A Systematic Literature Review on Security Challenges In Image Encryption Algorithms for Medical Images

Nora Almalki[1†] and Hatim Alsuwat[1†],
S44380307@st.uqu.edu.sa Hssuwat@uqu.edu.sa
[1] Department of Computer Science, College of Computer and Information Systems,
Umm Al-Qura University, Saudi Arabia

Summary
Medical data is one of the data that must be kept in safe containers, far from intrusion, viewing and modification. With the technological developments in hospital systems and the use of cloud computing, it has become necessary to save, encrypt and even hide data from the eyes of attackers. Medical data includes medical images, whether they are x-ray images of patients or others, or even documents that have been saved in the image format. In this review, we review the latest research and the latest tools and algorithms that are used to protect, encrypt and hide these images, and discuss the most important challenges facing these areas.

Keywords:
Medical Image , Encryption , Steganography.

1. Introduction

Medical data is one of the most important data that must be preserved from unauthorized access and modification, because any modification may harm human lives. Radiation is one of the most important medical procedures in which internal problems in the body are discovered, and it is one of the types of patient data that is forbidden to be viewed by non-authorized persons. Storing this medical data in unsafe containers may make it easier for unauthorized persons to access and modify it, and this may endanger people's lives, such as prescribing the wrong medicines or performing wrong medical procedures, and it is also considered a failure to maintain the privacy and confidentiality of patient data. In recent years, interest in encrypting medical data has increased, including these medical images, which are divided into two main parts: color and grayscale[1].

Encryption is the science of hiding data and protecting it from unauthorized access and modification [2]. Data encryption has many ways and multiple algorithms. Anyone who does not have the secret decryption key will not be able to read the sent messages. Just as the idea of text encryption depends on scattering letters and writing meaningless text, the idea of encrypting images depends on scattering the pixels to make the image look chaotic and meaningless. There are two main operations in Image encryption : confusion and diffusion as shown in figure1.

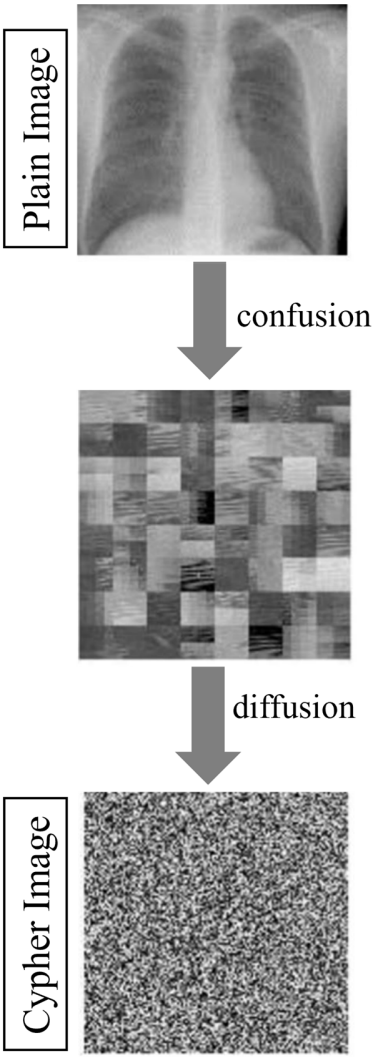

Fig. 1 Medical image encryption[6].

The chaotic images arouse the curiosity of the attackers and push them to try to crack the code and restore the image to its original form, so the principle of hiding encrypted images appeared. Steganography or hiding the encrypted text inside another image is an idea to give the

Manuscript received June 5, 2022
Manuscript revised June 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.6.13

message more security to ensure that it is not accessed by unauthorized persons[3].
Many algorithms have been introduced to encrypt images, but they may be broken by attackers. This research aims to know the challenges facing the protection of medical images by encrypting or hiding these files. This review presents some of the recent studies in this field to reveal the most important challenges that researchers faced. This review aims to identify the current gaps in the medical systems that protect patient data. This review also aims to give researchers ideas to work on more research to advance this aspect.

This paper is organized as follows. In section 2, background. Section 3, related works. Section 4, methodology. Section 5 result and discussion. conclusion in section 6.

2. Background

Since the ancient era, the idea of encrypting important messages began to prevent access to them by unauthorized persons, such as messages between military personnel in wars. In the era of computing and the Internet, and with technological services such as storing data and correspondence, conducting operations, and bank transfers, the risks of data theft and forgery increase, and this makes our age more in need of such methods of encrypting messages and important data. This prompted scientists to think of more feasible solutions to preserve this highly confidential data. From here, the idea of data encryption was launched, and different types of encryption emerged.
The term cipher comes from the Greek language, Kryptos meaning secret. The word graphein means writing. In most cases, we do not care if someone is listening in on our words or not, but in certain cases, the speech is strictly confidential and it is necessary to protect it from strangers. In such a case, encryption is used. Encryption is defined as a specific method and technique for securely transmitting data between two parties, the sender and the receiver, with the guarantee of non-interference from unauthorized third parties. Encryption depends on a specific algorithm, a message, and a key for encryption and decryption. The principle of encryption is to convert the message into an incomprehensible format, and when the key is used for decryption, the message returns to its original state. The original message is called plaintext, and the encrypted message is called cyphertext. Figure 2 shows the encryption and decryption method[4].

Encryption is to provide protection for information systems, hardware, and software, and to provide the main objectives of computer security, which are integrity, confidentiality, and availability. These three concepts are called the CIA triad. Confidentiality aims at the privacy of information and is to ensure that the data is controlled by authorized persons. Confidentiality also aims to make this information available only to authorized persons.

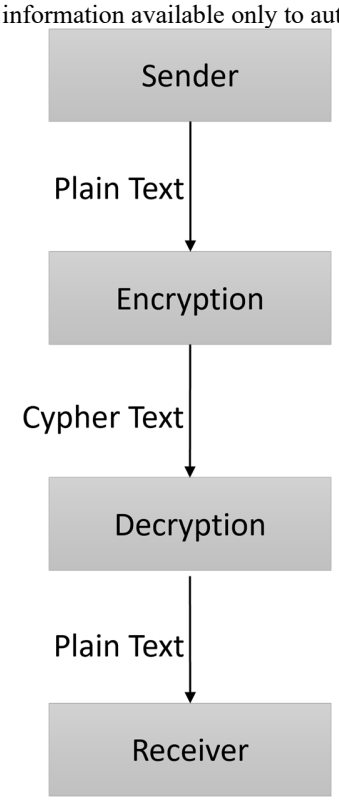

Fig. 2 Encryption Decryption Method[4].

Integrity Ensures data integrity from unauthorized change which is called data integrity. It also ensures that the system performs the tasks required of it correctly, and this is called system integration. As for availability, it is a concept that guarantees the provision of the required service to users and that it is not disabled or refused to them[5].

Algorithms are divided in terms of types of encryption and decryption keys into symmetrical algorithms or asymmetric algorithms, symmetrical algorithms are those that in the decryption process, the same key is used in the encryption. An asymmetric algorithm is an algorithm that uses a key in encryption that is known to the sender only, and a different key in the decryption process that is known only to the receiver[5].

To increase the security of the algorithm, it is taken into account that brute force can try to guess passwords after knowing the type of algorithm used in encryption. Therefore, algorithms compete in the strength and efficiency of the keys by which messages are encrypted and decrypted[5].

There are two traditional encryption techniques substitution and transposition. Some types rely on the substitution technique only, and there are encryption

algorithms that rely on the transposition technique only. While there are algorithms based on the two technologies together to provide the greatest degree of security and the difficulty of decrypting this data.

In addition to the concept of encryption, which aims to make the message incomprehensible, the concept of steganography, which is to hide the message, appeared. It is possible to hide the letters of a particular message inside another text so that the shape of the original text does not change. Historically, masking techniques such as the use of invisible ink were used until specific chemicals were applied to the paper[5].

3.Related Work

The issue of encrypting images and medical information for patients has become very important, especially with the trend of hospitals in recent years to technology, electronic patient records and cloud storage. We also know that one of the most important procedures that are performed for patients in hospitals are x-rays, CT (Computed tomography) scans, and other types of radiation, which represent important information for patients that must be kept confidential. To keep this data confidential, studies have provided a lot of solutions and algorithms to encrypt these images. The proposed algorithms differ in terms of encryption mechanism, encryption steps and complexity. They also differ in terms of their strength and image quality when decoding. The following presents the latest research and proposed algorithms for encoding grayscale medical images.

Relying on two basic steps in image encryption, which are Confusion and diffusion, the research[6] proposed a new algorithm for coding medical images even that gray or color image . This research aims to achieve the security of medical data and secure images while sending them to health care systems via the Internet of Things. The images are split in this algorithm based on image blocks and various random shuffle patterns. This algorithm used histogram, entropy, correlation coefficient, key space, differential attack, and key sensitivity. This research suggested four steps to implement encryption: first, dividing the image into several parts by suggesting a new method for partitioning, then the process of image distortion, then generating the keys, and diffusion. This algorithm was implemented using MATLAB on a laptop running Windows 7 .This algorithm has proven to be effective compared to the currently used algorithms.

The research[7] presented a symmetric encryption method based on Peace Wise Linear Chaotic Map (PWLCM) and Deoxyribo Nucleic Acid (DNA). First an XOR operation is applied to the image and then the random PWLCM sequences are combined. Then, replace each pixel with a random index. In this paper, the researchers used an encryption scheme based on the use of a secret key using the one-time padding (OTP) method. This algorithm has shown good efficiency in relation to its strength against differential attacks and statistical attacks. This algorithm is effective for secure real-time image transmission over the Internet due to its fast encryption and decryption.

The research[8] proposes a new algorithm called hybrid international data encryption algorithm (HIDEA), which is an algorithm that encrypts data in multiple stages. The first stage uses the Arnold transformation method to get a scrambled image. The next step is to use the international data encryption algorithm (IDEA) and key with 128 bit for encryption. When decrypting, this method is performed in reverse. This experiment was carried out using MATLAB and Windows 10 operating system. This experiment used famous images in this field such as cameraman, Lena, mandril, with dimensions of 512 x 512. To discover the power of this algorithm, multiple experiments were performed for encoding and decoding. More than one test was used to measure the strength and stability of this algorithm, such as additive noise attack analysis and key sensitivity analysis, and it proved to be successful.

The research[9] presents an illustration of the improved chaotic sequence in coding grayscale images. This method combines gray value diffusion and combining pixel position scrambling. This research provides feedback to improve the quality and increase the safety of this algorithm.

The research[10] is concerned with encryption through cloud computing and presents a new idea in the field of chaotic encryption methods Through a homomorphic encryption algorithm. The most common types of attacks are analyzed and a symmetric cipher array is created, then the image encryption instructions are split. This paper used the famous simulation program Matlab7.0 to implement the proposed algorithm. The quality of the algorithm was evaluated by calculating the time taken for both the encoding and decoding process, and then analyzing the statistics. The experimental results showed that the security and accuracy of the symmetric encryption algorithm for encrypting chaotic image data in the cloud computing environment are higher than that of the traditional encryption algorithms.

The research[11] proposes the Latin Square Image Cipher (LSIC) algorithm for grayscale image. This algorithm has several steps: Latin square whitening, then S-box, P-box, then LSB noise embedding for probabilistic encryption. It encodes the byte instead of the bit, which gives it more efficiency. This study seeks to provide an algorithm with better noise characteristics and better propagation. This algorithm has a large key space. This algorithm give a great security level in terms of UACI and entropy of NPCR cipher images as shown in the test result. The tests also proved that this algorithm has a good and effective performance in resisting the famous types of attacks such as the brute force attack because the proposed

algorithm in this research has a very large key length. It also has resistance to ciphertext and plaintext attacks.
In addition to the concept of encryption, another concept is used, which is steganography, which is the concealment of encrypted messages. The purpose of this masking is to not draw the attention of attackers and to provide more security for encrypted messages. Below we will review the latest research and algorithms developed by researchers that used this concept.

The research [12] suggests a different way of images encryption. The method begins with reducing the size of the image by compressing it. Then the algorithm distorts the image until it becomes meaningless. The last step is to hide the blurred image and embed it in another image to reduce the attention of the attackers. This algorithm showed good performance while reducing the computational cost.
Due to the ease of tampering with data over the Internet, research[13] used data hiding instead of encrypting it or using a watermark. The carrier image and the secret image are combined in this research. Using a genetic algorithm, the appropriate carrier image is selected to include the secret image from a huge database of images. This research used the mat lab 2017 program and stego image. The algorithm achieved a performance improvement of 30-40% compared to the current algorithms.

Using Beta Elliptic Modeling, paper [14] proposes a new method to hide signatures in document images. The new system consists of two steps: include steganography, and extract steganography. Using Binary Robust Invariant Keypoints (BRISK) appropriate locations are selected to embed the data into the host image. Using L3iDocCopies benchmarks, standard grayscale test images, and Tobacco800, it is found that this algorithm has outperformed similar algorithms in terms of Human Visual System (HSV), and Structural Similarity Index Matrix (SSIM), and Peak Signal to Noise Ratio (PSNR). The paper[15] proposes a system that uses a binary curve to process sensitive images based on color spaces. This system uses the Harvard Whole Brain Atlas database. EMOTE image encryption is based on three levels of encryption techniques. The first stage is Using rule-based logistic coding to obscure the original image. In the second stage, DNA coding is used to encode the masked image. In the third stage, an ECC encoder is used to encode the resulting image. Each of these stages provides a level of safety, and thus medical images receive a higher level of confidentiality. Attempting to crack this code with brute force requires at least 232 trials per stage. To decode the image, the steps are repeated in reverse. The algorithm was tested by scalable statistical analysis and showed that it is more suitable for medical image processing.

The paper[16] proposes a new GAN-based spatial cloaking scheme that performs simulation experiments on grayscale images. It differs from GAN-based steganography in that it uses linear convolutional neural networks in order to create generators. The research shows that this scheme is superior to GAN-based steganography in terms of the ability to combat steganography. This scheme is a supervised learning method in which training samples are inserted so that it can learn the optimal discrimination model. Using different cloaking analysis tools, this chart shows an improvement in the ability of anti-hijacking analysis. In terms of anti-steganography, it showed better performance by building the U-NET architecture.

In paper[17], propose a patented and copyrighted digital object watermarking technology. The watermark is embedded in the digital object by different techniques. In order not to change the quality of the digital object, it is preferable to use a small size watermark. This new and safe technique consists of two steps. In the first step, using a half-size encrypted watermark to embed the encrypted digital object, the XOR operation is used in the encoder. In the second step, watermark the unencrypted digital object taken from the first stage using LSB masking in order to include encrypted confidential information.

4. Methodology

A systematic literature review is a method used to interpret and evaluate previous studies related to a specific field or research question whose answer we want to know[18]. By conducting an SLR, we can summarize the current research and count its benefits and gaps, making it easier for other researchers to work, clarifying the current business gaps, and helping them to find solutions in future research. In the beginning, each research is studied independently and the required data is extracted, then the results are combined and evaluated at the end of the SLR.

4.1 Planning the review

The planning of this review study includes research questions, selection of the sources and keywords, and the criteria of inclusion and exclusion. In the following sections, we review the questions that prompted us to search for answers and make comparisons between research, the method of extracting appropriate research from scientific sources, and how these research were sorted and classified for use in this review.

4.2 Research question

In this review, we seek to reveal the challenges facing medical image encryption. We review the latest research and algorithms developed by researchers to encrypt medical images by reviewing the strengths and weaknesses of each algorithm and evaluating the best and most effective algorithm in this field. We try to answer several questions regarding the security of medical images, as it is one of the important patient data. We review the most important challenges they face. Are they safe? Is it sufficient to protect

against unauthorized access, alteration, and access? Are there current gaps that need to be addressed and developed? Based on this, the research questions were formulated as follows:
Q1: What are the problems faced by encryption medical images?
Q2: What are the problems faced by steganography medical images?
Q3: Is it better to encrypt or hide?

4.3 Selection of the sources and keywords

This paper use IEEE, Science Direct, Springer, and google scholar by using the Saudi Digital Library (SDL) to find resources. we search using "Medical Images Encryption " and " Grayscale Medical Images Encryption" keywords. We could not access some of the sources in IEEE and Science direct because they are not open access, so we used the open access papers only. Research published in the last five years has been selected to obtain the most recent results. Research titles were reviewed to extract the most relevant research with the research topic. Figure 3 shows how to plan to make this review.

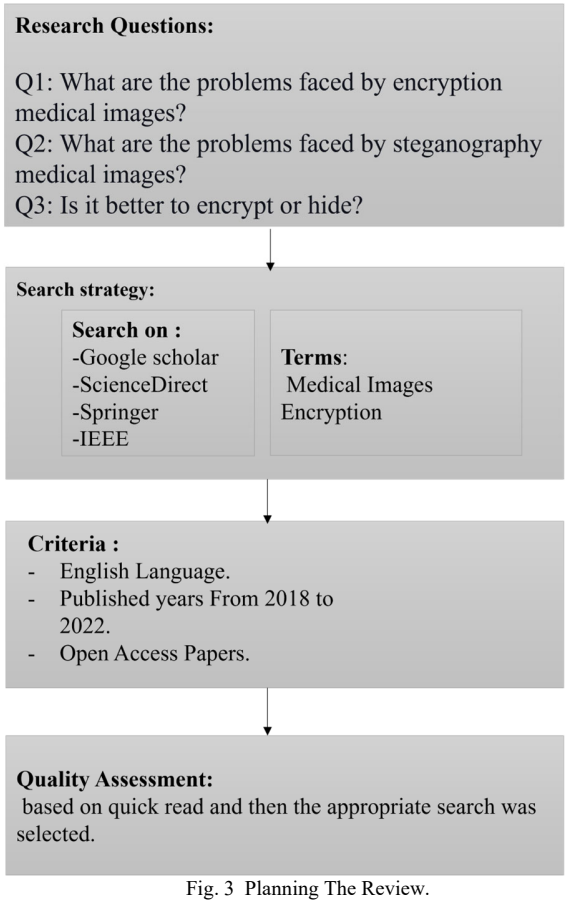

Fig. 3 Planning The Review.

4.4 The criteria of Inclusion and exclusion

When searching in Science Direct for "Medical Images Encryption", 4,640 search results appear, and when filtered to open access, the number of searches becomes 559. When we filtered the results to last five years we found 2201 papers and 358 of them are open access. When searching in Springer for "Medical Images Encryption", 1775 search results appear,1773 in English language. When we filtered the results to last five years we found 1035 papers. When we searching in IEEE for "Medical Images Encryption", 614 search results appear, and when filtered to open access, the number of searches becomes 63. When we filtered the results to last five years we found 295 papers and 63 of them are open access. When searching in Google Scholar for "Medical Images Encryption", 60600 search results appear. When we filtered the results to last five years we found 17600 result. The research in this review was selected based on reading the title and abstract of all research. Researches whose titles are identical to the topic of the review were included, as we excluded any title that did not answer our research questions.

The research extracted from the research process was sorted according to the years in which the research was published, as shown in the figure 4.

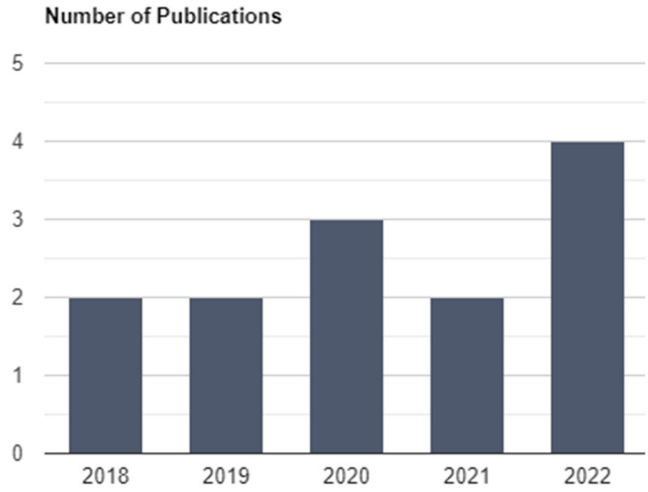

Fig. 4 Number of Publications per years.

The research extracted from the research process was sorted according to the scientific journals in which the research was published, as shown in the figure 5.

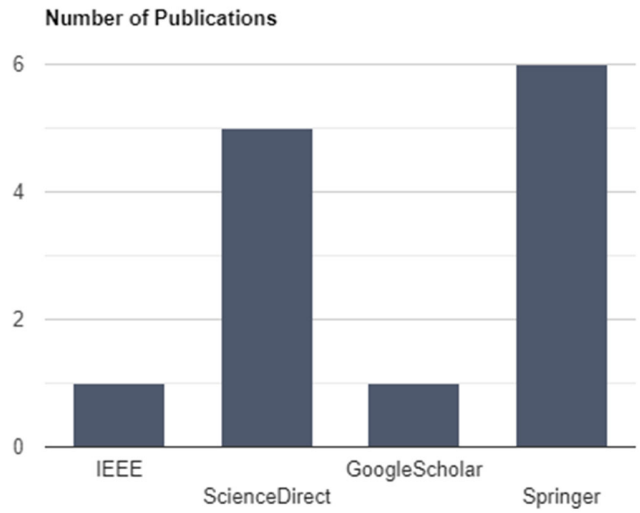

Fig. 5 Number of Publications per Journals.

4.5 Data synthesis and analysis

This part discusses the method of data extraction and analysis in order to answer the required research questions. Based on [19], the word cloud method was used to find out the most frequent words in the selected research. Word cloud is a method based on summarizing text documents and highlighting the most important words, where the largest word represents the most important words. In this research, the most important keywords are what appears in the figure 6.

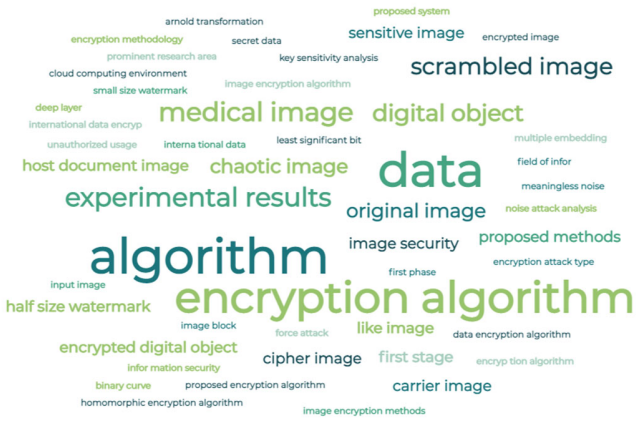

Fig. 6 Word cloud

In Table 1 a review of the techniques and technologies used in the extracted research and the frequency of each technique.

Name of Technique	Technique Frequency
Encryption	13
Steganography	6
Chaos Scheme	2
Cloud Computing	1
Latin Square	1

Table1. Research technologies.

5. Result and Discussion

Thirteen articles were nominated from among the articles that were read and sorted. The research was reviewed in order to answer the research questions and extract the necessary data. The research was divided in terms of the basic idea of protection into two parts, the first part used encryption. The second section used steganography. On the other hand, some research deals with gray images only, and others deal with color medical images. In this section, we made comparisons between these studies in terms of the type of images used, the type of analytical tools that were used, and the problems faced by the research.

5.1 Gray scale and color digital image

The research concerned with the encryption and protection of medical images was divided into two parts, the first section concerned only with grayscale images. The second section is concerned with color images only. The third section deals with grayscale images and color images together. In figure 7, we review the statistics of the research used in this review in terms of the color of the images used in the experiments.

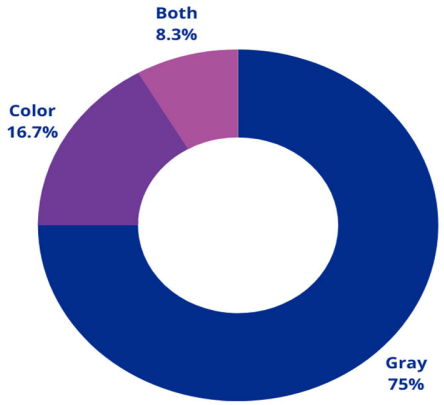

Fig. 7 Gray scale and color digital image statistics

5.2 Result Analysis

To test the strength and efficiency of an encryption algorithm, well-known tests are conducted to prove the efficiency and effectiveness of these algorithms. In the research that was used in this review, many analytical tests were conducted. Statistics show that key space analysis is the most used analysis in research, followed by histogram analysis and correlation analysis, the key sensitivity analysis, then differential attack analysis. The rest of the other types were used only by one research . Figure 8 illustrates the statistic for the use of analyzes in the studies.

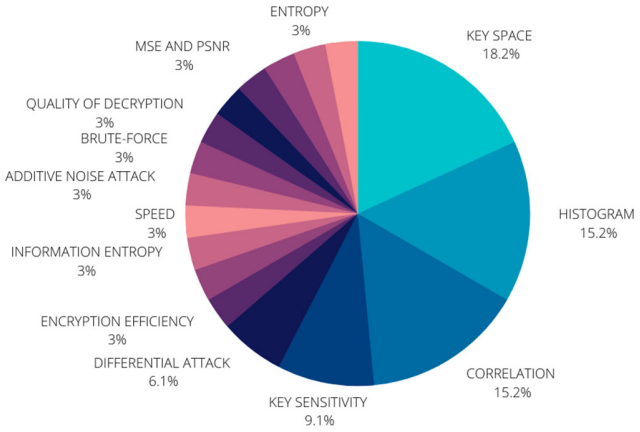

Fig. 8 Analysis statistics

In table2, we review the most prominent analyzes that were conducted on the research presented in this review.

ANALYSIS TYPE	RESEARCH
KEY SPACE	[6], [7], [11], [13], [15], [16]
HISTOGRAM	[6], [7], [8] , [15], [16]
CORRELATION	[6], [7], [11], [15], [16]
KEY SENSITIVITY	[7], [8] , [16]
DIFFERENTIAL ATTACK	[6], [7]
ENCRYPTION EFFICIENCY	[6]
ENCRYPTION QUALITY	[6]
INFORMATION ENTROPY	[6]
SPEED ANALYSIS	[7]
ADDITIVE NOISE ATTACK ANALYSIS	[8]
BRUTE-FORCE	[11]
QUALITY OF DECRYPTION	[13]
VISUAL SECURITY	[13]
MSE AND PSNR ANALYSIS	[15]
LOSSLESS ENCRYPTION ANALYSIS	[16]
ENTROPY ANALYSIS	[16]
SECURITY ANALYSIS	[16]

Table2. Research Analysis.

5.3 Research Limitations

In paper [8], images with small dimensions 256 x 256 are encoded, which may be ineffective for larger medical images. The problem of the small size of encrypted and protected images is also present in research [16] and [17], which reduces the quality of protection for larger images.
In research [14], steganography of image documents lacks a set of data for testing and experiments. This reason shows us the lack of experiments to verify the efficiency and effectiveness of the algorithms.
In research [16], the proposed experiment for steganography of image still needs many training samples in order to prove its effectiveness and it needs a long time to train. but if there are high-efficiency devices, this will not be a problem at all.

5.4 Discussion

Through the studies reviewed, each of the studies reviewed gave good results, both in encryption and in stenography. This gives us an answer that there may not be a preference between the two methods in terms of strength, effectiveness, and providing the desired protection for medical images and data. But the problems faced by researchers in the scenography, which were discussed previously, give a clear perception that this aspect still

needs many studies in order to be developed in the desired manner. This gives a wide scope for researchers in research and development in this aspect. As for the encryption of medical images, extensive studies in this aspect show the remarkable development and high efficiency. In medical image encryption, researchers still have many opportunities for improvement, for example repeating previous experiments with larger size and larger dimensions.

For the analyzes that were performed on the algorithms to verify the efficiency, stenography still needs to perform many analyzes to prove the efficiency and effectiveness of the protection as the research that were included in this review did not contain a sufficient amount of analysis of the efficiency and safety.

6. Conclusion

The medical data of patients is one of the most important data that must be protected from unauthorized access. Therefore, many methods and algorithms have appeared that encrypt this data to protect it from any modification, forgery, or any unauthorized access. In this article, we presented a review of the most important challenges facing the protection and encryption of medical images. We tried to find out the challenges facing this work in order to push researchers to intensify the work and find the best ways to make this data more secure and reliable. The studies that were reviewed in this review showed that encryption is safer and more effective when encrypting medical images, because the research that focused on encrypting medical images showed more security in terms of conducting many analysis tests for algorithms and showed good results. In contrast to research that hides images , steganography , in which the experiment is not tested with multiple tests. Also, there are a number of problems faced steganography of medical images, one of the most prominent problems is the lack of a data set ready to test the experiments carried out by researchers. Furthermore, training in steganography requires more time, except in the case of high-efficiency devices. This review aimed to discover gaps, answer research questions, and give researchers ideas for future work.

References

[1] Vengadapurvaja A, Nisha G, Aarthy R, Sasikaladevi N.: *An Efficient Homomorphic Medical Image Encryption Algorithm For Cloud Storage Security.* Science Direct.Procedia Computer Science (2017)

[2] Stallings W.: *Cryptography and Network Security* (2011)

[3] X. Liao, J. Yin, S. Guo, X. Li, and A. K. Sangaiah,.:*Medical JPEG image steganography based on preserving inter-block dependencies*. Comput. Electr. Eng., vol. 67, pp. 320–329, Apr (2018)

[4] Saraswata A , Khatria C , Sudhakara , Thakrala P , Biswas P.: *An Extended Hybridization of Vigenere and Caesar Cipher Techniques for Secure Communication*. Science Direct. Procedia Computer Science (2016)

[5] William S.: *Cryptography and Network Security Principles and Practice Fifth Edition* (2011)

[6] Kamal S , Hosny K, Elgindy T, Darwish M, Fouda M.: *A New Image Encryption Algorithm for Grey and Color Medical Images*. IEEE (2021)

[7] Ahgue A, Nkapkop J, Effa J, Franz S, Malutan R, Borda M.:*A New DNA-Combining Chaos Scheme for Fast and Secure Image Encryption.* Springer Nature Switzerland AG (2019)

[8] Bongale A, Bhamidipati K, Bongale A, Kumar S.: *Hybrid International Data Encryption Algorithm for Digital Image Encryption* . Springer (2021)

[9] Chen X, Wu H.: *Image Encryption Algorithm Based on Chaotic Sequence*. Springer (2020)

[10] Jiang B.:*A Homomorphic Encryption Algorithm for Chaotic Image Coding Data in Cloud Computing*. Springer (2019)

[11] Kumar P, Aswatha A, Sasi S.: *Grayscale Image Encryption Based on Symmetric-Key Latin Square Image Cipher (LSIC)* .Springer (2018)

[12] Zhang R, Jiang D, Ding W, Wang Y, Wu Y, Guang Y, Ding Q.: *Visually Meaningful Image Encryption Algorithm Based on Parallel Compressive Sensing and Cellular Neural Network.* Advances in Smart Vehicular Technology, Transportation, Communication and Applications, Smart Innovation, Systems and Technologies 250. Springer (2022)

[13] Shyla M , Kumar K, Das R.: *Image steganography using genetic algorithm for cover image selection and embedding.* Science Direct, Soft Computing Letters (2021)

[14] Zenati A , Ouarda W, Alimi A.: *SSDIS-BEM: A New Signature Steganography Document Image System based on Beta Elliptic Modeling*. Science Direct. Engineering Science and Technology, an International Journal (2020)

[15] Sasikaladevi N , Geetha K , Revathi A.*: EMOTE – Multilayered encryption system for protecting medical images based on binary curve*. Science Direct. Journal of King Saud University – Computer and Information Sciences(2022)

[16] Li F, Yua Z, Qinb C.: GAN-based spatial image steganography with cross feedback mechanism. Science Direct. Signal Processing (2022)

[17] Hussain A , Bora P.:*Novel Watermarking Technique Using Encryption Steganography, Chaotic Logistic Map and Multiple Embedding*. Science Direct. Procedia Computer Science (2020)

[18] Kitchenham, B., Charters, S. *"Guidelines for performing systematic literature reviews in software engineering 2".*

[19] Heimerl F, Lohmann S, Lange S, Ertl T.: *Word cloud explorer: Text analytics based on word clouds*. IEEE. Hawaii International Conference on System Sciences (2014)