q., Wan, Z., Zhang, H., & Chen, G. (2023). Design and Analysis of Multiscroll Memristive Hopfield Neural Network With Adjustable Memductance and Application to Image Encryption. *IEEE Transactions on Neural Networks and Learning Systems*, 34(10), 7824–7837. <https://doi.org/10.1109/TNNLS.2022.3146570>
- Lai, Q., Yang, L., Hu, G., Guan, Z.-H., & Iu, H. H.-C. (2024). Constructing Multiscroll Memristive Neural Network With Local Activity Memristor and Application in Image Encryption. *IEEE Transactions on Cybernetics*, 54(7), 4039–4048. <https://doi.org/10.1109/TCYB.2024.3377011>
- Lee, J.-W., Kang, H., Lee, Y., Choi, W., Eom, J., Deryabin, M., Lee, E., Lee, J., Yoo, D., Kim, Y.-S., & No, J.-S. (2022). Privacy-Preserving Machine Learning With Fully Homomorphic Encryption for Deep Neural Network. *IEEE Access*, 10, 30039–30054. <https://doi.org/10.1109/ACCESS.2022.3159694>
- Li, H., Li, C., Ouyang, D., & Nguang, S. K. (2021). Impulsive synchronization of unbounded delayed inertial neural networks with actuator saturation and sampled-data control and its application to image encryption. *IEEE Transactions on Neural Networks and Learning Systems*. <https://www.scopus.com/pages/publications/85097773605>
- Man, Z., Li, J., Di, X., Sheng, Y., & Liu, Z. (2021). Double image encryption algorithm based on neural network and chaos. *Chaos, Solitons & Fractals*, 152, 111318. <https://doi.org/10.1016/j.chaos.2021.111318>
- Mani, P., Rajan, R., Shanmugam, L., & Hoon Joo, Y. (2019). Adaptive control for fractional order induced chaotic fuzzy cellular neural networks and its application to image encryption. *Information Sciences*, 491, 74–89. <https://doi.org/10.1016/j.ins.2019.04.007>
- Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. *Knowledge and Information Systems*, 67(8), 6969–7055. <https://doi.org/10.1007/s10115-025->

02429-y

- Phong, L. T., Aono, Y., Hayashi, T., Wang, L., & Moriai, S. (2018). Privacy-Preserving Deep Learning via Additively Homomorphic Encryption. *IEEE Transactions on Information Forensics and Security*, 13(5), 1333–1345. <https://doi.org/10.1109/TIFS.2017.2787987>
- Prakash, M., Balasubramaniam, P., & Lakshmanan, S. (2016). Synchronization of Markovian jumping inertial neural networks and its applications in image encryption. *Neural Networks*, 83, 86–93. <https://doi.org/10.1016/j.neunet.2016.07.001>
- Prangon, N. F., & Wu, J. (2024). AI and Computing Horizons: Cloud and Edge in the Modern Era. *Journal of Sensor and Actuator Networks*, 13(4), 44. <https://doi.org/10.3390/jsan13040044>
- Radanliev, P. (2024). Artificial intelligence and quantum cryptography. *Journal of Analytical Science and Technology*, 15(1), 4. <https://doi.org/10.1186/s40543-024-00416-6>
- Taherdoost, H., Le, T.-V., & Slimani, K. (2025). Cryptographic Techniques in Artificial Intelligence Security: A Bibliometric Review. *Cryptography*, 9(1), 17. <https://doi.org/10.3390/cryptography9010017>
- Trigka, M., & Dritsas, E. (2025). Edge and Cloud Computing in Smart Cities. *Future Internet*, 17(3), 118. <https://doi.org/10.3390/fi17030118>
- Wang, C., Tang, D., Lin, H., Yu, F., & Sun, Y. (2024). High-dimensional memristive neural network and its application in commercial data encryption communication. *Expert Systems with Applications*, 242, 122513. <https://doi.org/10.1016/j.eswa.2023.122513>
- Wang, X.-Y., & Li, Z.-M. (2019). A color image encryption algorithm based on Hopfield chaotic neural network. *Optics and Lasers in Engineering*, 115, 107–118. <https://doi.org/10.1016/j.optlaseng.2018.11.010>
- Wang, Z., & Tabassum, M. (2024). A Holistic Secure Communication Mechanism Using a Multilayered Cryptographic Protocol to Enhanced Security. *Computers, Materials & Continua*, 78(3), 4417–4452. <https://doi.org/10.32604/cmc.2024.046797>
- Wen, S., Zeng, Z., Huang, T., Meng, Q., & Yao, W. (2015). Lag Synchronization of Switched Neural Networks via Neural Activation Function and Applications in Image Encryption. *IEEE Transactions on Neural Networks and Learning Systems*, 26(7), 1493–1502. <https://doi.org/10.1109/TNNLS.2014.2387355>
- Wood, A., Najarian, K., & Kahrobaei, D. (2021). Homomorphic Encryption for Machine Learning in Medicine and Bioinformatics. *ACM Computing Surveys*, 53(4), 1–35. <https://doi.org/10.1145/3394658>
- Xu, S., Wang, X., & Ye, X. (2022). A new fractional-order chaos system of Hopfield neural network and its application in image encryption. *Chaos, Solitons & Fractals*, 157, 111889. <https://doi.org/10.1016/j.chaos.2022.111889>
- Yaqub, M. Z., & Alsabban, A. (2023). Industry-4.0-Enabled Digital Transformation: Prospects, Instruments, Challenges, and Implications for Business Strategies. *Sustainability*, 15(11), 8553. <https://doi.org/10.3390/su15118553>