Nepal Journal of Mathematical Sciences (NJMS)
ISSN: 2738-9928 (*online*), 2738-9812 (*print*)
Vol. 5, No. 1, 2024 (February): 15-28
DOI: https://doi.org/10.3126/njmathsci.v5i1.76443
©School of Mathematical Sciences,
Tribhuvan University, Kathmandu, Nepal

Research Article
Received Date: December12, 2024
Accepted Date: February22, 2025
Published Date: February28, 2025

Security of E-health Image in Cloud Environment Using Hybridization of DNA Cryptography: Systematic Literature Review

Madhav Dhakal[1]* & Subarna Shakya[2]

[1]*Central Department of Computer Science and Information Technology, Tribhuvan University, Nepal*
[2]*Department of Electronics and Computer Engineering, Institute of Engineering, Pulchowk Campus*
Tribhuvan University, Kathmandu, Nepal
Corresponding Author: *madhav.dhakal@mu.edu.np

Abstract: *This study focuses on addressing the critical issue of maintaining the confidentiality of valuable and confidential e-health records during transmission through cloud-based environments. It specifically investigates the hybridization of DNA-based computing with other encryption techniques. A systematic literature review was performed using the concept of the PRISMA framework. In this review, 12 kinds of literature related to the security of e-health images are selected from an initial pool of 1117 literatures from databases such as Science Direct, Springer Link, and Google Scholar. The reviewed studies were examined based on key security criteria, including resistance to statistical, differential, and exhaustive attacks, as well as randomness of pixels in images through entropy analysis. The findings indicate that the integration of DNA cryptography with chaotic maps offers a highly effective solution for enhancing data security during transmission. This hybrid encryption approach meets the minimum security requirements across multiple evaluated parameters, providing robust protection for sensitive e-health image data.*

Keywords: DNA Cryptography, Chaotic map, Cloud environment, e-Health, Data security

1. Introduction

Cloud computing is a mechanism for storing, accessing, and manipulating data over the internet, It has become an integral part of e-Health, e-Learning, e-Governance. The objective of cloud computing is to provide quick, simple data storage and computing service. In today's technology-driven world, all institutions have started to transmit and store confidential data in cloud environments. Maintaining the confidentiality of this data is the most crucial and significant task. To achieve this, it is mandatory to adopt any reliable and trustworthy security technique that ensure the protection of users data. Several cryptographic approaches like symmetric, asymmetric, biometric , quantum , block chain , and other non-cryptographic approaches, including server-side application security, hardware-level security, operating system security have been implemented in cloud computing.

Most of the healthcare organizations adopt cloud computing services to enhance service quality. To address this, they are shifting their operations from a traditional manner to an online service. They began storing data in cloud databases and provide the e-health services, such as telemedicine or smart health care. Cloud databases improve efficiency, but they also offer a significant impact and challenge to the security of shared data. Thus, data stored in the cloud has to be secured in a proper and systematic way.

In e-health, all health-related documents are stored on highly capable storage devices, such as cloud computers or local drives and all confidential details of patients are transmitted to remote areas with the public unsecured network like internet. Such valuable data is then used by the medical entities, just as doctors use those records at every new checkup time and also deliver them to the patient through email whenever necessary. Sukumaran and Mohammed[21] have considered an authentic health record to be the most valuable document in a patient's life. If tiny changes are made unexpectedly, it affects the whole treatment process in the future, which affects not only the health of the patient but also the reputation of the hospital and medical team. For better, faster, and more secure transmission of health-related documents, e-health data must be kept secure and confidential way, and a confidential mechanism for storage is mandatory. Banu et al.[7] have studied that in image data security, large volume of data, data redundancy, and highly correlated adjacent pixel intensities, traditional cryptosystems like AES, RSA are not applicable. Therefore, different image encryption algorithms, including integration of the chaotic system with DNA computing and cellular automata, are used.

In this review, we focus on the security of data using DNA based concepts, either as a standalone method or integration with other innovative techniques. DNA cryptography uses DNA as an information carrier to solve complex problems, including the clique problem of a graph, the directed Hamilton problem of seven vertices, the Turing problem, and the NP-complete problem. In DNA-based cryptography information is secured using the four nucleotides, i.e., Adenine (A*)*, Cytosine (C), Guanine (G), and Thymine (T). Here, Adenine is complementary to Thymine and Cytosine is complementary to Guanine.

The structure of this paper is outlined as follows: Section 2 reviews related studies; Section 3 discusses the motivation and limitations of this study; Section 4 outlines the materials and methods; Section 5 provides a security analysis and its parameters; Section 6 presents results and discussion; and section 7 summarizes the conclusion and future directions.

1.1.Research Questions

The research questions of the study are set as:

- What are the existing hybridization techniques that combine DNA cryptography with other encryption techniques for securing e-health images in cloud environments?
- How effective are hybrid DNA cryptography techniques in mitigating brute force attacks on e-health images transmitted in cloud environments?

1.2.Objectives of the Study

To accomplish the research questions, research objectives of the study are set as:

- To evaluate the effectiveness of hybrid DNA cryptography techniques in mitigating brute force attacks on e-health images transmitted in cloud environment.
- To identify the real-world applications of hybrid DNA cryptography for securing e-health images in cloud environment.
- To evaluate the outcomes of hybrid DNA cryptography in terms of security and usability for securing e-health images.

2. Related Work

The transmission of data using cloud-based technology is increasing everywhere and the risk of data breaches and alternations caused by unauthorized users is also growing at the same rate. Several researchers have published works to address the security of data in cloud environments using the concept of DNA computing and its integration with other innovative techniques. Among them, an overview of some works is listed as follows:

Can et al.[8]have explored innovative cryptographic methods inspired by genetic science base encryption technique to strengthen cloud data security. These methods show promise for enhancing data security but present challenges related to computational complexity and practical implementation within real-time cloud applications. The paper underlines the potential of genetics-based cryptographic techniques to address specific cloud security but also points out gaps in scalability and adaptability, which could hinder widespread adoption. Thus, while genetic cryptography introduces innovative possibilities, further research is needed to resolve these limitations and fully harness its capabilities in large-scale cloud applications.

Sukumaran and Mohammed[21] have proposed the implementation of the DNA-based authentication technique for the awareness of the health record and remedies of childbirth and about pregnant women through the message, voice, and flash alter. The main concept behind this technique is to link the Electronic Health Records (HER) and DNA, which ensure the usability and confidentiality of electronic data and help minimize maternal and infant mortality rates in India.

Le [15] has studied the CS-E2E protocol, a DNA-based authentication approach designed for healthcare services in the Internet of Living Things (IoLT). This protocol enables mutual authentication between patients and establishes a secure, shared key for private communication, bolstered by multiple security measures such as Single Sign-ON (SC-SSO), Elliptic Curve Cryptography (ECC), and bio-hashing. Security analyses demonstrate that CS-E2E is resistant to a range of attacks and maintains cost-efficiency in terms of computational and communicational overhead. However, while the study provides a promising framework for patient authentication, it could benefit from further examination of scalability under high network loads, as well as potential vulnerabilities when integrated with broader IoLT applications.

Joseph and Mohan[14] introduced an innovative algorithm aimed at ensuring secure data sharing in cloud environments by integrating the Grey Wolf Optimization Algorithm (GWOA) with DNA cryptography. The algorithm begins by transforming the data into DNA sequences, followed by the generation of cryptographic keys using GWOA. During the encryption phase, XOR and complementation are applied to the DNA sequences to secure the data. For decryption, reverse operations are carried. The results from various tests indicate that the proposed concept is highly effective and secure during the transmission of data through cloud-based systems.

In the face of escalating cyber threats to electronic health records (EHRs), the research by Banu et al. [7] introduced a robust encryption framework for medical images that leverages DNA subsequences, SHA-256 hashing, and the Hyper Chaotic Multi-Attractors Chen System (HCMACS). The integration of HCMACS generates pseudorandom keys, enhancing the resilience and unpredictability of the encryption. The approach achieves the CIA triad, and its performance has been validated against statistical, differential, and chosen-plaintext attacks, affirming the model's robustness. A key advantage lies in its sensitivity to initial conditions, where secret keys are tightly linked to the hash of the original image, adding an extra layer of security. While the model shows considerable strength in protecting EHR data, its reliance on computationally intensive operations, such as DNA-based encoding and hyper-chaotic mapping, may raise efficiency concerns for real-time applications.

To encrypt the medical images, Dagadu et al. [9] recommended a hybrid chaotic and DNA technology. The cipher image is created by performing a row-by-row diffusion process utilizing the DNA XOR algebraic operation between the plain image matrix and the two chaotic key matrices in an alternating pattern. The DNA encoding and decoding rules are chosen for each row using the logistic map. Experimental findings from statistical, differential, and key studies show that the suggested system is reliable and offers defense against a variety of attacks.

Akkasaligar and Biradar[4] suggested DNA cryptography and the dual hyperchaotic map for maintaining the confidentiality and sensitivity of selected digital images in the medical area. Only a few images are used here due to the large size and longer calculation time of digital images. Confusion and Diffusion mechanisms are used on certain image pixels during the encryption of specific images using this hybrid technology, and then DNA encoding rules are used. This approach requires less computing time and is highly effective for securing e-health images.

In 2021,Elamir et al.[10] proposed a three-stage technique for hiding medical images, where first the information is hidden using the least square bit of pixel, and the resultant image is compressed with the combination of six chaotic maps, namely Chebyshev, Gauss, Logistic, Tent, and Piecewise maps, and then into DNA encoding format. In the DNA encoding technique, e-health images are stored through DNA molecules, so the size of the image is reduced and the data transmission rate is increased.

To maintain healthcare security between patient and doctor, Naing et al. [13] in 2023 proposed a symmetric key encryption algorithm called Key Encryption Decryption (KED) using modulo 92, aimed at protecting Patient Health Information (PHI). This approach combines AES S-box transformations with DNA cryptography for a more robust security framework. Especially, it is designed to resist cryptographic attacks like differential and linear cryptanalysis.

Researchers Qiqieh et al.[19] proposed a DNA-based Cryptographic Security Framework (DNA-CSS) with the concept of Diffie-Hellman key exchange and the Feistel structure of cryptography to improve the health record in cloud environments. This study combines a strong key agreement protocol and encryption algorithm with a new wrapping technique for encryption and decryption techniques. However, the absence of a thorough comparison with other cutting-edge encryption frameworks for medical records and the requirement for practical testing.

3. Motivations and Limitations of the Study

This study examines data security in the e-health sector, focusing specifically on approaches that incorporate the hybridization of DNA-based cryptography with other established security standards. Given the increasing importance of protecting sensitive health information, this review aims to explore how DNA cryptography, a relatively novel approach inspired by the structure and encoding properties of biological DNA, can be integrated with conventional techniques to enhance data security in e-health applications.

A notable limitation of this study is that, despite availability of various data security techniques, the selected literature primarily emphasizes DNA-based cryptography in medical sectors. This restricted focus means that other well-established data security methods used in the e-health sector are not covered in detail, which may limit the generalizability of findings. As a result, this review highlights only a specific subset of security solutions within a broader field.

4. Materials and Methods

This review of the literature covers the data source and search strategy, study selection,& inclusion-exclusion criteria, data extraction mechanism, analysis & publication, and results.

Information source and Search strategy

Preferred Reporting Items for Systematic Review and Meta-Analysis (PRISMA) guideline by Page et al.[18] are followed for this review. At the final stage of these phases, it is assumed that the review process is free of biases and that the final outcome will maintain the consistency and accuracy of the review. Several scientific papers were accumulated from the international standard digital bibliographic databases like Science Direct, Springer Link, and search engine Google Scholar, which are the primary sources for finding the literature related to data security in Images of e-health using the hybrid concepts of DNA cryptography. Searching for data was done from 2020 to December 14, 2023. A total of 1117 pieces of literature are downloaded, and out of them, 672 are from Springer Link, 247 from Science Direct, and 198 from Google Scholar. To find the literature related to our review, "Data security", "DNA cryptography", "Medical Image Encryption", "Cloud Data security", "Chaotic Map" keywords are used with the combination of "AND, OR," and "NOT" operators to narrow or broaden the search. We also searched the literature on the basis of alternative words for the included keywords. Combination of keyword and operator is randomly interchanged until and unless our required literature is not found. Retrieved literature from databases was found via their search engine. In Springer Link and Google Scholar, results were retrieved using the provided export function in CSV format, but in Science Direct, datasets were downloaded in BibTex format, and further with the JebRef tool, they were converted into CSV format, after that, all datasets were compiled in Microsoft Excel with the same file but different worksheets.

Study Selection and Inclusion Exclusion Criteria

Among the various reference management systems, the current study uses Zotero to manage the literature searched from the above databases and search engines. It is open-source software that can be downloaded easily and freely. First, all selected articles are exported into Zotero either by entering their ISDNs, DOIs, or any unique number, or by linking the downloaded file or storing a copy of the file. It merges the results and eliminates any duplication, if any are found. In this systematic review, inclusion/ exclusion, and restriction criteria are listed as: Those literatures are included if 1) they are related to cloud data security, 2) they are related to the images of e-health or with other synonyms 3) original paper, peer review article, conference proceeding paper 4) Studies on hybrid cryptography with DNA cryptography or image encryption 5) written in English and from the field of computer science & Information Technology 6) published between 2020 to December 14, 2023. Studies are excluded if they are: 1) duplicate research papers; or 2) not related to the security of the e-health image. 3) Thesis report 4) non peer-reviewed article; 5) having inadequate information.

Using the PRISMA Framework, 1031 literatures were eliminated by screening titles, abstracts, and published years and the remaining 86 literatures were thoroughly reviewed. 71 of the 86 items were not matched with our review topic, so these are also excluded from our review, and out of the remaining 15 articles, 1 is not in English, 1 is a thesis document, and another 1 does not contain full information. The current systematic review and analysis study employed and included 13 articles. Finally, all selected literature's evaluation factors were examined, and their results were summarized.

Data Extraction

All reviewers studied the inclusion literature for the extraction of data in a systematic way independently, and all of them came together to verify if any uncommon views or confusion were observed between them. To extract the result, each reviewer, contributes equally.

Quality Assessment

During the review process, a critical component of a systematic review of the literature is quality assessment. In this study, each researcher carefully examined and ranked the standard of each abstract independently to assess the quality and maintain the similarities, standard, and unbiased judgment and purification of each selected article. To maintain the quality of the review, only original, peer-reviewed publications and conference proceedings were used. After analyzing and evaluating all relevant articles, all authors evaluate the quality of the research. The numbers of downloaded and reviewed literatures in our study are presented in Fig-1, and the overall steps of the study are given in Fig-2.

Data Synthesis

Synthesis of data is carried out to systematize and aggregate the results of the study. And determine whether the obtained result supports the objective to address the answer of the research question or not.

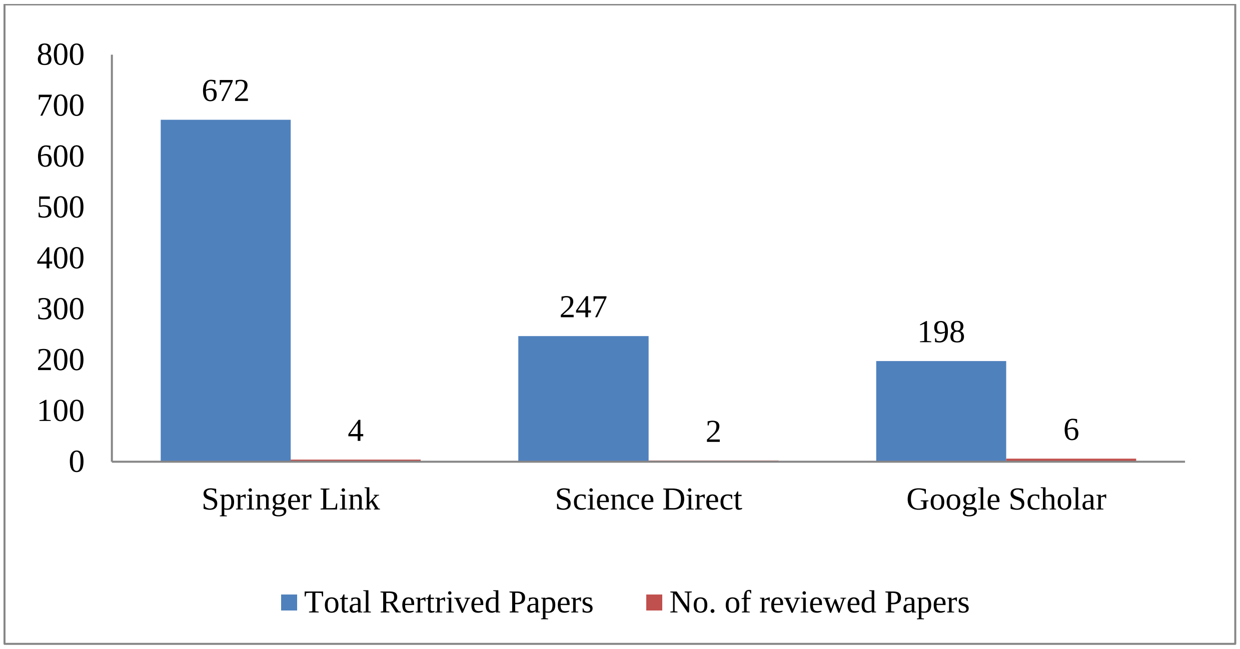

Fig-1: Number of downloaded and selected papers for review

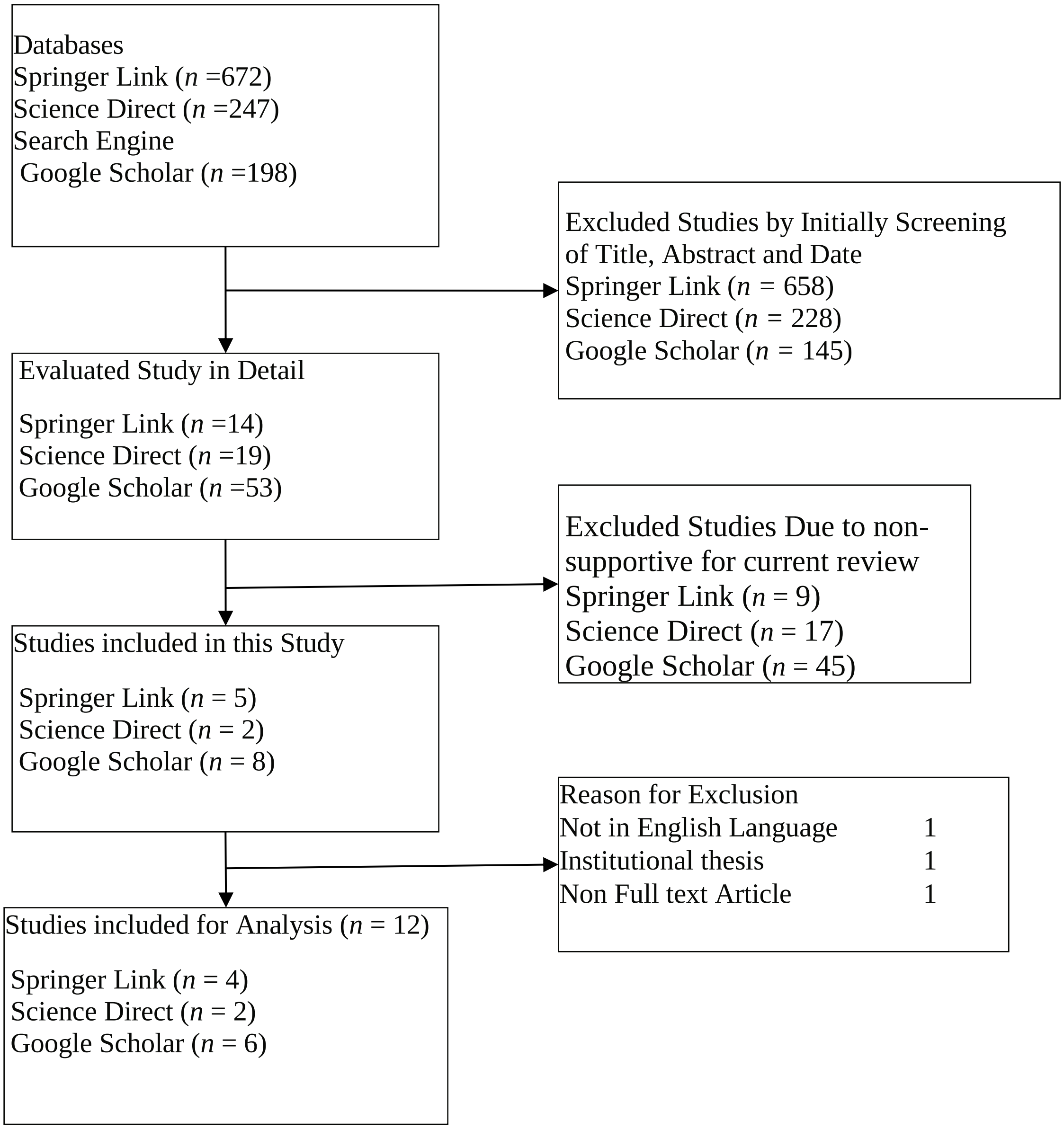
Databases
Springer Link (*n* =672)
Science Direct (*n* =247)
Search Engine
Google Scholar (*n* =198)
Excluded Studies by Initially Screening of Title, Abstract and Date
Springer Link (*n* = 658)
Science Direct (*n* = 228)
Google Scholar (*n* = 145)
Evaluated Study in Detail
Springer Link (*n* =14)
Science Direct (*n* =19)
Google Scholar (*n* =53)
Excluded Studies Due to non-supportive for current review
Springer Link (*n* = 9)
Science Direct (*n* = 17)
Google Scholar (*n* = 45)
Studies included in this Study
Springer Link (*n* = 5)
Science Direct (*n* = 2)
Google Scholar (*n* = 8)
Reason for Exclusion
Not in English Language 1
Institutional thesis 1
Non Full text Article 1
Studies included for Analysis (*n* = 12)
Springer Link (*n* = 4)
Science Direct (*n* = 2)
Google Scholar (*n* = 6)

Fig-2: PRISMA framework for selection of literatures

5. Security Analysis Parameters

All the selected reviewed articles focus on securing medical images by leveraging the hybrid characteristics of DNA cryptography. Result obtained from the secured encrypted image is test over the various parameters including (a) Histogram analysis (b) Correlation analysis (c) Encryption/Decryption time (d)Entropy (e)Unified Average Changing Intensity(UACI)(f) Number of Changing Pixel Rate(NPCR) (g)Mean Square Error(MSE) (h) Peak Signal to Noise Ratio(PSNR) and(i) Structure Similarity Index Measurement(SSIM).

a. **Histogram Analysis:** Histogram analysis is carried out to analyze the pixel distributions in the image. If the distribution of pixel intensities in encrypted image is uniform, the encryption technique is considered secure. Otherwise, an unauthorized person may access the valuable information from the image .

b. **Correlation Analysis:** In image data security, correlation analysis is carried out to determine the quality of the ciphertext image. Correlation analysis is carried out between two adjacent pixels of an image. In the plaintext image, the correlation between neighboring pixels is high (near about 1), i.e., there is, more redundancy, but in a better cryptosystem, the correlation is low (near about 0), which means, that the encrypting algorithm is better. Correlation coefficients are calculated using a formula.

$$r_{x,y}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\ \ \sqrt{D(y)}} \tag{1}$$

$$\mathrm{cov}(x,y) = \quad E\{(x-E(\mathrm{x}))(y-E(y))\} \tag{2}$$

$$E(x) = \ \frac{1}{N}\ \ \sum_{\mathrm{i}=1}^{N} \mathrm{x_i} \tag{3}$$

$$D(x) = \ \frac{1}{N}\ \ \sum_{\mathrm{i}=1}^{N}(x_i - E(x))^2 \tag{4}$$

Where x and $y$are gray scale values of neighboring pixels in the original image and ciphered image with correlation coefficient $r_{x,y}$.

c. **Encryption/Decryption Time:** It is the total time taken for the encryption of the original image and the return to the original image from the cipher image.

d. **Entropy:** Entropy measures the degree of randomness and disorder in data. For an enciphered image of 256 grayscale levels, entropy is 8. Thus, the randomized image has entropy near about 8. Entropy of image is calculated as:

$$H(x) = -\sum_{\mathrm{i}=0}^{255} p(x_i)\mathrm{logp}(x_i) \tag{5}$$

Where, $x_i \in p(x)_i$ is the probability of occurrence.

e. **Unified Average Changing Intensity (UACI):** UACI represents the average change in intensity level in two ciphered images. It is calculated by the equation:

$$\mathrm{UACI} = \sum_{\mathrm{i,j}} \frac{|C_1(\mathrm{i,j}) - C_2(\mathrm{i,j})|}{255 * \mathrm{M} * \mathrm{N}} * 100\% \tag{6}$$

Where C_1 is the encrypted form of original image$O_1$and C_2 is the encrypted image of O_2,where O_2 is obtained by single pixel change in O_1

f. **Number of Changing Pixel Rate (NPCR):**NPCR calculates the number of changing pixels in both the cipher image and the same position. NPCR can be determined as:

$$\mathrm{NPCR} = \frac{\sum_{\mathrm{i,j}} D(i,j)}{\mathrm{MxN}} \times 100\ \% \tag{7}$$

$$\mathrm{D}(i,j) = \begin{Bmatrix} 0 \qquad \mathrm{C_1(i,j)} = \ \mathrm{C_2(i,j)} \\ 1 \quad \mathrm{Otherwise} \end{Bmatrix}$$

If the value of NPCR is small, then it means that there is a small variation between two cipher images. Therefore, the NPCR value must be near 100%.

g. **Mean Square Error (MSE):** MSE calculates the differences between two images. Which is given by the equation as:

$$\mathrm{MSE} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[\ I_1(i,j) - I_2(i,j)\ ]^2}{M \times N} \tag{8}$$

Where I_1 and I_2 are the pixel values of the original and encrypted images, respectively, and (i, j) is the pixel location. M and N are the dimensions of images. If the resultant value obtained from the above equation is large, it means the encryption algorithm is better.

h. **Peak Signal to Noise Ratio (PSNR):** PSNR value is used to check whether noise affects the quality of an image. PSNR is inversely proportional to the MSE of the image. It is calculated as

$$\mathrm{PSNR} = 20 * \log_{10}(\frac{255}{\sqrt{\mathrm{MSE}}})\mathrm{dB} \tag{9}$$

i. **Structure Similarity Index Measurement (SSIM):** To determine the degree of similarities in plaintext image and deciphered image the value of SSIM is use. It is calculated from the equation as:

$$\mathrm{SSIM} = \frac{(2\mu_I\mu_D + C_1) + (2\sigma_{ID} + C_2)}{({\mu_I}^2 + {\mu_D}^2 + C_1)(\sigma_I{}^2 + \sigma_D{}^2 + C_2)} \tag{10}$$

Where C_1, C_2 are constants, (μ_I, μ_D) is the average of deciphered (*D*) and input (*I)* image. Similarly, $({\sigma_I}^2, {\sigma_D}^2)$ is the variance of *I* , *D* and σ_{ID} is covariance between *D* and *I*.

6. Result and Discussion

The key space requires to encode the original message to prevent from the exhaustive attack is listed in Table 1. Here, results from the reviews are placed in structured ways in tabular form and the reviewed literature demonstrates a key space larger than 2^{100}, indicating that each technique provides robust security against brute-force attacks in a cloud environment. This substantial key space ensures that the adopted methods effectively safeguard data by making brute-force attempts computationally infeasible. In some of these selected literatures, key space analysis is not listed but these researches utilize the concept of chaotic system and it demonstrate the initial value sensitivity, it means, when unauthorized person try to access the information with tiny modification in secured key then the image is not decrypted properly. This characteristic shows the robustness in image data security. Trends in publications of literature with their applications, proposed method, and result are expressed as Table 2 and various metrics related with the literatures are listed in Table 3.

These tabulated results addressed the research questions and associated objectives of the present review of e-health image data security in cloud environments based on various security analyses, offering a clear perspective on the evidence gathered and the thematic trends observed.

Table 1. Key Length in Selected Study

References	Key length
Aashiq Banu and Amirtharajan [1]	2^{680}
Adithya and Santhi [2]	2^{128}
Ahuja et al.[3]	2^{448}
Akkasaligar and Biradar [4]	2^{366}
Akkasaligar and Biradar [5]	2^{399}
Alqazzaz et al.[6]	… … ..
Elamir et al. [10]	……
Elamir et al. [11]	……
Ettiyan and Geetha [12]	… ….
Liu et al.[16]	2^{704}
Nezhad et al. [17]	. . … ..
Sarosh et al. [20]	. . … …

Table 2. Summary of Reviewed Article

Ref.	Encryption Technique	Application	Result
Ahuja et al.[3]	DNA computing with Arnold Map	Generate more secure medical images than the lower-dimension chaotic map.	Proposed method provides better protection of the image and visual data in the field of biometric and normal grayscale images.
Akkasaligar and Biradar[5]	DNA computing with dual hyper-chaotic map	Reduce the computation time of image.	Take less computation time. Diffusion and confusion is conducted only for the selected image.
Akkasaligar and Biradar[4]	DNA computing with 4D Lornez chaotic map	Use Discrete Haar Wavelet for lossless compression of images.	Compressed image was changed into four different sub image, which was shuffled using 4D chaotic map,
Adithya and Santhi[2]	DNA computing with chaos map, Knight's Travel map	Applicable for smart healthcare including telemedicine, e-health.	Reduces computing time while offering adequate security. On selected pixels of medical images, the proposed DMIES cryptographic system applies the chaos intertwining logistic map diffusion and confusion process.
Alqazzaz et al.[6]	DNA computing with hyperchaotic RKF-45	Application in image data security in e-health system.	Ciphertexts' efficiency and unpredictability were increased by using DNA addition and subtraction operations.

Liu et al.[16]	DNA computing with SHA-512	Encrypt medical image using the integration of chaotic properties and Sin-Arcsin-Arnold Multi Dynamic random nonadjacent Coupled Map Lattice (SAMCML).	The SAMCML technique secures multi-images with various algorithms. Security analysis results close to optimal values with strong robustness.
Ettiyan and Geetha [12]	Hybrid chaotic DNA and AES encryption	This study focuses on developing a more secure system to prevent security breaches in IoT.	Combining a 3D chaotic map with DNA encoding for enhanced IoT security in medical data transmission. Experimental evaluations demonstrate the system's strong performance and robustness.
Nezhad et al. [17]	DNA sequencing and Tent Chaotic system	Secure fingerprint images during transmission.	Encrypt the fingerprint images using chaotic mapping and DNA sequencing with XOR operations.
Elamir et al. [11]	RSA with DNA Cryptography	To block the unauthorized access from the IoT devices in network. It reconstructs the medical image with high quality.	Enhance image data security in cloud computing, a hybrid approach of RSA with DNA based cryptography.
Sarosh et al. [20]	PWLCM and DNA Cryptography	To maintain the confidentiality of medical images during transmission from IOT devices using the concept of DNA-3D chaos and PWLCM system.	The approach stated in the research leads to lossless medical data recovery. The image obtained through the Map, maintain the security by diffusion the pixel of that image.
Elamir et al. [10]	DNA encoding and Least Significant Bit	Hiding the confidential information of patient's in medical with Least Significant Bit.	Six stages generated key for image compression : Chebysev, Gauss, Henon.Logistic,Tent , and Piecewise maps of chaotic map.
Aashiq Banu and Amirtharajan [1]	DNA and Chaotic Fused approach	Propose a new way of scrambling and then DNA method was used to encrypt the digital image,	Strong resistance to statistical attack, exhaustive attack and others parameters. This study highlights hybrid chaos-DNA based cryptosystem.

Table 3.Security Analysis of Review Article

Ref.	System	Enc / Dec Time	Hist.	Entropy	Cor.	PSNR/MSE	NPCR/UACI (%)
Ahuja et al.[3]	… …	… …	Uniform	7.99	Negative	∞/0	99.95/32.53
Akkasaligar and Biradar[4]	Intel Core i7,7th Generation	14/23	Uniform	7.99	… …	… …	99.72/37.68
Akkasaligar and Biradar[5]	Intel Core i7, RAM:8GB,CPU: 2.70GHz	0.236/0.248	Uniform	7.8446	0.00154/ 0.9946	5.72 / 739.13	99.68/33.55
Adithya and Santhi[2]	Intel Core i5, RAM:4GB CPU: 2.7GHz	0.233/0.243	Uniform	7.9975	… …	7.91/12077.12	99.789/33
Alqazzaz et al.[6]	Intel Core i7-4910MQ, CPU: 2.90GHz , RAM: 16GB	… …	Uniform	7.99	≈ 0	… …	99.603/33.32
Liu et al.[16]	… …	… …	Uniform	7.9994	≈ 0	… …	99/33
Ettiyan and Geetha [12]	AWS cloud server, 1,4GHz processor, MICOT BOARDS	… …	… …	… …	… …	… …	… …
Nezhad et al. [17]	… …	… …	Uniform	7.98	… …	… …	99.60/33.46
Elamir et al. [11]	Dell Core i7, 8 GHz RAM	31.329/18.472	Uniform	… …	0.85746	41.439/ 1.39 e-04	X/32.68
Samiullah et al.[20]	Window 7,core I3, RAM: 4GB	22.43/23.12	Uniform	7.99	Near 0	∞/0	99.62/33.40
Elamir et al. [10]	Intel i7, RAM: 8 GB	Depend upon Image	Uniform	< 8	Near 0	> 11.6 /> 10000	≈ 99 / ≈ 0
AashiqBanu and Amirtharajan [1]	Window 10, Xeon(R) E3–1220 v6 at 3GHz , 32 GB HD	… …	Uniform	7.99	Near 0	∞/0	99.6 / 33.4

7. Conclusion and Future Work

Maintaining the confidentiality of e-health images is one of the most pressing and intriguing challenges in the current landscape. This paper presents a systematic review of techniques for securing medical images, focusing on a hybrid approach that combines DNA cryptography with other methods to protect data during transmission. Twelve articles from various databases and search engines are reviewed based on different security metrics. All selected studies address the security of medical images through the hybrid approach of DNA cryptography. Some of these literatures integrate the DNA computing technique with chaotic system and some other with RSA, and AES. From analyzing key space and other security parameters it is evident that the combination of DNA cryptography with other techniques provides a comparable level of confidentiality for medical images across multiple security parameters. DNA encoding techniques are frequently used alongside chaotic maps and other security measures, with results showing that this combined approach is increasingly effective for image security.

Overall, the reviewed security measures for safeguarding medical data through DNA-based techniques are satisfactory. Looking ahead, this review proposes the development of a new model incorporating DNA based computing and other standard data security measures to further enhance data confidentiality and integrity.

References

[1] Aashiq Banu, S. & Amirtharajan, R. **(2020)**. Tri-level scrambling and enhanced diffusion for DICOM image cipher DNA and chaotic fused approach. *Multimedia Tools and Applications.*, **79(39):** 28807-28824.

[2] Adithya, B. & Santhi, G. **(2022).** A DNA Sequencing Medical Image Encryption System (DMIES) Using Chaos Map and Knight's Travel Map. *International Journal of Reliable and Quality E-Healthcare (IJRQEH).*, **11(4):** 1-22.

[3] Ahuja, B., Doriya, R., Salunke, S., Hashmi, M. F. & Gupta, A. **(2023).** Advanced 5D logistic and DNA encoding for medical images. *The Imaging Science Journal.*, **71(2):** 142-160.

[4] Akkasaligar,P.T. & S. Biradar,S. **(2020).** Medical Image Compression and Encryption using Chaos based DNA Cryptography, *IEEE Bangalore Humanitarian Technology Conference* ., 1–5.

[5] Akkasaligar, P. T. & Biradar, S. **(2020).** Selective medical image encryption using DNA cryptography.

Information Security Journal: A Global Perspective., **29(2):** 91-101.

[6] Alqazzaz, S. F., Elsharawy, G. A. & Eid, H. F. **(2022).** Robust 4-D Hyperchaotic DNA Framework for Medical Image Encryption. *International Journal of Computer Network & Information Security.*, **14(2):**67-76.

[7] Banu, S. A., Al-Alawi, A. I., Padmaa, M., Priya, P. S., Thanikaiselvan, V. & Amirtharajan, R**. (2024).** Healthcare with datacare—a triangular DNA security. *Multimedia Tools and Applications.*, **83(7):** 21153-21170.

[8] Can, O., Thabit, F., Aljahdali, A. O., Al-Homdy, S. & Alkhzaimi, H. A. (**2023**). A comprehensive literature of genetics cryptographic algorithms for data security in cloud computing. *Cybernetics and Systems.*, 1-35.

[9] Dagadu, J. C., Li, J. P. & Aboagye, E. O. **(2019)**. Medical image encryption based on hybrid chaotic DNA diffusion. *Wireless Personal Communications*, **108:** 591-612.

[10] Elamir, M. M., Al-atabany, W. I. & Mabrouk, M. S. **(2021).** Hybrid image encryption scheme for secure E-health systems. *Network Modeling Analysis in Health Informatics and Bioinformatics*., **10(1):**35.

[11] Elamir, M. M., Mabrouk, M. S. & marzouk, S. Y. **(2022).** Secure framework for IoT technology based on RSA and DNA cryptography. *Egyptian Journal of Medical Human Genetics*, **23(1):** 116.

[12] Ettiyan, R. & Geetha, V. **(2023).** A hybrid logistic DNA-based encryption system for securing the Internet of Things patient monitoring systems. *Healthcare Analytics*.,**3:** 100149.

[13] Naing,H.H., Aye,Z.M. & Naing,S.K**.(2023).** E-Health System Based KED and DNA Cryptosystem, *IEEE Conference on Computer Applications.*, 169-173.

[14] Joseph, M. & Mohan, G. **(2022).** A Novel Algorithm for secured data sharing in cloud using GWOA-DNA cryptography. *International Journal of Computer Networks and Applications.*, **9(1):** 114-124.

[15] Le, T. V. **(2023).** Cross-server end-to-end patient key agreement protocol for DNA-based U-healthcare in the internet of living things. *Mathematics*., **11(7):** 1638.

[16] Liu, H., Teng, L., Zhang, Y., Si, R. & Liu, P. **(2024).** Mutil-medical image encryption by a new spatiotemporal chaos model and DNA new computing for information security. *Expert Systems with Applications*., **235:** 121090.

[17] Nezhad, S. Y. D., Safdarian, N. & Zadeh, S. A. H. **(2020).** New method for fingerprint images encryption using DNA sequence and chaotic tent map. *Optik*, **224:** 165661.

[18] Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D. & Moher, D. **(2021).** The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *bmj*, 372.

[19] Qiqieh, I., Alzubi, J. & Alzubi, O. **(2025)**. DNA cryptography based security framework for health-cloud data. *Computing*.,**107(1):** 35.

[20] Sarosh, P., Parah, S. A. & Bhat, G. M. **(2022)**. An efficient image encryption scheme for healthcare applications. *Multimedia Tools and Applications*., **81(5):** 7253-7270.

[21] Sukumaran, S. C. & Misbahuddin, M. **(2018).** DNA Cryptography for Secure Data Storage in Cloud. *Int. J. Netw. Secur.*, **20(3):** 447-454.

□□