Republic of Iraq
Ministry of Higher Education
and Scientific Research
University of Babylon
College of Engineering/ Electrical Engineering

A New Approach For Intelligent Steganography System Based Advance Microcomputer in Optical Application

A Thesis Submitted to the Department of Electrical Engineering / College of Engineering / University of Babylon in Partial Fulfillment of the Requirements for the Degree of Ph.D. in Science of Electronic and Communication Engineering

By

Heba Abdul-Jaleel Al-Asady

Supervised by

Prof. Dr. Osama Qasim Jumah Al-Thahab

Prof. Dr. Saad Saffah Hreshee

2021A.D **1443 A.H**

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

(الَّذِينَ آمَنُوا وَتَطْمَئِنُّ قُلُوبُهُمْ بِذِكْرِ اللَّهِ أَلَا بِذِكْرِ اللَّهِ تَطْمَئِنُّ
الْقُلُوبُ ۝)

سورة الرعد (الاية 28)

ACKNOWLEDGMENTS

In the name of Allah, Most Gracious, Most Merciful

Praise be to God, Lord of the Worlds, who gave me health, patience, and knowledge to fulfill my promise.

I extend my highest appreciation to my supervisors, Prof. Dr. Osama Qasim Jumah Al-Thahab and Prof. Dr. Saad Saffah Hreshee, for their assistance, encouragement, guidance, patience, and support through this research.

My thanks and gratitude to those who braved the circumstances so that I could reach my mother and father; This is what I promised you

My thanks to my brothers and sisters for providing support and encouragement throughout the study period.

I would also like to thank the College of Engineering in general and the Electrical Engineering Department in particular, the faculty and staff of the Electrical Engineering Department for their kind support.

Finally, my thanks and gratitude to everyone who said that you would not reach, but I do.

ABSTRACT

As a result of the development of information technologies and the Internet, electronic governments appeared. These electronic governments make all institutions deal with archiving and preserving data via the Internet by creating a single and joint database for the one country system to facilitate work with documents and facilitate employment for citizens.

The data must be encrypted to protect the information in the Database and not allow unauthorized persons to access it. Encryption protects information by hiding it in other data types such as pictures, sounds, messages, and videos. A decoding system is used to know the encrypted data, relying on the primary keys used in encryption. Thus, this thesis sought to build a distinct and unique coding scheme to safeguard Database and archived data. The patient's encrypted electronic medical file was recommended as a case study because all Iraqi health institutions lack a patient database.

The proposed system has three stages: The first stage is the data gathering, including patient images and information such as full name, mother's name, weight, height, blood type, blood pressure, respiration rate, and specialty doctor (the family doctor).

The second stage is data processing that consists of three steps where. The first step is to determine the face part of the image by using the face detection algorithm to hide information in it. After the face image is detected, the picture is then trimmed and extracted the primary colors (red, green, and blue) to prepare it for the data cancellation.

The second step is the data encryption using the chaotic Logistics map. The novelty of this dissertation is presented in the encryption. The new method is by using the 2D-cubic spline in the second stage of encryption. This is done by selecting places from the green matrix of the

image. After changing the green color from a decimal matrix to a binary matrix with the three dimensions (x,y, and z), the encryption procedure occurs.

The length of the patient data is encrypted in the red color of the image, which is utilized as a decoding key.

After converting from binary to decimal, combining the primary colors, and restoring the image to its original form.

The last step is archiving images in the cloud, which provides complete data protection with the person's name who enters this data automatically saved in the central Database. Another benefit of archiving data on the cloud is that the patient's name and picture are displayed when searching the Database. This function further secures the patient's electronic medical file.

The second half of the system allows only the owner of the decoded software to extract data, which is the reverse of the encryption and data protection procedure. A reverse algorithm is used in Matlab to segment an image into its primary blue, red, and green colors and extract the length of the encrypted data via the red color, which is used as a key for the rest of the functions, such as logistic function and two-dimensional cubic spline function,then extracting the areas where the information is encrypted (green color) using the logistic map to get the encrypted data and restore it to text as it was read in the data processing process results in an integrated report of the patient's data.

Images with JPEG and PNG formats are used to test this application; their data was input, encrypted, and transferred to the server.

The algorithm's strength is evaluated with assaults such as Gaussian, salt & pepper, Poisson, and speckle. The results show a high PSNR reaching 105.871dB, 0.0001 RMS values, and the data recovered with a 0.00001 bite error rate. The system is implemented using windows ten on tablet (ThinkPad tablet with processor intel(R) Core(TM)-m7-6y75) where the picture and information are taken by a GUI of the MatLab program installed in this tablet and then the data is processed and uploaded to the cloud.

LIST OF SYMBOLS AND ABBREVIATIONS

Symbol	Meaning
x_i	The root of the logistic map
r	Control parameter of the logistic map
S(x)	Cubic spline function
C_0, C_1, C_2, C_3	Roots of the cubic spline function
R	one-dimensional interpolation of the cubic spline function
$\propto$	kernel's first derivative or slope
PSNR	Peak Signal to Noise Ratio.
RMS	The roots mean square value.
SNR	Signal to noise ratio.

LIST OF TABLES

LIST OF FIGURES

LIST OF CONTENTS

Title **Pg. No.**

CHAPTER ONE: INTRODUCTION

CHAPTER TWO:ENCRYPTED SYSTEM FOR ELECTRONIC PATIENT FILE

CHAPTER THREE: IMPLEMENTATION OF PROPOSED SYSTEM

CHAPTER FOUR: LABORATORY RESULTS AND DISCUSSION

Chapter One

CHAPTER ONE

INTRODUCTION

1.1 Brief Consideration

The concept of watermarking and steganography are intertwined. Steganography is a descendant of the ancient technique of" Cryptography." The contents of the message are protected by cryptography. Steganography, on either side, is a method of concealing data by invisibly writing on a cover piece. Steganography originates from the Greek term "stego-graphy," which translates as "hidden writing" since "stego" means "hidden" and "graphy" means "writing." The approved party is only aware of the secret message's presence in this case. An ideal steganography technique conceals a considerable quantity of data so that the change of object cannot distinguish from the original thing visually or audibly[1].

In the sense of digital content, the word watermarking has been defined in various ways. However, here's a broad concept that can be applied to any application: Watermark; it is defined as a method of invisible change that comprises masking and embedding a message linked with this operation to protect it. The term "massage" refers to music, video, or image in this sense. This description implies an important point: the secret information inside the work and the watermark itself should contain information about the position at which it is incorporated. This feature establishes a fundamental prerequisite for a watermarking scheme that distinguishes it from a general stenographic method[2].

Watermarking is a technique for concealing a hidden signal in a digital signal while maintaining the original signal's overall consistency[3].

By embedding ownership data (watermark) into digital material (picture, audio, and video) without compromising its perceptual quality, it is a new technology used to enforce copyright protection of digital data[4, 5].

Steganography, Cryptography, and Watermarking are the three forms of information concealment techniques[6,7]. Figure(1.1) depicts the three significant types of information concealment techniques.

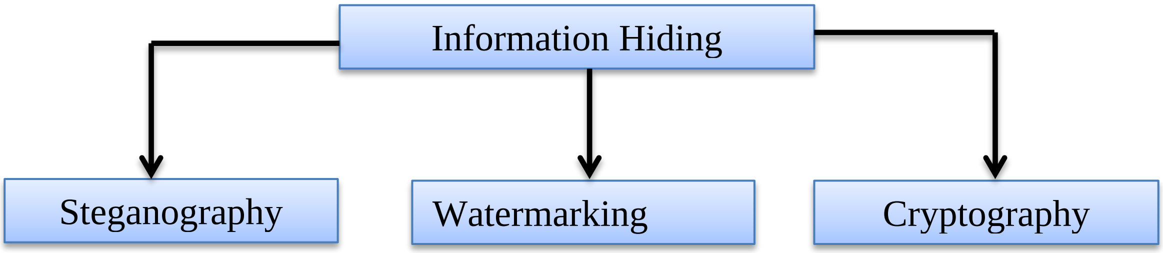


Figure (1.1): Information hiding techniques

Steganography Technique: It is a science that entails concealing knowledge from unauthorized individuals. Steganography is the process of concealing a file, message, picture, or video within another file, message, image, or video by using a unique code. Figure (1.2) depicts a simple steganography model. The secret and cover messages are fed to the encoder using steganography techniques. Then the same encryption algorithm is used in reverse order to retrieve the original secret message and cover message. The importance of the key in recovering the original message cannot be disregarded.

Unauthorized individuals cannot even presume the existence of a secret message. The art of hiding data inside data is known as digital steganography. Steganography aims to conceal data well enough that unintended recipients are unaware that it contains personal data[8]. Because of their large scale, media files are suitable for steganography transmission.

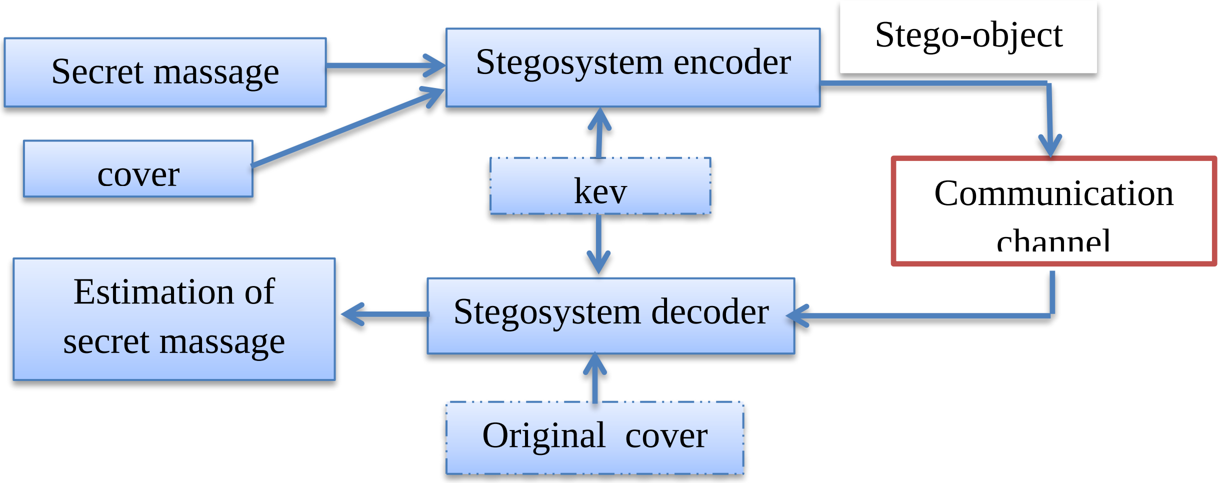


Figure (1.2): Process of Steganography

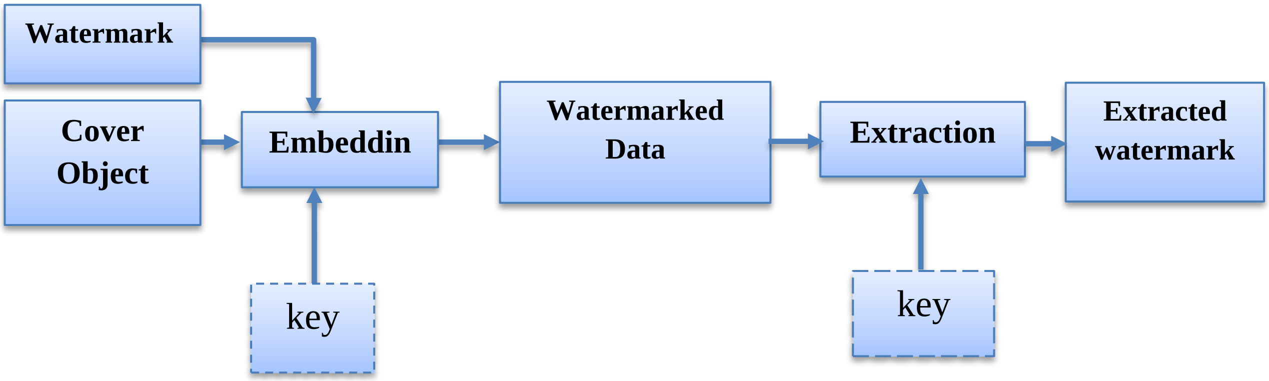
There are two forms of steganography: fragile and robust, whereas fragile: It entails embedding information into a lost file if the file is changed. Since the copyright holder of the file can be easily replaced, this approach is not appropriate for documenting it. It comes in handy when verifying that the file hasn't been tampered with. This approach is less complicated to execute than robust methods[3], [4].

Robust method: Embedded knowledge is difficult to destroy. The steganography should be placed in a section of the file that is not visible.

Watermarking Technique: Watermarks embedded in the cover work, i.e., the initial work, can be retrieved by repeating the method for embedding them in the cover art. This implies that any watermarking system must have two general components: a watermark embedding method and a watermark recovery mechanism[2].

As with steganography, the device has an embedded key. The key is to improve protection by preventing unauthorized users from manipulating or extracting data. An object initially used as a sign or cover is the watermark embedding medium, and the changed object is the data with an embedded signal or data with a watermark.

Watermark and watermarking keys are the inputs for the embedding block (to generate the encapsulated signal or watermarked information). In contrast, the embedded thing (data with an embedded signal or data with a watermark), key, and sometimes watermark are the inputs for the extraction block (as shown in Figure (1.3)[1].



Figure(1.3): Watermarking embedding and extraction.

Cryptography Technique: Humans have had two innate needs throughout history; these two requirements create the art of encoding messages so that only the intended recipients can read them. Even if the scrambled letters fell into their hands, unauthorized people would be unable to obtain any information. Figure(1.4) depicts the steps involved in cryptography[9].

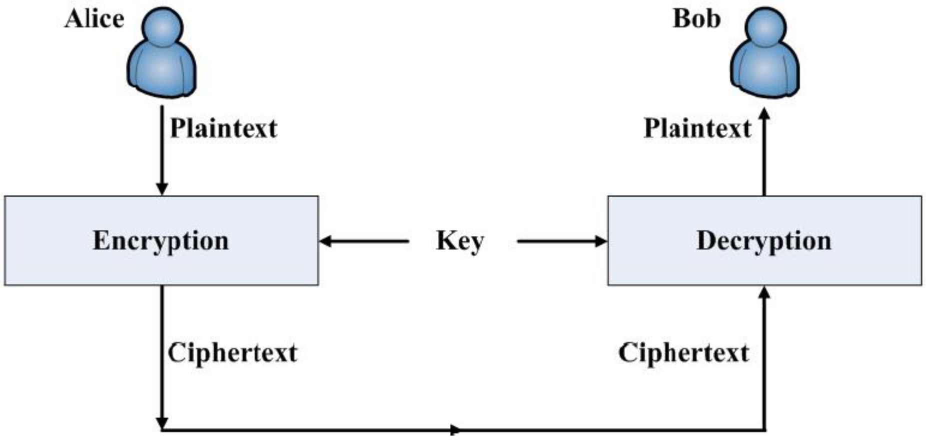


Figure (1.4): Cryptography model[9]

The original message is encrypted using plaintext and key. Ciphertext refers to the encrypted message.

Decryption is the opposite of encryption, i.e., going from unintelligible ciphertext to plaintext. The original plain text is retrieved [5].

Encryption is the method of encrypting information using cryptography. The information that has been locked is a message that has been encrypted. Key is a secret used during encryption and decryption, similar to a password. Decryption is the method of using encryption to decrypt encrypted data. A cryptosystem is a collection of cryptographic techniques and the infrastructure that supports them that are used to provide information. Cryptography is the art of creating cryptosystems that can protect information. Cryptanalysis is the art of deciphering cipher texts[6]. Cryptography is concerned with the transmission or storage of ciphertext. It entails the investigation of cryptographic systems, the mechanism of breaking them. Cryptanalysis is also used to test new cryptographic techniques' security during their development[8].

A growing body of individual clinical experiences can produce new knowledge and best practices; we introduced a new security system to deal with clinical data, representing the extensive database of the most central resource to healthcare progress.

1.2 Problem Statements

1- Clinical data is stored in several locations, many of which are unavailable and unconnected from the rest of the network.

2- Data fragmentation, the private nature of data, and privacy concerns are just a few of the roadblocks to making greater use of these resources.

3- The lag between public policy development and public awareness of and attention to these issues; and the necessity to address the critical problems prevents the data from being distinguished, such as whether the data constitutes a public benefit or not.

4- Due to the logistical, organizational, and other practical restrictions of employing a paper-based record, traditional forms are less effective at keeping and organizing an ever-increasing number of disparate data.

5- Despite the existence of the electronic patient file, but he still did not maintain the confidentiality of the patient's information, which can only declare to the patient and the competent doctor.

1.3 The Main Contributions and Objective

The main objectives of this thesis are:

1- Authorized clinicians can access data stored on a secure network from the office, home, or emergency room, allowing them to make timely informed judgments.

2-Electronic Patient File System (EPFS) technologies enable the regulation and tracking of patient record access to comply with accountability and the transfer of health insurance privacy regulations and make data more available to authorized individuals for valid purposes.

3- With this system, the right laws and policies are in place. Data stored on computers can more safe and private than data kept in paper-based records.

4- Because of the significant resources required and the wide-ranging potential advantages, implementing an EPFS system is a strategic decision. Therefore, the cost-benefit analysis must consider the influence on the organization's strategic goals and personal health care aspirations.

1.4. Related Works

This section will introduce some related work about every subsystem of the proposed system.

1.4.1 Some Related Work of Chaotic Algorithm.

In 2017, Milad YousefiValandar, Peyman Ayubi, and Milad Jafari Barani proposed a new transform domain steganography method for digital images (IWT). It also utilized a modified logistic map, which improved the suggested method's length and security and its performance compared to current transform domain steganography methods like PSNR: 54.387 and SSIM: 0.9984[10].

In the same year, Hegui Zhu and his group presented a two-dimensional homogeneous hyper-chaotic compound system and LBP-based image encryption method, which comprises CHHCS- based permutation and LBP-based diffusion. The updated cipher pictures can be decrypted using

CHHCS with excellent visual quality and just 3.56 and 33.65% data loss, respectively[11].

Moreover, Yassine Himeur and Abdelkrim Boukabou present a The watermark information is encoded using a new chaotic encoding method based on gradient size similarity deviation in the video watermark approach. It is possible to reduce the complexity of video watermarking systems (GMSD); based on the obtained results, it can be concluded that the approach's characteristics have high performance [12].

In 2018, S. Thakur, A. K. Singh, S. P. Ghrera, and A. Mohan's way to secure medical image watermarking that is chaotic-based was proposed. To assure the security of the technique, it is necessary to apply two-dimension logistic map encryption to encode the medical image. The proposed method achieved the highest possible PSNR, NC, NPCR, and UACI values [13].

In the same year, G. Singh Walia, S. Makhija, K. Singh, and K. Sharma presented and developed The new LSB substitution mechanism directed with a stego key to transmit a secret message over a public network. As previously stated, a large keyspace for stego-key is required to defeat any force assault in the public domain. Following an analysis of these findings, it was discovered that the approach achieves an average PSNR value of 44.09, an RMSE value of 2.15, and an SSIM value of 0.97 throughout a range of payload values[14].

2019, Umer Aziz Waqas and his group devised a new watermarking strategy that uses a multilayer system of information security algorithms. It has been demonstrated that we can build nonlinear components of block ciphers using the chaotic logistic map method. The recommended substitution box (S-box) method may be used to encrypt a "quick response code (QR-code)." A novel watermarking strategy is also proposed; it uses the Daubechies wavelet transform, a multi-selection frequency domain algorithm, to enter a digital logo recorded in the form of QR codes and other novel techniques[15].

Shiv Prasad and Arup Kumar Pal Watermark developed in two steps; the scheme computes a secure authentication code/watermark bit from a subset. The watermark bit is first hidden into the most significant bit (MSB) of each pixel using the watermark embedding process described by the author and then hidden into the least significant bit (LSB) of each pixel using the watermark embedding procedure recommended by the author. The results are satisfactory, with PSNR (dB)=42.79, SSIM 0.9932, and IF 0.9864 for each pixel[16].

In 2020, Jun-YunWu and colleagues developed a new undetectable and robust digital picture watermarking system by integrating four-level DWT, DCT, and SVD to ensure the security of the watermarked image, which was published in Nature Communications. Due to the requirement of the human visual system for masking features of image brightness, texture, and frequency, the cover image is processed using a 4-level DWT and the DCT to achieve the desired results[17].

In the same year, Phuoc-Hung Vo and his team have developed a secure and durable watermarking technique that improves the system's overall security by protecting the watermark image and embedding positions in the watermarking scheme. Comparisons with similar state-of-the-art algorithms reveal that the suggested method provides good imperceptibility of each view, as demonstrated by the results of the performance evaluations. The PSNR and SSIM metrics were validated as 56.99 and 0.999, respectively[18].

1.4.2 Some Related Works of Cubic Spline Interpolation

In 1998, Using cubic Splines, Sky McKinley and Megan Levine demonstrated that data could be correlated efficiently and effectively, no matter how random the data appears to be. Once the spline generation technique has been developed, interpolating data with a spline becomes simple.[19].

In 2000, Etienne Cuche was a French actor and director. Cubic slice interpolation was used to create anodized slots with a propagation profile that follows a predetermined curve, which Pierre devised Exhibits the best and Christian Depeursinge. To reduce the standard deviation and phase distribution, the method was tested using a computer-generated three-dimensional image, and the robustness of the method was not tested using noise[20].

In 2002, The authors George Wolberg and Itzik Alfy demonstrated how cubic splines could interpolate monotonic data sets in their paper. For 1tting data, cubic splines are commonly used because they employ low-order polynomials and have C2 continuity, which allows them to generate the smoothest possible curve that passes through its control points while also satisfying the monotonicity condition[21].

In 2003, Piecewise cubic convolution (PCC) was a technique developed by Stephen E. Reichenbach and Frank Geng for two-dimensional image interpolation (2-D), non-separable. The traditional approach to PCC implementation is based on a one-dimensional (1-D) derivation that may be generalized to two dimensions in a detachable manner. This 512*512 scene is sampled to 16 16 and then reconstructed to 512 512 using several optimization techniques, including the following: Wiener, optimal 2-D PCC, optimal separable PCC, separable PCC with, and cubic spline interpolation [22].

In 2004, Lung-Jen Wang, Wen-Shyong Hsieh, Trieu-Kien Truong presented a novel simplified cubic-spline method approach that uses a "cross-zonal filter" and an asymmetric extension method designed for picture coding. Compared to the old CSI scheme, the new CSI scheme significantly reduces the number of additions, multiplications, and calculations of the autocorrelated filter coefficients required during the decimation process[23].

In 2006, According to Jiazheng Shi and Stephen E. Reichenbach, two new non-separable, 2D cubic-convolution kernels were derived in this paper. The first seed has three parameters, cubic interpolator defined on the two-dimensional matrix with constraints for continuity, smoothness, and continuity with constraints, diagonal (or 90 rotational) for biaxial symmetry, continuity, and smoothness. In contrast, the second seed, which has five parameters (called 2D-5PCC), loosens the restriction of diagonal symmetry, based on the observation that many images exhibit statistical features that are rotationally asymmetric[24].

With the help of an FIR digital filter, Llus Ferrer-Arnau and his team demonstrate how to compute the interpolant with fewer operations per interpolated point and more accuracy than previous methods. It is also possible to compute the results in real-time as the signal samples are being acquired. As a result of this approach, and similarly, we can easily derive the derivatives of the interpolant and signal approximations to lessen the oscillations that occur when employing high-order splines[25].

In 2017, Simone S., Michele S., Danilo C., and Aurelio U. provided a principled approach to having a data-dependent modification of the activation functions performed independently for each neuron in a network setting. This is accomplished by capitalizing on past and present improvements in cubic spline interpolation, which allows for local modification of the functions in the vicinity of their application areas. The resulting algorithm is relatively simple to construct, and overfitting is mitigated by including a novel damping criterion in the literature [26].

In 2019, According to Osama Q.Al-Thahab and Hasan A. developed a novel mapping algorithm presented here. It relies on the cubic spline algorithm as a key element for controlling the pixel position in the RGB image. They also used the proposed system in conjunction with a copyright application. The cover image element is completely exchanged (pixel). Four samples of the host image vector are taken. The position of the cover image pixel is exchanged concerning another four samples of the information (secret)image vector to construct a spline curve and completely exchange the cover image element. This cubic spline curve is used for watermarking purposes, and the slopes of this curve are used for this purpose[27].

1.4.3 Some Related Works of Face Detections

In 2016, John McDonagh Developed a unified framework for face detection and feature alignment in random wild pictures. AFW data set shows that our detector outperforms all commercial and published approaches by more than 10%, demonstrating the effectiveness of the suggested standardized framework in terms of face detection and face alignment[28].

In 2017, Jifeng Shen, Xin Zuo, Jun Li, Wankou Yang, and Haibin Ling based on multi-channel maps, we proposed a new statistical feature for pedestrian and face detection called differential pixel neighborhood statistical feature. It is necessary to perform two procedures to compute LBP: Pixel Differential Advantage Computation (PDF) and PDF Signature Encoding. The results reveal that our method outperforms the most recent technology while running at 20 frames per second for 480 × 640 images, which is a significant improvement[29].

In 2018, Wanxin Tian and his team Face detection were made possible using a novel framework called DF2S2 (Detection with Feature Fusion and Segmentation Supervision). They provide a feature fusion pyramids structure that is effective and a segmentation branch that is beneficial in helping the model learn more accurate features[30].

In 2019, Hoda Q., Babak M., and Mohammad Taghi M. In this paper, we offer a computer vision method for partially covered face detection in low-resolution surveillance recordings that feature traditional Middle Eastern attire such as the headscarf. Face categorization is accomplished using a mixture of the Haar cascade and the Locally Binary Patterns Histogram (LBPH) algorithms. The suggested framework also uses the Support Vector Machine (SVM) method[31].

In the same year, Cheng Chi and A novel single-shot face detector named Selective Refinement Network (SRN) are presented by his team, which incorporates novel two-step classification and regression operations selectively into an anchor-based face detector to reduce the risk of false positives while simultaneously improving location accuracy. It is composed of two modules in particular: the Selective Two-step Classification (STC) module and the Selective Two-step Regression (STR) module, both of which are used in the SRN[32].

In 2020, The following principle was presented by Haiwen Huang and his team as a simple yet effective technique. Samples with well-constrained parameters are concentrated in a specific area in a trained neural network. The "Space Singularity Feature (FSS)" refers to the OoD Feature Center. The feature space singularity distance is between the sample feature and the FSS (FSSD). Setting a restriction on FSSD then permits OoD samples to be chosen[33].

In the same year, Zhang Chifeng and Zhang Chifeng's team created RefineFace, a single-shot refinement face detector, to attain excellent performance. Here's where you can get a more thorough breakdown: Two-step selective regression approaches include, for example, loss of scale perceived margin, feature moderation unit, and receptive field optimization[34].

1.4.4 Some Related Works of DataBase

In 2015, Andrew P. and To maximize our computing resources, his team unbinds our databases from specific hardware. It allows them to be stopped when not in use and restarted on demand using any available hardware. They also delegated the end-user the ability to do the most common actions on these databases on-demand, without special system privileges, which allows them to save time[35].

In 2016, 1Kodrat I. Satoko, R. R. Isnanto, Rinta K., and Kurniawan T. Martono Discuss how to optimize the database system so that when data is accessed, it does not have an adverse effect on the performance of the server systems. When designing the database system, process optimization should be considered. In this study, process optimization is accomplished by using one of the functions provided in MySQL through VIEW. The system will handle this virtual table operation more efficiently [36].

In 2017, Dana V.Aken, Andrew P. Geoffrey J. Gordon, and Bohan Z. described an automated technique to tuning DBMS setups that take advantage of experience while also collecting new information: To choose the most impactful knobs, the authors use a combination of supervised and unsupervised machine learning algorithms to link unknown database workloads to past workloads from which we can learn, and propose knob settings for the databases under consideration. They integrated their methods into a new Otter Tune program and tested it on three distinct databases. In our evaluation, Otter tune offers settings on par with or better than those created by existing tools or by a human expert in terms of quality[37].

In the same year, Joy A. and Andrew P. presented an idea for developing a new database management system in light of the changes in the hardware landscape brought about by NVM. They draw attention to several unsolved research difficulties and suggest addressing them[38]. We review recent breakthroughs in this field and examine the lessons gained from previous research on the design of NVM database systems[38].

In 2018, Basit Raza and his team produced OtterTune, a tuning tool that may automatically determine optimal settings for the configuration knobs of a database management system (DBMS). It was first launched in 2010. OtterTune uses data gathered from prior tuning attempts to train machine learning models, which then recommends new configurations on par with or better than those provided by existing tools or by an expert in the field[39].

In 2020, Ben Jiang and colleagues created the world with the help of an open-source web server, free software for automated data storage and processing, and powerful management analyzing the needs on fusion and comparison algorithms for microsatellite DNA fingerprinting data first

Forensic DNA system (PIDS). Whenever the matching capillary electrophoresis image is identified at each primer point, this system may create fingerprint data, which may be sent to the server.[40].

In the same year, Shin-Shing Shin Concept maps are used to explain the SQL statement execution process, which helps learners gain a better grasp of SQL statements. To investigate the relationship between concept maps and the knowledge of SQL from the standpoint of cognitive load theory, an actual experiment was undertaken utilizing two database courses, namely concept map-based and conventional training[41].

In the same year, Nawar Alseelawi, Hussein T. Hazim, and Ali D.Alramadan created and maintained a database. The database is organized using the ASP.NET (Active Server Pages) application (written in C# and serves as an assisting tool to manage the files used on the site). To develop a medical treasury, which comprises (medical supplies), a database was designed and built expressly to handle the problem of estimating the annual requirement for medications (medical supplies) to fulfill their needs and, consequently, the needs of patients[42].

1.5 Organization of the Thesis

The central idea of this thesis is to propose a security electronic patient file system based on the steganography technique for a Databased application using statistical parameters and energy of the signal in the logistic map and 2D-cubic spline interpolation.

Chapter one Introduces the subject and the keywords and phrases that will be utilized later in the thesis document.

Chapter two describes the prerequisites for a secure electronic system that is an effective patient file system based on steganography technique, which explains the signal's energy in the logistic map and 2D-cubic spline interpolation in the encryption.

Chapter three introduces the security electronic patient file system.

Chapter four explains the cases studies with laboratory results and discussion.

Chapter five contains the results of practical application (field implementation).

Chapter six contains the conclusions and future works of this thesis.

Finally, Chapter seven is used to show the references.

Chapter Two

CHAPTER TWO
ENCRYPTED SYSTEM FOR ELECTRONIC PATIENT FILE

2.1 Introduction

The theoretical concepts of the proposed security system based on the steganography Technique are discussed in this chapter. This chapter has been divided into sections based on the essential principles and strategies for creating a secure electronic patient file.

2.2 Steganography

The term "steganography" originates from the Greek term "stego-graphy," which translates as "cover writing"[5]. Steganography is often referred to as "invisible" communication. The term "steganography" refers to the practice of concealing the existence of messages in another medium (audio, video, image, communication). Because individuals frequently send digital photographs via email or other online communication applications, today's steganography systems use multimedia objects as cover media, such as images, audio, and video. It's not the same as safeguarding a message's real content. In simple terms, it would be the same as that, with information being hidden among other information[6].

Steganography refers to the process of hiding a secret message inside a cover object rather than altering its structure (carrier object). "Cover object" and "stego-object" (containing concealed media) are comparable after the hiding procedure. As a result, steganography (hiding information) and cryptography (preserving information) are opposed. In steganography, recovering information without a recognized process is difficult due to invisibility or hidden factors. Steganalysis is a steganography detection procedure[8].

2.2.1 Steganography vs. Watermarking

Both steganography and watermarking are covert communication methods. Steganography usually refers to confidential point-to-point communication between two parties. Rather than making the thing inaccessible, watermarking is a steganographic technique whose primary objective is to protect the object rather than make it invisible[7]. Transmission, storage, format conversion, and data alterations are not weakening the steganographic methods.

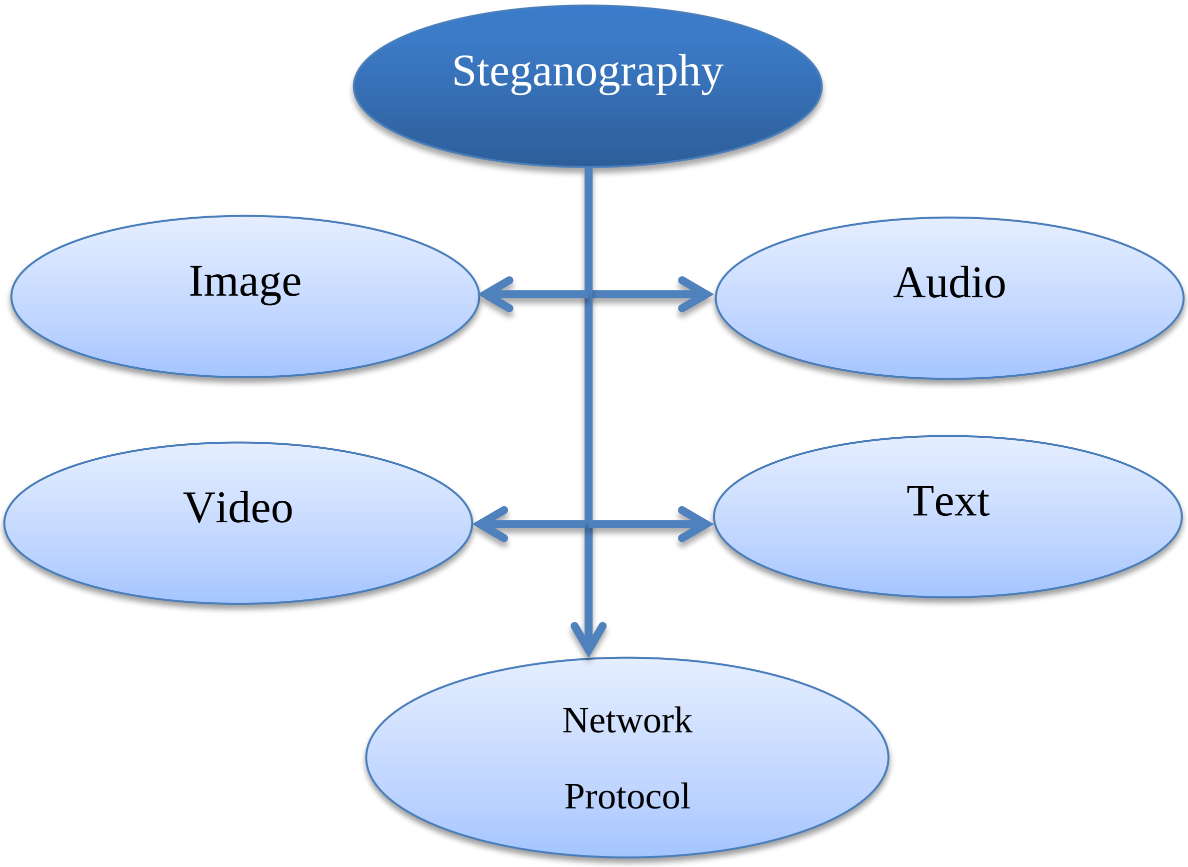
The superior robustness capability of watermarking schemes is a significant difference between the two techniques. To summarize, an ideal steganographic system would embed a large amount of information with no apparent deterioration to the cover object. In contrast, an excellent watermarking system can embed information that could not be changed or removed without rendering the cover object, which may be completely useless. A watermarking scheme requires a capability and security trade-off [3].

2.2.2 Steganography Vs. Cryptography

Cryptography is the study of concealing information, while steganography is the process of writing coded messages so that only the sender and receiver are aware of their existence. In cryptography, anyone can see the encrypted letter, while only the sender and recipient are aware of its presence in steganography. To hide data, cryptography employs mathematics and number theory. Steganography does not require a lot of math. The confidential data does not impact the quality of the message file when using steganography.

2.2.3 Techniques of steganography

Various stenographic approaches can be used to achieve security depending on the type of cover object. Figure(2.1) depicts the situation[43].



Figure(2.1): Steganography in Digital Medium.

i. **Image Steganography:** refers to employing a cover image itself to disguise as an image in steganography. Pixel intensities are often utilized to conceal information with this method[43].

ii. **Network Protocol Steganography**: A carrier-assisted attack happens when the media is disguised as a network protocol (such as "TCP, UDP, ICMP, or IP"), and the protocol is employed as the carrier. Secrecy channels exist in the OSI network layer architecture, and steganography may be implemented in "new header bits for TCP/IP fields," according to the Open Systems Interconnection (OSI) [42][43].

iii. **Video Steganography**: Any data or file may be concealed in a digital video format using this technique to remove information from each picture in the video that is not apparent to the human eye. A videotape is used to transport secret information (a combination of images). "H.264, Mp4, MPEG, AVI," and other video codecs are examples of this [42].

iv. **Audio steganography**: refers to the use of audio as a carrier for the concealment of information. Due to the popularity of voice-over IP (VOIP), it has become an essential medium. For audio steganography, digital audio codecs like WAVE, MIDI, AVI MPEG, and others are used[44].

v. **Text Steganography:** To achieve information concealment, The "number of tabs," "white spaces," and "capital letters" are all used as a generic text steganography method, and so on, similar to Morse code[44][43].

Image steganography is the process of hiding information in another image or video files, such as text, photos, or audio files. Using the spatial domain technique, this thesis tries to use steganography for text with another image. Only by using suitable decoding techniques can this buried information be obtained.

2.2.4 Terminologies for Image Steganography

Image steganography generally conceals information in a cover image to create a stego-image. This "stego-image" is then transmitted to the other party through a known medium, where the third party is unaware of the concealed message included in the stego-image. After receiving a stego-image hidden message, the receiving end can extract it with or without using a stegokey (it depends on the method used for inserting)[47].

The following are the terms used in image steganography:

• Cover-Image: An original image that serves as a vehicle for concealing data.

• Message: The actual data that is hidden within graphics. The message could be basic text or a picture.

• Stego-Image: A stego-image is created by integrating a message into a cover image.

• Stego-Key: This is a key used to embed or extract messages from cover images and stego-images.

2.2.5 Steganographic Image Techniques

The following domains can be used to categorize image steganography techniques.

i. **The Spatial Domain Technique:** There are numerous different types of spatial steganography, all of which hide data by changing some bits in the image pixel values. The least significant bit (LSB) approach is one of the most fundamental methods for hiding a secret message in the LSBs of pixel values without generating apparent distortions regarding steganography. The human eye cannot detect the LSB's value because the human eye is incapable of seeing changes [42]

ii. **The Transform Domain Technique**, concealing information in an image, is more sophisticated. It is possible to hide information in an image using a variety of approaches and transformations. Several methods have been developed for transform domain embedding, a category[44]. It is significantly more powerful to embed data in a signal's frequency domain than it is to embed principles in a signal's time domain, and this is because the frequency domain contains more information. The transform domain is where the vast majority of today's highly effective steganographic systems operate in their operations. Because they conceal information that is sensitive to compression, cropping, and image processing [43]

iii. **The Distortion Technique:** When using distortion methods to retrieve the concealed message, knowing the original cover picture is necessary throughout the decryption process. Decoders are used to compare the discrepancies between the original cover picture and the distorted cover photo, which is how they function. The encoder modifies the cover image in a series of steps. As a result, signal distortion is regarded as storing information[44]. Using this approach, a stego object is formed by applying a sequence of adjustments to the cover picture. This change sequence is needed to ensure that the secret message to be conveyed is correctly identified[45].

iv. **Masking and Filtering Technique:** Like paper watermarks, these obscure techniques of information work by marking a picture. These approaches embed it in more appropriate locations rather than just burying the information from the noise level. The cover image is more important to the secret message. Because watermarking techniques are better integrated into the image, they can be used without worry of image damage due to lossy compression[45]

2.3 Electronic Patient File System

Emerging advancements in information and communication technology have resulted in significant improvements in community services, particularly in the healthcare sector, over the previous decade. Several studies have arisen to support the healthcare domain; these include creating a framework for electronic-health readiness that focused on the information and Communication Technology infrastructure at a micro level, as defined by the World Health Organization's definitions of e-health[46].

The first reason for developing an e-health system; any person might be able to access and photocopy critical documents information without the knowledge or permission of the registry officer if the paper medical file was left outside instead of being returned to the filing cabinet. But in an electronic medical record system, it is feasible to precise who may have accessibility to the patient's medical records [47].

Secondly, data is ensured to be safe using encryption. Electronic documents may be safeguarded using robust encryption techniques to keep important patient information safe from intruders. As a result, the medical institution must do everything in its power to comply with privacy legislation and electronic health record requirements to make the process of maintaining the confidentiality of paper health records easier. [47], [48].

For a third time, paper records that are susceptible to tampering can be altered in a problematic way to detect. For example, anyone may have documents removed from a report or create a modified version to replace accurate information. At the same time, the protection of patient data is provided through encryption and strong log-in and password processes. It is complicated for anyone to make illegal changes to patient documents or other data stored on the system[49].

Fourth, Audit pathways Electronic health records and Medical organizations benefit from clinical information systems because they provide sufficient security: they allow audits to be performed. Usually, there is currently no reliable method of creating tracking on documents. With an electronic health record system, it is possible to quickly determine who has access to a patient's medical records, when they had access, and whether or not access is permitted. And if someone has access to information they shouldn't see, the audit will highlight the situation[49].

Finally; Maintaining the privacy and security of patient records is significantly more critical than merely restricting access to personal information in the event of a disaster. Disaster data backup must ensure that the information will be made accessible even in the worst-case scenario when using this method. Any time criminal activities or a natural catastrophe such as a fire or earthquake occurs, or landslide occurs, it is far easier to retrieve patient data from an offsite backup; the business will be able to recover more swiftly and function more efficiently than if it depended exclusively on a paper-based approach. According to the organization, more protection will be provided to the organization due to health records and security for private patient data[50].

Medical treatment is generally divided into in-patient (hospitals), out-patient (clinics), and emergency. Here chose to improve the services in hospitals because they are regarded as crucial in the healthcare infrastructure. The implemented system (EPFS) is the first database and workflow system in Iraq (in general hospitals). It's useful for administration, patient care, research, and archiving. It could be used by a hospital director to monitor performance or for statistical reporting in management in less time.

2.4 Face Detection

Over the past few years, advances in computing technology have made it possible to construct visibility components that communicate with people in real-time. There are many instances when the information stored in faces must be evaluated for computers to react efficiently, especially fingerprints and human contact. Before any recognition algorithm can be applied to faces are used as quasi input modules in biometric systems that do not need a password, faces must be identified in a situation to be recognized. To respond appropriately, a user's attention focus (i.e., where the user's gaze is directed) using an intelligent vision-based user interface[54]. Faces must first be identified and registered for facial features to be reliably detected for applications such as digital cosmetics. Face detection is obvious to play a crucial role in the efficiency of any facial recognition technology. Face detection is problematic because it must account for all possible variations in appearance induced by changes in lighting, facial characteristics, occlusions, and other factors. It also has to distinguish faces that appear at varied scales, poses, and rotations in planes. Despite these challenges, significant progress has been achieved in the last decade, with many systems showing excellent performance. Recent improvements in these techniques have also been beneficial in identifying other things, including humans/pedestrians and cars[55].

2.4.1 The Operation of Face Detection System

A standard method of accomplishing this task is to extract specific attributes, "e.g., local characteristics or patterns of intensity that are considered as a whole," from a sequence of training pictures taken in an off-line scenario while performing a prescribed pose (upright frontal stance). These photos are treated with equal histograms or uniformity, "i.e., zero mean unit variance" to mitigate the impacts of changing lighting conditions[54]. These algorithms generally scan on the characteristics that have been collected at every conceivable position and scale to locate faces [55]. The retrieved properties may be explicitly programmed (using human expertise) in newer systems or learned from data collection[50]. The detection method must be repeated on a pyramid of pictures whose resolution is decreased by a specified factor from the original to identify faces at various scales[54]. It is possible to include other visual signals accurately. Pre-processing techniques such as color and motion, for example, may decrease the search area and speed up such processes[56]. The raw discovered faces are generally processed to integrate overlapped findings; This is because faces are commonly recognized at different sizes.

Face detections have been proposed to use pixel-based, parts-based, local edge features, Haar wavelets, and Haar-like features in various applications. In contrast to prior holistic representation methods, existing systems using Haar-like characteristics have shown outstanding empirical results in identifying faces while other objects obscure their portions. For learning-based face detectors to be successful, they must be trained on a large and representative set of face photographs. Using the retrieved data, it is possible to create more good instances by manipulating the original face photographs in various ways, such as perturbing, mirroring, rotating, and scaling them[54].

Because face identification is primarily a pattern recognition problem, various techniques for learning a variety of general templates and discriminant classifiers have been created, and AdaBoost is an example of machine learning techniques used in practice. A decent method for detecting people's faces usually requires multiple iterations of training. Bootstrapping a trained face detector with test sets and re-training the system with the false positives and negatives is a systematic strategy for further improving the system [55].

2.4.2 Performance Evaluation of the Face Detection System

Even if today's face detection systems have outstanding real-time performance, there is still a lot of opportunity for development in terms of accuracy. Face detection systems are evaluated based on various parameters; detection structure, positive and negative error ratio, number of ratings, number of features, number of images, time, precision, and memory requirements are only a few examples of these parameters. The reported performance is also reliant on the definition of what constitutes a "correct" detection result[54]. "Plotting the curve using the de facto standard data set", which incorporates face on the frontal lobe photos, is the most widely used method[56]. A few pixels (around 5) off from the "correct" placements is not uncommon when using state-of-the-art algorithms to recognize faces in photographs that are typically 21 by 21 pixels in size. This is notable because face photos are commonly standardized to 21 by 21 pixels; when trade-offs between speed, robustness, and accuracy result in such outcomes [54], the performance of any biometric applications reliant on the contents of recognized faces is necessarily hampered.

2.4.3 The Applications of Face Detection

It has various applications in various fields, including computer vision, monitoring, feature extraction, facial shape extraction, gender categorization, and clustering are all examples of machine learning techniques used in face recognition. It is also used in multiple applications, including digital cosmetics, biometric systems, and attentive user interfaces, to name a few. More than that, most facial recognition algorithms can spread to distinguish additional objects such as automobiles, people walking along the street, and signs, amongst other things [57].

2.4.4 Face Detection Techniques

Detection of a computerized representation of a person's face is accomplished by using a computer technique known as face detection. The facial features in the digital image are recognized. However, no other items in the picture, such as trees, houses, and other objects, are considered. When making object class identification, it is essential to keep in mind that the goal is to locate and size all objects in an image associated with a particular class. If you think about it, face detection is just a complete version of face localization. When it comes to detecting face elements in a digital image, there are two methodologies to consider: feature-based approaches and image-based approaches[54].

2.4.4.1 Feature-Based Approaches

The feature-based technique extracts image features and matches them against facial feature knowledge. Low-level analysis, feature analysis, and active shape model are the three categories of this technique.

i-Low-level Analysis: Using pixel properties, grayscale level, and motion information, it deals with segmenting visual features. It may also use modifications in visual properties to recognize face characteristics in line drawings and create an edge representation method for identifying these characteristics. The ability to recognize the shape of a human head Edge-based algorithms rely on labeled edges that are matched to a face model to do the verification. Because the brows, pupils, and lips are often darker than the surrounding areas, extraction algorithms may hunt for local minima in the brows, pupils, and lips. When it comes to identifying striking facial characteristics such as nose tips, local maxima can assist in this process. Following that, a low-level grayscale threshold is used to detect anomalies[57], [58].

ii-Feature Analysis: Using more info about the face may help reduce the uncertainty introduced by low-level analysis. In the first, sequential feature searching methods are used to find specific facial characteristics depending on the face's relative location [55]. After identifying the most prominent facial characteristics, hypotheses about minor, major elements might be developed.

iii-Active shape models Analysis: explain the physical appearance of characteristics more detailed than previously described. Modeling objects such as these are put close to a feature, where they interact with the surrounding image and deform to take on the pattern of this feature [56].

ASM stands for object shape model, and it is a model that repeatedly deforms to create a new picture and place an example of the item. It acts in two steps, which are as follows: Check the area around each point in the image for a better location, and then adjust the model parameters to best fit these new positions[56].

2.4.4.2 Image-Based Approaches

Face detection of facial features via explicit modeling is a simple method that can be hampered by the unpredictable nature of faces and surrounding variables. As a result, more robust techniques, capable of functioning in hostile circumstances, such as detecting many faces against cluttered backdrops, are required. Face identification using images has sparked a new study field, and as a result, face detection is regarded as a generic pattern recognition problem. The image-based method attempts to achieve the best match between training and testing images. Various methodologies such as neural networks, eigenfaces method, and support vector machines are included in the image-based approach[54].

i-Network of neurons: The reasoned neural net assesses the curved mirrors of a photograph and decides whether or not each window includes a face in each instance of evaluation. The system switches across various networks to perform better over a single web. As a result, the time-consuming operation of manually picking unguided training data that must cover the whole non-face picture region has been eliminated[54].

ii- Eigenfaces method: When it comes to face recognition, eigenvectors have been proven effective, and a rudimentary neural network has been facing recognition for affiliated and standardized face images has been shown. Face pictures can be compressed by linearly encoding them with a few core photographs as possible, which allows them to be compressed further[57,59].

iii- Support vector machine (SVM): Support vector machines have also been used to recognize faces in various situations (SVMs). As a novel paradigm, SVMs are being used to train polynomial function, neural network, and radial basis function (RBF) classifiers, among other things. To decrease the predicted overfitting to the least possible level, SVMs use the extrapolation concept known as functional risk reduction, which aims to reduce dimensionality in the model to the minimum possible level.

2.5 Chaotic system

Chaos originates from the "Greek term Xaos," which means a state in which there is no order or predictability in the situation. Unpredictable behavior and the appearance of randomness are characteristics of chaotic systems [60], which are simple, nonlinear, dynamic, and deterministic systems. A further characteristic of this system is that it is susceptible to the beginning conditions. When an input parameter's value changes, the result produced by a computer system can be dramatically different from the original. As an alternative, tiny alterations to a starting point may result in minor modifications in the outcome in classical science[60]. According to [61], the chaos sensitivity varies depending on the original conditions and produces unpredictable effects.

In 1975, Li and Yorke were the first to use the term 'chaos' in mathematical literature to describe a situation where system results appear random. Further research into chaos theory was conducted by Edward Lorenz (1963), who also developed an essential weather forecasting mathematical model. The first measurement simulation to identify chaos in a nonlinear dynamical system was Lorenz's Model[62], and it remains the most often used today. Lorenz discovers an unusual behavior in some equations that gives rise to some very complex behavior and chaos behavior that relies on the initial condition that Lorenz finds [62]. Because of its properties, such as sensitivity to the beginning value, complicated behavior, and completely deterministic nature, chaotic maps have been the topic of intense investigation in recent years. Chaotic behavior can be observed in various systems, including electronics, hydrodynamics, lasers, meteorology, climatology, economics[60, 62], and other natural phenomena.

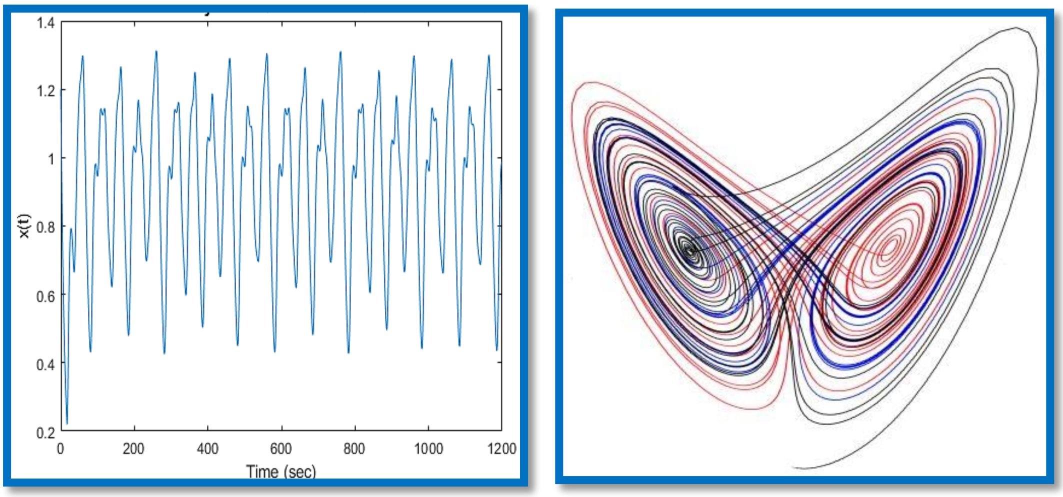
2.5.1 Definition of Chaos.

Chaos is a principle/highly sensitive to initial conditions and has non-periodic behavior Long-term in a deterministic system. One of the essential characteristics of chaos is the following[61].

- Aperiodic long-term behavior: Indicates that pathways of the system do not settle on any fixed points" quasiperiodic Orbits" or periodic Orbits. Thus, the following path will have limited predictability.
- A deterministic system in which a particular initial state or state always leads to the same results. There is no randomness or variance in how inputs are delivered as outputs.
- Sensitivity to initial conditions: Arbitrarily approximating other points with significantly different paths causes a change in the current path to different behavior in the future.

2.5.2 Types of Chaotic Systems

Systems characterized by chaotic behavior can be classified into two types: differential equations (also known as flows) distinguish between those described by difference equations and those described by nonlinear equations (known as maps). Their trajectory and orbit describe the evolution of these dynamic systems. The path that a flow travels as time proceeds are referred to as the trajectory of the flow. An orbit is a collection of points through which a map traverses due to iteration. Chaos can be represented in two ways: as a time series in the temporal domain, as shown in figure (2.2a), or phase space as a weird attractor, as shown in figure (2.2b)[62].



(a) (b)

Figure(2.2) Types of Chaotic Systems:(a) chaotic time series, (b) a strange attractor[62]

An amplitude-time series graph is created by graphing the signal's amplitude against the passage of time. Alternatively, the weird attractor is generated by pitting two or more of the system's state variables against one other. The system variables are most typically characterized as the first or second in a time series or a combination of them [61].

2.5.3 Logistic Map

Chaotic maps are mathematical equations used to generate random sequences that are highly sensitive to their initial conditions and control parameters. Chaotic maps are classified into one-dimensional (ID) and multi-dimensional (MD) chaotic maps; One of them is there are many well-known chaotic maps. The logistic map is one of the simplest and most visible systems for displaying order to chaos transition. The logistic map is a discrete dynamical system with the following definition[61]:

$$\mathrm{x}_{\mathrm{i}+1} = \mathrm{r}\mathrm{x}_{\mathrm{i}}(1 - \mathrm{x}_{\mathrm{i}}) \qquad (2.1)$$

This formula consists of many parts defined as x_i is the initial point which is also called the seed or the root (x_0) of the logistic map. There is an intrinsic growth rate in this equation, and the dimensionless population measure is used to calculate the intrinsic growth rate for the nth generation of the population. In Figure (2.3), the graph of equation(2.1) is a parabola, having a maximum value of r/4 at x =1/2, as seen in the graph of equation(2.1). When limiting the control parameter r to the range of values from zero to four, this equation translates the interval from zero to one into itself. However, the pattern is far less intriguing for other numbers of x and r)[62].

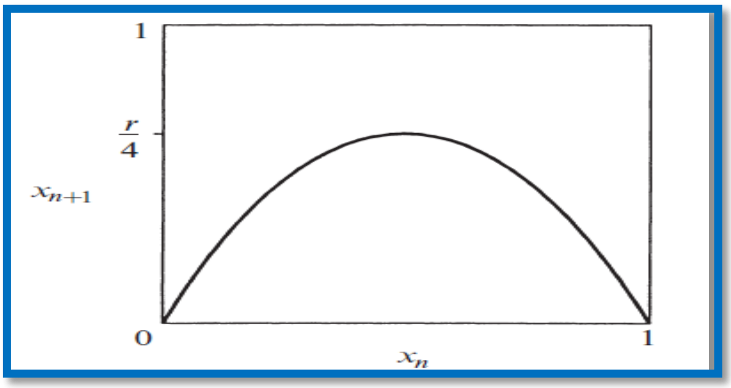


Figure (2.3): The graph of equation(2.1)[62]

Assume r is fixing, choose some initial population x_o, and then use equation (2.1) to produce the progression of x_n, then calculate the period of the logistic map. So, what happens next?

Whenever the population's growth rate is less than one, the population will go extinct: $x_n \to 0$ as $n \to \infty$[62]

For 1 <r<3, The range expands until it reaches a stable condition Figure (2.4). The results are shown as a time series of x_n vs. n in this graph. To make the sequence clearer, Connect the discrete points (n,x_n) with line segments but keep in mind that only the corners of the jagged curves are significant[61].

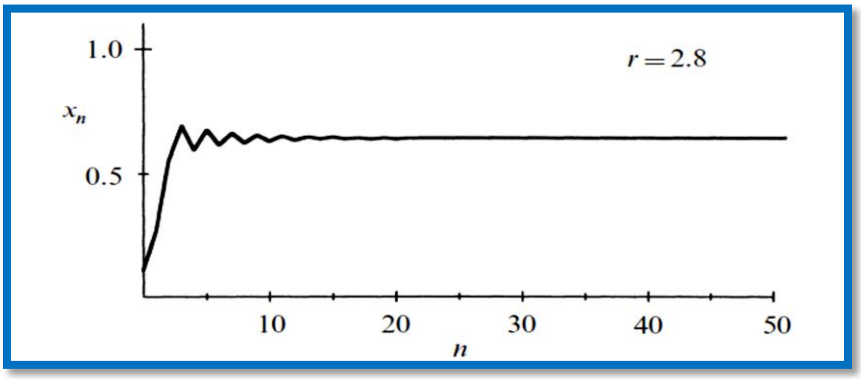


Figure (2.4):The population for 1 <r<3[61]

Increasing the number of generations (r, nearly r=3.3) causes the population to expand again. Still, it does so in an erratic manner, oscillating around the previous steady-state; the huge number of iterations are shown in the figure (2.5). Every two iterations, x is repeated, creating a kind of oscillation called a period-2 cycle[61].

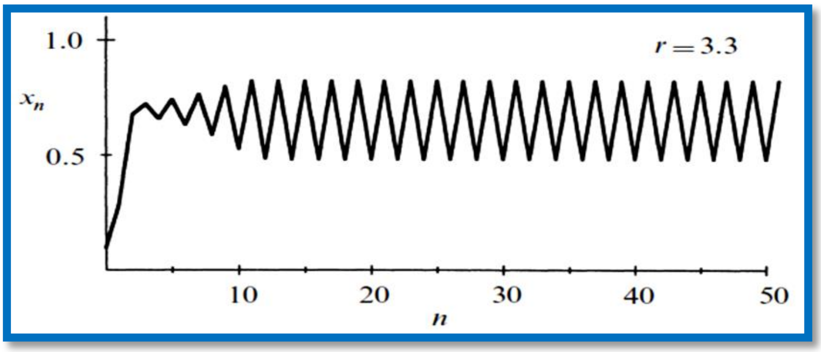


Figure (2.5): The population for as r = 3.3[61]

The population is approaching the end of a cycle that occurs every four generations at greater r, says r =3.5; the previous cycle has doubled its length to period-4 Figure (2.6)[61].

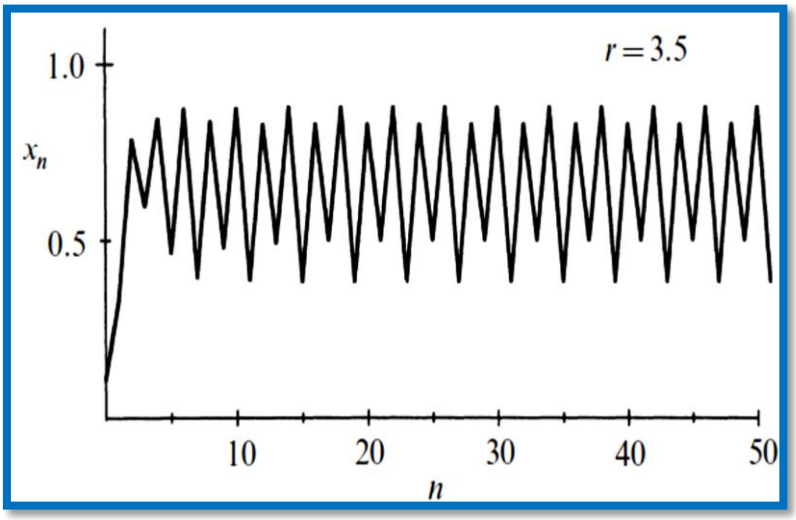


Figure (2.6): A cycle that now repeats every four generations[61]

As r grows, more period-doublings occur, leading to cycles of 8, 16, 32, and so on. Let r_n stand for the value of r when a 2^n-cycle first arises. Then, in the table(2.1), a result of computer experiments discovered.

Table(2.1): the relation between r and number of period

Value of r	**period**
$r_1 = 3$	(period two is born)
$r_2 = 3.449...$	4
$r_3 = 3.54409$	8
$r_4=3.5644$	16
$r_5 = 3.568759$ ...	32
$r_\infty = 3.569946...$	∞

It's worth noting that the bifurcations get faster and faster as time goes on. The r, con eventually becomes a limiting valuer. The convergence is fundamentally geometric, which in the limit of large n, the interval between consecutive transitions decreases by a constant factor[61].

$$\text{constant factor} = \lim_{n\to\infty} \frac{r_n - r_{n-1}}{r_{n+1} - r_n} = 4.669 \qquad (2.2)$$

As r increases, the system will get increasingly chaotic, but the dynamics are more nuanced than that[60]. The essential element of the diagram, in region 3.4 ≤r ≤4, is depicted in figure 2.6. The attractor is a period-2 cycle at r= 3.4, as evidenced by the two branches. As r rises, both branches break simultaneously, resulting in a period-4 cycle. The period-doubling bifurcation is the source of this splitting. As r rises, a cascade of additional period-doublings happens, providing period-8, period-16, and so on, until the map degenerates into chaos and the attractor evolves from a finite to an endless set of points at r = r_∞ ≈3.57[60,61].

The orbital diagram of r > r∞ presents an unexpected mixture of order and chaos with rotating windows amid the chaotic point clouds. A steady period-3 cycle can be found about r=3.83 in the big window. In the lower panel of the figure (2.7), a portion of the period-3 window is magnified. Amazingly, a smaller version of the orbit diagram reappears![63].

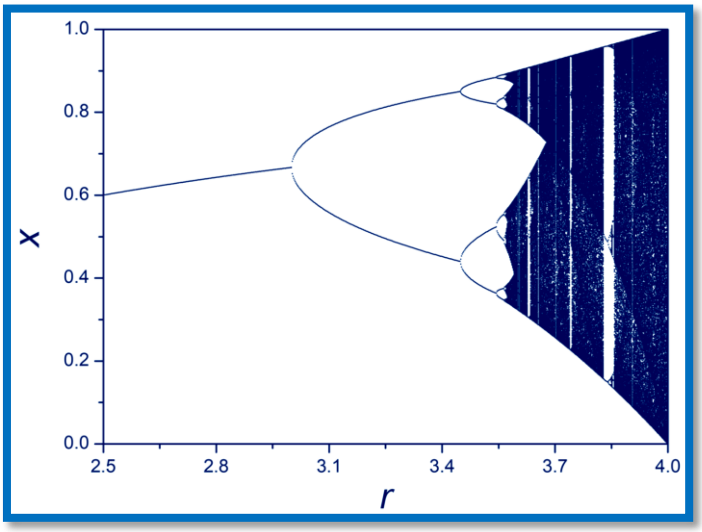


Figure (2.7): Bifurcation diagram for the Logistics map[63]

So the behavior of the logistic map can summarize as the bifurcation of r as follows

1- For $r < 1$, x_i It is a fixed point that is both appealing and stable. As a result, for every value of the seed x_0 between 0 and 1, x_i approaches 0 in an exponential manner

2- For $0 \leq r \leq 3$, $x = ((r - 1)/r)$ is an attractive fixed point.

3- For $3 < r < 4$, The logistic map exhibits various exciting behaviors, such as recurrent period-doubling, the emergence of irregular periods, and others.

4- For $r = 4$ the logistic map is a chaotic situation.

2.6 Cubic Spline Interpolation

To explain the two-dimension cubic spline interpolation, we must know the one dimension cubic spline interpolation.

2.6.1 One Dimension-Cubic Spline Interpolation

Weights are fixed to a flat surface at the points connected in this spline. The consequences are then bent over each other with a flexible strip, resulting in a smooth curve. In theory, the mathematical spline is identical. In this case, the points are numerical data. The weights are the coefficients on the cubic polynomials used to interpolate the data. These coefficients 'bend' the line to move through each data point with no irregular action or breaks in continuity[20]. A series of unique cubic polynomials are equipped between each data point, requiring that the curve obtained be continuous and appear smooth. These cubic splines can then calculate change rates and total change over time. Since the 1970s, cubic interpolation has been used for image interpolation, and it offers a strong balance of complexity and encoding performance[27]. Cubic convolution can be parameterized and optimized for either general efficiency or optimum fidelity over a range of images with unique characteristics. Cubic splines play an essential role in modeling, such as image scaling and animation, where quiet interpolation is required. Splines are useful in image processing for implementing high-quality image magnification. Cubic splines use piecewise cubic polynomials to interpolate (pass-through) the data. Curve fitting with low-order polynomials is particularly appealing because it reduces the computational requirements and numerical instabilities associated with higher-degree curves[26].

The cubic spline function is a third-order polynomial with the following properties in its derivatives: a smooth curve in the first derivative and a continuous curve in the first and second derivatives[20]. In mathematical representation, the cubic spline function S(x) is illustrated in equation (2.3)[20].

$$S(x_i) = y_i\,, \qquad i = 0,1,\ldots n-1 \tag{2.3}$$

The first version of these points is (x_i, $x_{(i+1)}$), so the 2'nd derivatives of these points are $S''(x_i)$ and $S''(x_{i+1})$ respectively. Equations indicate the cubic-polynomial and its parameters are shown in equations(4,5,6,7,8) [27].

$$S(x) = C_1 S(x_i) + C_2 S'(x_{i+1}) + C_3 S''(x_i) + C_4 S'''(x_{i+1}) \tag{2.4}$$

where x ∈ (x_i, x_{i+1})

$$C_0 = \frac{(x_{i+1} - x)}{(x_{i+1} - x_i)} \tag{2.5}$$

$$C_1 = \frac{(x - x_i)}{(x_{i+1} - x_i)} \tag{2.6}$$

$$C_2 = \frac{(C_1{}^3 - C_1)}{6}(x_{i+1} - x_i)^2 \tag{2.7}$$

$$C_3 = \frac{(C_2{}^3 - C_2)}{6}(x_{i+1} - x_i)^2 \tag{2.8}$$

Fourth coefficients (parameters) are needed for cubic-spline interpolation, and the boundary is given as in equation(2.9)[20,27]:

$$S_0''(x_0) = S_{n-1}''(x_n) = 0 \tag{2.9}$$

finally, The mathematical cubic spline equations can be written as equations (2.10)[27].

$$S(x) = c_0 + c_1.x + c_2.x^2 + c_3.x^3 \tag{2.10}$$

2.6.2 Two Dimensional -Cubic Spline Interpolation

The cubic kernel has traditionally been derived in one dimension with one parameter and applied in a detachable manner to two-dimensional (2-D) images. On the other hand, photos are usually statistically indistinguishable[22]. Using the least-squares method and a cubic-spline algorithm, the (2-D) cubic-spline interpolation scheme recalculates the sampled values from the image data[22]. For both definitions and notation, it is helpful to revisit the standard 1-D derivation of the separable kernel. The continuous result R of one-dimensional interpolation is defined by convolving a digital image I samples with a piecewise-cubic kernel S[22].

$$R = \sum_{m=-\infty}^{\infty} I(m)S(x-m), \quad -\infty < x < \infty \qquad (2.11)$$

Where m is the image's dimensions, piecewise cubic polynomials in the intervals define the one-dimensional, asymmetric kernel |x|≤1, and 1< |x|≤2. for |x|>2, the kernel is zero. There are eight degrees of freedom in its most general (symmetric) form [24].

$$S(x)\begin{cases} c_3|x|^3 + c_2|x|^2 + c_1|x|^1 + c_0 & if\ x \leq 1 \\ d_3|x|^3 + d_2|x|^2 + d_1|x|^1 + d_0 & if\ 1 < |x| \leq 2 \\ 0 & otherwise \end{cases} \qquad (2.12)$$

Constraints at the knots are needed to ensure continuous, smooth interpolation and flat-field response. A smooth function is one that never finishes[24].

$$\lim_{x\to -1} S(x) = \lim_{x\to +} S(x) \qquad (2.13)$$

$$S(2) = 0 \qquad (2.14)$$

$$S'(0) = 0, \lim_{x\to -1} S'(x) = \lim_{x\to +1} S'(x)\ S'(2) = 0 \qquad (2.15)$$

The interpolated image will have a constant value if the digital image has constant pixel values. For a unified response x, the following is necessary:

$$\forall x \qquad \sum_{m=-\infty}^{\infty} S(x-m) = 1 \qquad (2.16)$$

Excepting the root, interpolation demands that the function value is 0 for integer abscissa[23].

$$S(1) = 0 \qquad (2.17)$$

If the kernel's first derivative or slope is $\propto at\ x = 1$. The kernel function can be written as the sum of two independent and weighted components ∝.

$$S(x) = S_0(x) + \propto\ S_1(x) \qquad (2.18)$$

Finally, the 1-D Cubic kernel's 2-D separable generalization

$$\mathrm{S}(x, y) = \mathrm{S(x).S(y)} = (S_0(x) + \propto\ S_1(x))(S_0(y) + \propto\ S_1(y))$$

$$= S_0(x)\, S_0(y) + \propto (S_0(x)\, S_1(y) + S_1(x)\, S_0(y)) + \propto^2 S_1(x)\, S_1(y) \qquad (2.19)$$

The equations involved in this work can be obtained by selecting four points from the vector obtained from each dimension of the cover image(RGB) to create the spline curve centered on four points selected from the corresponding information (secret) vector.

Table 2.2. Control Point Choices for Spline Curve Construction.

Cover image vector	**1**	**988**	**3410**	**8090**
Information(secret)	1	39	150	200

The 2D-Cubic spline curve shown in Figure (2.8) is built from the positions of all points in each dimension for the cover image.

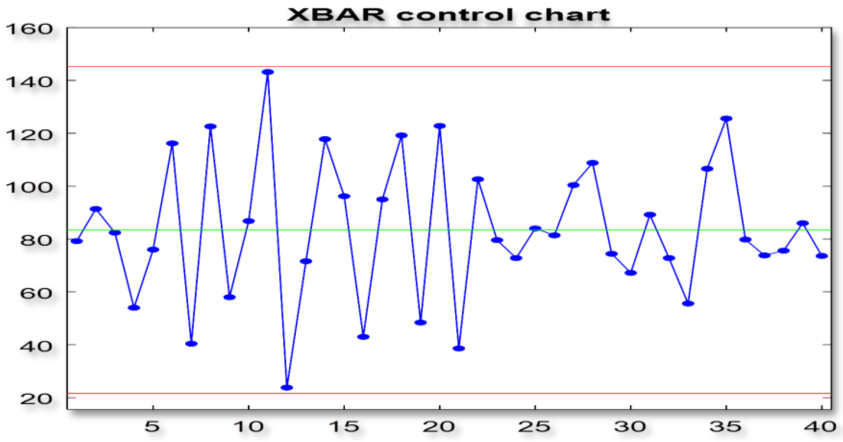


Figure (2.8): The 2D-cubic spline curve

2.7 Database Administration System

The term "databases" refers to the software that maintains ordered, distinct groupings of data that are linked, electronically transmitted, and digitally stored (Database Management Software). In addition to its innate capacity to store data, a database gives the option to retrieve and change information through assessment to evaluate it speedily and prioritization, in addition to its inherent capacity to store data[64].

Many applications in numerous commercial fields have been computerized due to recent advancements in information systems technologies. In many businesses, data has become an essential resource. Thus, efficient access to data, sharing data, extracting information from data, and making use of the information has become a pressing demand[66]. As a result, several attempts have been made to integrate the various data sources distributed over multiple sites and extract information from these databases in the form of patterns and trends. These data sources could be databases managed by Data Base Management Systems(DBMSs) or data warehoused from several data sources in a repository. The introduction of the World Wide Web (WWWW) in the mid-1990s increased the demand for valuable data, information, and knowledge management[65]. The amount of data on the internet has grown to the point where handling it with traditional methods is nearly impossible. As a result, many technologies are being created to provide interoperability and warehousing between multiple data sources and systems and extract information from databases and warehouses on the web[67].

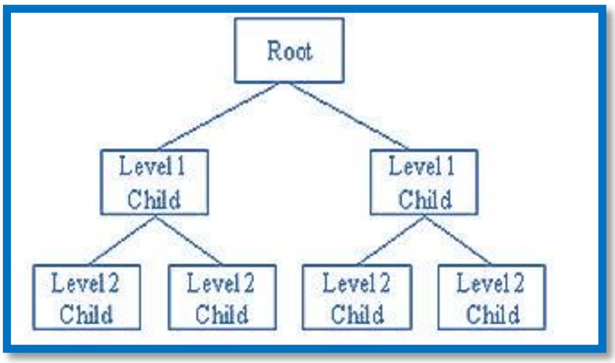
Data or records are stored in a database, which is a collection of information. The objective of database management systems is to facilitate the management of data. A "database management system (DBMS)" is a kind of software system that manages, stores, and organizes data in a standardized manner using a standardized technique. Adding, updating, deleting, and traversing data can be accomplished by using standard procedures and queries. Database management solutions are available in several configurations and sizes[68]. The following is a list of the most widely used database management systems:

1. Hierarchical databases
2. Network databases
3. Relational databases
4. Object-oriented databases
5. Graph databases
6. Entity-Relationship model databases
7. Document databases
8. NoSQL databases

2.7.1. Hierarchical Databases

When implementing a hierarchical database management system (hierarchical DBMSs), information is stored in a parent-children relationship node. In addition to actual data, entries in a hierarchical database carry the data about their parent/child linkage groupings. Hierarchical database models arrange information into a tree-like structure, similar to how trees are structured in nature. That's how the data is kept informed, though many fields have just a single value. The entries are linked together to build a parent-child relationship through links. In a hierarchical database model, each child entry has only one parent and vice versa. Figure (2.9)[65] shows that a parent can have more than one kid.

Structure inflexible but straightforward. To get the data for a field, you need to go through each tree to find the record. IBM creates the hierarchical database system structure in the early 1960s. The one-to-many connection between parents and children creates a hierarchical structure. High performance and availability systems are required when developing, especially in the banking and financial industries. Hierarchical databases are often used to achieve these goals[69].



Figure(2.9): Hierarchical databases include the IBM Information Management System[65].

2.7.2 Network Databases

A system for managing relationships between items built on a network structure is called a network database management system (Network DBMS). Users of network databases are primarily comprised of large digital computers. Unlike hierarchical databases, which allow each node to have only one parent, network databases allow each node to have several associations with other nodes in the same network, as shown in figure(2.10). According to [67, 68], network databases are similar to a cobweb or a network of interconnected records. Families with children in the network are referred to as database members; in contrast, their offspring's parents are referred to as database occupiers. It differentiates them from the others since they may have more than one parent, which is possible for a child or member[68].

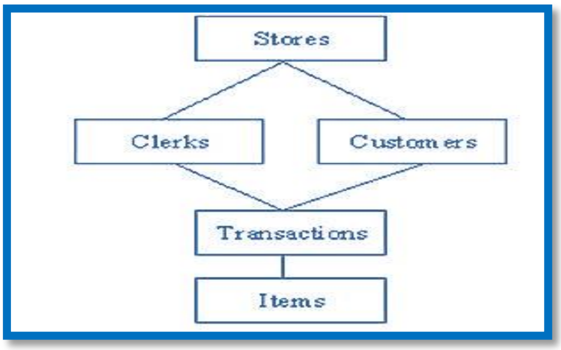


Figure (2.10): Network database management systems [68]

2.7.3 Relationships Databases

Relational databases are the most often used databases nowadays because they are more effective than any other database type in dealing with enormous amounts of data. A relational database is a collection of data structured in connected tables that provides a system for reading, writing, altering, and even more complicated data activities all at the same time. The database tries to arrange information storage and extract this information in a more structured manner based on queries entered into the relational database. Without needing to reorganize the physical tables that store the data, it can be reorganized in various ways, including unimaginable tables[65]. Coded invented the relational database in 1970[64]. Although interest in this architecture was first limited to academia, relational databases have become the dominant kind for high-performance applications[64].

When using a relational database management system (RDBMS), the link between data is relational, stored in tabular form, consisting of columns and rows. Each row in a table represents a record, and each column represents a characteristic of that record. The field in a table represents a data value in the form of a number.

Structured Query Language (SQL): is the language that is used to query "relational database management systems" (RDBMSs), including inserting, updating, removing, and querying records. Each row in a relational database is uniquely identified by a key field present in each table. It is possible to link two information tables together using these key fields, as shown in figures(2.11)[70].

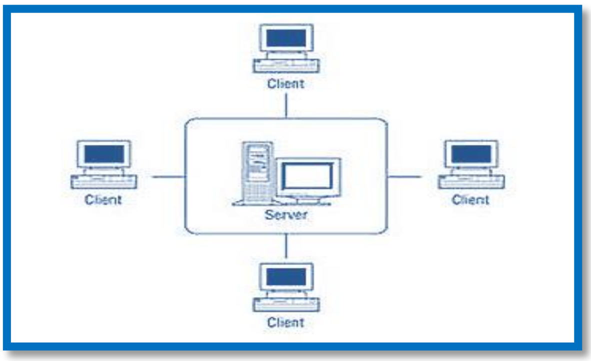


Figure (2.11): Relationships Databases management systems[70]

The most common and widely used databases are relational databases. Oracle, SQL Server, MySQL, SQLite, and IBM DB2 are the most used. Observe the properties listed below:

i. The values are atomic.

ii. Each row is a complete unit.

iii. The phrase "column values" relates to the same concept as "row values."

iv. The columns are unimpressive in their appearance.

v. The order in which the rows are shown is irrelevant.

vi. Each column has a common name.

2.7.4 Object-Oriented Model

In order to operate effectively, it is essential to know the importance of "object," "oriented," "programming" in everyday life. As a consequence of the development of object-oriented database management systems, the syntax of C++ and Java have improved. In addition to native language compatibility, it also features comprehensive database-building capabilities[66]. This strategy is equivalent to designing applications instead of using various programming languages and a consistent data structure and functional programming environment. Consequently, less code has to be written, unique data structuring is employed, and software models are simpler to maintain. Designers of object-oriented databases may create entire database applications with a little more effort if they work hard enough[65].

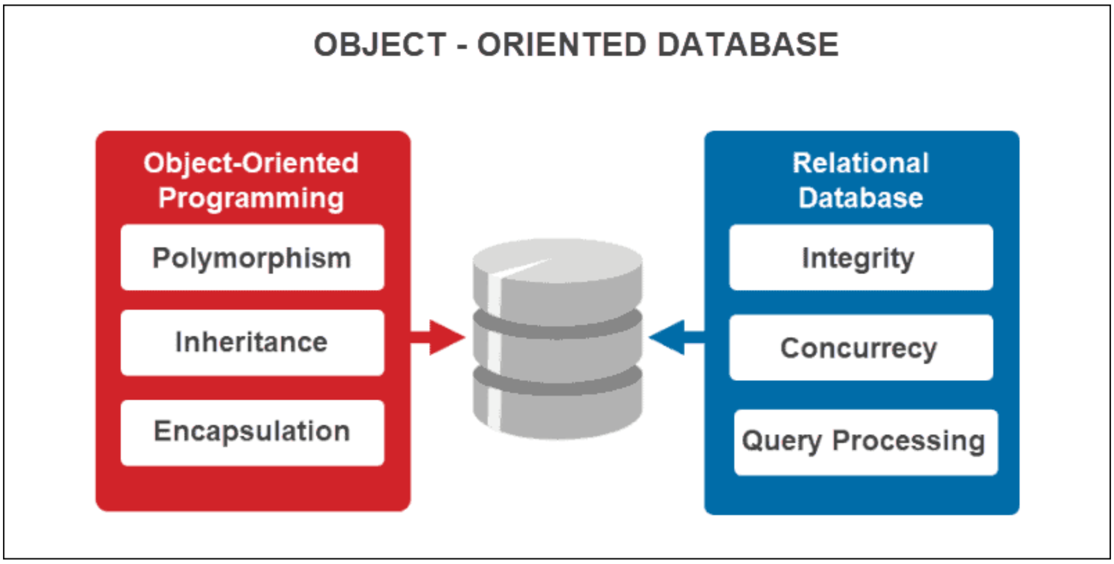


Figure (2.12): Object-oriented Databases management systems[65]

Object-oriented databases use objects, which are little pieces of software that can be reused. The object-oriented database stores the objects themselves. Each item has two components:

i. a piece of information (e.g., sound, video, text, or graphics).
ii. Methods are specifications or program applications that teach you how to use the data.

In the early 1980s, object-oriented database management systems (OODBMs) were developed. Some OODBMs were created to operate with object-oriented programming languages like Delphi, Ruby, C++, Java, and Python. TORNADO, Gemstone, ObjectStore, GBase, VBase, InterSystems Cache, Versant Object Database, ODABA, ZODB, Poet, JADE, and Informix are some of the most popular OODBMs[71].

2.7.5 Graph Databases

Graph databases are non-relational databases (NoSQL databases). that utilize a data structure for varying purposes and are a kind of NoSQL database. Nodes, edges, and properties are used to store the information.

A Node represents an entity or instance in a graph database, such as a customer, person, or car, and it is the same as a record in a relational database system. An edge is a node-to-node connection in a database table. A node's properties may store extra information about the node that belongs to it. Examples of database systems include Neo4j, Azure DB, SAP HANA, Ignite, Oracle Spatial Graph, ArrangoDB, MarkLogic, etc. Some relational database management systems, including Oracle microsoft SQL Server 2018 and later, support graph database structures [66].

2.7.6 Entity Relationship Models for Databases(ER)

A database is commonly used to implement an ER model. The fields in a table reflect the attributes of the entity types that are represented in a basic relational database system. The rows of the table represent the instances of the entity types. In a relational database, a connection between entities is created by putting the primary key of one entity as a pointer or "foreign key" in the table of another entity. The entity-relationship model was developed by Peter Chen in 1976[66], [67].

2.7.7 Databases of Documents

Document databases (Document DB) are another type of NoSQL database that stores data as documents. Each document represents data and its relationships with other data pieces and data attributes. In document databases, information is kept in a key-value format[66], [67].

As a result of their document store and NoSQL features, document databases have risen in popularity in recent years. NoSQL data storage enables you to store and seek content more rapidly than conventional SQL data storage, advantageous in certain situations. Among the most prominent NoSQL databases are: Hadoop/Hbase, Cassandra (Hbase), Hypertable (MapR), Hortonworks (Cloudera), Amazon SimpleDB (SimpleDB), Apache Flink (Apache Flink), IBM Informix (IBM Informix), Elastic (Elasticsearch), MongoDB (MongoDB), and Azure DocumentDB [66].

2.7.8 NoSQL databases

Databases that don't use SQL as their primary data access language are NoSQL databases. In addition to graph and network databases, object and document databases are also included in the NoSQL database category. What is a NoSQL database, according to this article?

Because NoSQL databases do not have established schemas, they are an excellent choice for quickly changing development environments. Changes to NoSQL databases can be made on the fly without disrupting applications. The five main kinds of NoSQL databases are column-based, document-based, graph-based, key-value-based, and object-based. The following is a list of ten widely used NoSQL databases which are: DB Cosmos, ArangoDB, Couchbase Server is a database management system; CouchDB, Amazon DocumentDB is a database that stores documents, CouchBase, MongoDB, Elasticsearch\sInformix, and SAP HANA Neo4j are a database management system for SAP HANA[72].

2.8 Cloud Computing of the System

The term "cloud computing" is currently the most popular in the information systems industry is a broad term. A cloud computing environment is a method of obtaining on-demand computer resources such as software, storage, and even infrastructure through the usage of the internet. It has been around 50 years since cloud computing first appeared, but it is only recently that technology has progressed to the point that it has become a multi-million dollar industry. When it comes to cloud computing, It may signify many separate stuff to various people, because there are many multiple definitions of what it means. To put it simply, cloud computing is the act of temporarily accessing information on-demand computer resources via the internet or even a network connection. Cloud computing is becoming more popular due to its simplicity[73].

For the most part, the Cloud is an amalgamated mix of operating systems that enables access to information technology services (IT). The flexibility of providing these services through the Cloud is advantageous because it is possible for cloud services to be provisioned and de-provisioned on-demand, based on the supply for such services[66]. The idea of cloud computing is storing data and information away from our physical location and accessing it via the internet. Thus the data and information are not bound to any area. Whenever you gaze up, Clouds may be seen in the distance someplace in the sky, regardless of geographical position. Data and information are available whenever someone connects to the internet, regardless of his actual location. How did a straightforward explanation become known as "cloud computing"? There are suggestions that the name was chosen for technological reasons[67].

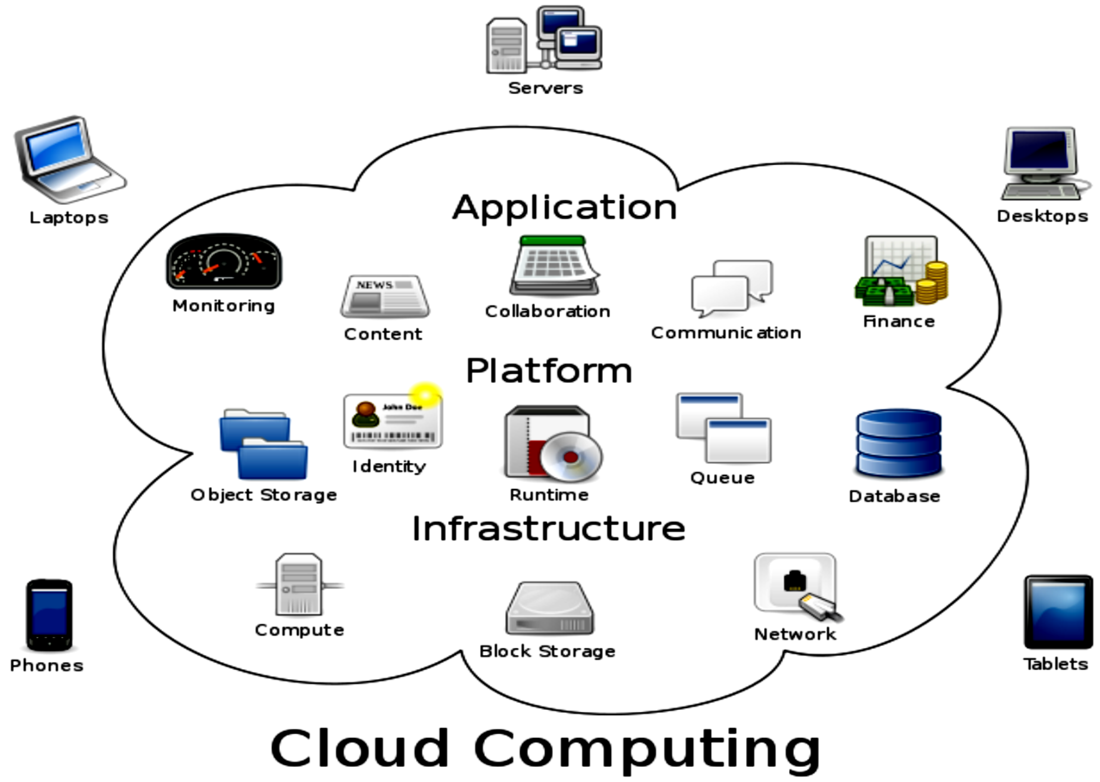


Figure (2.13): Cloud Computing Logical Diagram
"Source: Wikipedia < http://en.wikipedia.org/wiki/cloud_computing>"

Cloud computing was created for commercial objectives and is by definition, service-oriented. It is built on the foundation of centralized data centers. It's not possible that the protocols and interfaces utilized by different cloud providers are the same. Google, Amazon, and others have demonstrated how it is possible for cloud computing infrastructure to serve a number of customers and thousands of activities at the same time. It hasn't been easy for them since they first went to the Cloud, but they've learned a lot along the way thanks to security flaws and trial-and-error approaches, and they've resolved many of these difficulties. They can also claim near-perfection, but in the Cloud, near-perfection only lasts until someone shows differently[71].

2.8.1Clouds Computing Categories

There are three types of clouds category. A Private Cloud is usually hosted on-premises and secured by the company's firewall, as opposed to a public cloud. Using the Public Cloud, you may access a network of virtualized servers located offsite that are shared by a variety of customers and can be accessed via a broadband connection. The resources of a Private Cloud are not made available to anybody else. Using a hybrid cloud, you may mix resources outsourced to third parties with the bulk of your data banks and infrastructure still at your location and secured by a trusted firewall[66, 67].

A confluence of such technologies seems to be what Cloud Computing is all about, combining some of their most essential characteristics to provide consumers with a better experience. Cloud Computing comprises five fundamental characteristics, three service models, and five deployment methods, all of which work together to achieve this goal.

2.8.2Major technologies

Throughout the years, the evolution of computing has seen some adjustments. Other technologies arose and were used at some point during this progression. It was necessary to discuss them to help grasp the significance of our current shift into a computing environment driven by cloud computing[66].

i.Virtualization: One of these technologies is virtualization, a technique for concealing physical characteristics of computer resources that enable other computers, programs, or line services to interface with those resources. When it was initially launched in 1972, IBM's platform 370 would be the one to take advantage of it. In addition to having the operating system CP / CMS installed, this would be the first industrial computer designed for virtualization, which allowed several copies of the software to run simultaneously.

ii. Grid computing The term "distributed computing" refers to a system that allows parallel applications to execute on heterogeneous distributed resources while ensuring constant and low-cost access to help regardless of the user's location. By speeding up several simultaneous applications and repurposing previously underutilized processing capacity, the grid computing technique consolidates previously scattered computer resources into a joint "virtual supercomputer." As a result of considerable advancements in both the performance and the cost of computer networks and microprocessors[66, 67], it has been possible to use networks (grids) in recent years.

iii. Utility computing refers to the practically automated leasing of computing. Resources like equipment, application, and communications networks (bandwidth) are allocated based on customer needs. To put it another way, what was once deemed a product is now considered a service—a "utility" service, such as electricity or a phone. "If computers of the kind you have proposed become the computers of the future, then computing may someday be organized as a public utility, just as the telephone system is a public utility" [66].

2.8.3 Models of Cloud Computing Services

To get the best cloud computing solution, you must first understand the fundamental characteristics of cloud computing and its main architectures. Each firm chooses a cloud service and deployment model depending on its business, operations, and technology needs. Here, a quick overview of the three models (IaaS, PaaS, and SaaS), which as a basis for learning more about the advantages of cloud computing [74].

i. **SaaS (Software as a Service)** indicates that a customer can use a program that has not been downloaded onto his or her machine. It is saved in the Cloud and may be viewed on his own computer through the internet using a web browser.

ii. **PaaS (Platform as a Service)** describes a client's ability to transfer cloud apps developed using a software package and tools cloud infrastructure provider to a cloud environment.

iii. IaaS (Infrastructure as a Service) refers to the provision of virtual machines to customers, including processing, data storage, servers, and network components. The consumer "rents" the computers from the supplier, and the client pays for utilization or usage time. The client's computer environment is delivered as desired, and he is not responsible for the costs of maintenance or upgrades of the utilized hardware.

2.8.4Cloud Computing, Deployment models

Based on requirements, cloud computing deployment can take on a variety of shapes and forms. The following five deployment types have been recognized, each with its own set of features that uniquely satisfy cloud services and users' needs [67], [75].

i.Private Cloud - The Private Cloud model is predicated on assuming that a single firm only utilizes the Cloud's infrastructure. An external entity may be in charge of this, or an external entity may control it, and it may or may not be located on the company's premises.

ii. A community cloud : is a model that predicts that cloud platform support will be provided by a collection of businesses that have come together to create a community with common interests. Operation of the system may be performed out by every company or by an independent organization. It can occur either within or outside its physical structures and facilities**.**

iii. The Public Cloud: Model forecasts that infrastructure will be open to the general public or a large number of businesses and that it will be handled and regulated at all stages by a business that offers Cloud computing services

iv. Hybrid Cloud: The hybrid Cloud model forecasts that the infrastructure will mix private and public cloud types.

v. Cloud Partner: It is assumed that credible cloud services host the architecture and that it is maintained in cooperation with the same provider under the terms of the Cloud Partner model. The firm may utilize its resources on the Cloud and make them available to other businesses to use.

2.9 Problems and Attacks on the Cover Image.

As previously noted, resilience and security of the information are two essential characteristics for a reliable steganographic technique to be effective. There is a trade-off between these two needs; however, by testing the method with signal processing assaults, this trade-off can be minimized to the greatest extent possible. Every application has its own set of criteria, and each one offers the choice of selecting high robustness while sacrificing signal quality or vice versa. Every steganographic technique is effective even when there are no transformations or attacks. The following are some of the most typical types of processes that a signal goes through when it is transferred across a medium: amplification

2.9.1 Salt & Pepper Noise.

A fault in the camera's sensor, a software failure, or a hardware malfunction during the capture or transmission of an image is the most common cause of Salt & Pepper noise. As a result of this condition, according to the Salt & Pepper noise model, only a proportion of all image pixels are affected, while the remaining pixels are not contaminated[76].

2.9.2 Additive White Gaussian Noise (AWGN).

Additive White Gaussian Noise (AWGN) is familiar to every communication channel, the statistically random radio noise characterized by a wide frequency range regarding a signal in the communications channel. Noise with the same power at all frequencies in the range of $\pm\infty$ would necessarily need to have infinite power and is therefore only a theoretical concept as in equation (2.20) [77,78].

$$p(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-m)^2}{2\sigma^2}} \qquad (2.20)$$

X is a random number with center or means (m) and standard deviation (σ).

2.9.3 Poisson noise.

Optical variation, also known as Poisson vibration, is a fundamental uncertainty connected with light analysis. It is caused by the quantitative nature of light and the autonomy of photon detections, and it is intrinsic to the measurement of light[79].

2.9.4 Speckle Noise

Speckle noise is a form of noise. Because of the dispersion of electromagnetic waves induced by the transducer, pictures of this form of noise have a granular pattern. When waves reflected on a rough texture interact, interferences are created, resulting in noise in the registered image. This noise is hazardous because it makes it difficult to detect injuries, particularly in low-contrast images. It is essential to have an accurate and reliable model to perfect the de-noising methods[80].

2.10 Performance Parameters.

The bit rate (BER), power ratio (SNR), peak signal to noise ratio (PSNR), and root mean square value are used to assess the quality of the correlation between the original and derived information.

2.10.1 Bit Error Rate.

The bit error rate (BER) is the percentage of corrupted bits during digital data transmission due to noise, interference, and distortion. The BER of a binary image is usually determined using the equation below, where BER stands for the number of error bits and relates to the picture size calculated in equation (2.21)[81].

$$BER = \frac{B_{err}}{M*N} * 100\% \qquad (2.21)$$

Where *M* and *N* are the dimensions of the host image.

2.10.2 Signal to Noise Ratio.

The signal-to-noise ratio measures how much the signal has been damaged by noise. The signal-to-noise ratio is defined as the power ratio of the signal to the noise. It can also be thought of as the ratio of the intended signal (say, a music file) to the background noise level. The equation can be used to calculate SNR (2.22)[81].

$$SNR = \frac{Power_{signal}}{Power_{Noise}} \tag{2.22}$$

SNR can also be calculated by equation (2.23):

$$SNR = 10 \log_{10} \frac{\sum_{n=1}^{N} x^2(n)}{\sum_{n=1}^{N}(x(n)-x'(n))^2} \tag{2.23}$$

X is the un-watermarked (original) image, and x's is the watermarked image. Both x and x's have N samples calculated by equation (2.23) above.

2.10.3 Root Mean Square Value

The square root of the mean value of the squared values of the quantity obtained over an interval, which can be determined using equations (2.24)and (2.25)[82]:

$$RMS = \sqrt{\overline{MSE^2}} \tag{2.24}$$

$$MSE = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [x'(i,j) - x'(i,j)]^2 \tag{2.25}$$

2.3.4 Peak Signal to Noise Ratio

PSNR (peak signal to noise ratio) measures signal to noise ratio in digital signal processing. It is calculated as the proportion between such a signal's most significant possible signal and the maximum possible noise power and corrupting noise that affects how well an image is represented.

PSNR is commonly stated on a decibel scale, as in the example below. The peak signal-to-noise ratio (PSNR) is a regularly used indicator of image reconstruction quality. In this situation, the signal is the original data, and the noise represents the created error. A high value of PSNR implies that the image is of excellent quality; it can be calculated using the following equation (2.26)[82]:

$$SNR = 10\log_{10}[(255)^2/\mathrm{MSE}] \qquad (2.26)$$

Chapter Three

CHAPTER THREE

IMPLEMENTATION OF PROPOSED SYSTEM

3.1 Introduction

Emerging advancements in information and communication technology have resulted in significant improvements in community services, particularly in the healthcare sector over the previous decade. Several studies have arisen to support the healthcare domain; these studies include the following: It created a framework for e-health readiness that focused on the information and communications technology infrastructure at a micro-level as defined by the World Health Organization's definitions of e-health.

As hospitals realize the value of using Electronic Patient Records, the concentration in healthcare information technology is growing. The electronic Patient File System (EPFS) job is to offer health professionals and medical research a comprehensive picture of hospital work health in general. To do so, some obstacles must be overcome, including interoperability, which occurs when a patient has multiple medical records, accountability, which refers to the ability to identify the healthcare parties who handle medical data, the inability to uniquely identify patients, the use of standardized medical terminology, maintaining patient privacy, and effectively retrieving patient data.

This study aims to answer the following research questions: What are the advantages of the present patient record system in hospitals? What is the most practical strategy to support medical researchers by leveraging patient healthcare data? And how might electronic patient record systems increase the quality of diagnosis data retrieval while also saving time for healthcare providers?

The need to protect the contents of the information generates many techniques; one of these is chaos-cubic spline transforms. In these techniques, the data of the host image is encrypted by a logistic map, and the content of the massage (patient information) is encrypted and passes through a 2D-cubic spline transform which is used for the first time to increase its security and then embedded in the content of the logistic map.

This chapter describes The Electronic Patient File System using encryption techniques and domain transformations.

3.2 Proposed System Design

An electronic record is a record in digital format that contains all information and notes related to a patient's health collected by authorized physicians and employees within a single health facility, such as personal and administrative information of the patient, diagnostic information, medical history, vital signs, and therapeutic procedures, and stored in a secure database that can be access to it from different areas and for authorized persons only.

The principal motivation for creating and using the electronic record was based on several factors related to healthcare financial management, the most important of which are Significant material losses due to paper archiving equipment. Medical treatment is generally in-patient (hospitals), out-patient (clinics), and emergency. By calculating the time, the doctor wastes approximately 38% of his time working on the paper; the nurse, on the other hand, spends roughly half of his time dealing with paper. Furthermore, 30% of paper records are lost or destroyed, and many errors occur while filling the paper. Focusing on the privacy risks in the paper record and archiving the patients' safety did not receive any attention in our country, unlike the developed countries that paid much attention to this aspect.

Implementing the Electronic Patient File System (EPFS) is the first database and workflow system in Iraq (in general hospitals). It's useful for administration, patient care, research, and archiving. It could be used by a hospital director to monitor a physician's performance or for statistical reporting in management in less time.

The suggested system may be implemented by combining some of the subsystems that execute particular tasks with the primary purpose of the overall system. According to its role, the proposed system consists of some subsystems: face detection part, steganography using logistic-2D cubic spline transformation parts, database and clouding part, and finally, the reversed system to recover the patient information. Figure (3.1) shows the block diagram of the central system and the subsystems of the encrypted parts, cloud computing system, and the subsystem to recover the patient information.

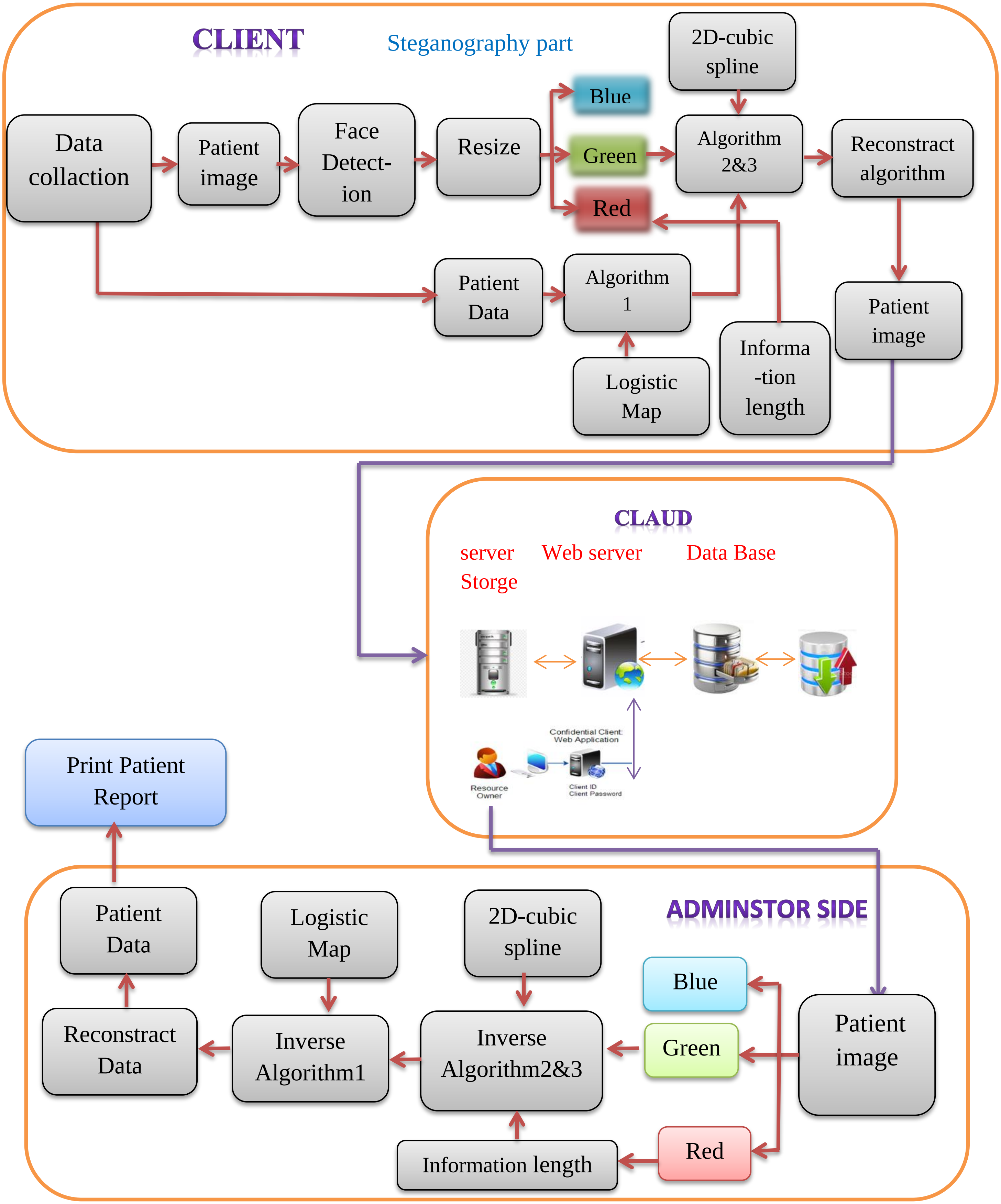


Figure (3.1) :The block diagram of the proposed system

The first subsystem is the embedding process side which can describe in the following steps:

a) Read the original(patient) image of size N*N, which is the patient image.

b) Entering the patient file information.

c) Apply the face detection algorithm on the patient image, resize it to 180*180 in this thesis, and extract each image color alone.

d) convert the green color to the binary image with three-dimension (x,y, and z plans).

e) Generate the 2D- cubic spline interpolation to locate the binary green color positions to hide the patient information in these positions.

f) Generate the chaos attribution, the logistic map with dimensions equal to the size of the patient file information.

g)Encrypt the patient file information in the logistic map to produce secure information.

h)Applying the encryption algorithm to hide the secure patient information in the location identified using 2D-cubic spline interpolation.

i) Hid the length of the patient file as a key in the red color.

j) Finally, Apply the inverse encrypted algorithm to reconstruct the original, secured image.

The second subsystem is the channel side, which the information is passing through it to the administer side for storing, interfacing and is subject to attack and noise.

The third subsystem is the cloud computing side, the steps of giving information are as follows:

a)Upload the information that is needed to complete the patient file information to sort it in the database

b) Access the information in the cloud computing of a web design interface that gives access to the moderator and specific user to reach for specific information.

Finally, On the receiver side, the extraction process of the patient information is as follows:

a) Read the patient image of size N*N, which is 180*180 from the uploading side.

b) Extract the colors of the image alone(red, green, and blue).

c) convert the red color to the binary to extract the key from it, representing the length of the patient file information.

d) convert the green color to the binary image with three-dimension (x,y, and z plans).

e) Generate the 2D-cubic spline interpolation with a length of the patient information to locate the binary green color positions and extract the patient data from these positions.

f)Generate the logistic map attribution with dimensions equal to the key(length of patient file information) to extract the patient data.

g) Finally, convert the patient data from the string value to the characters and print the patient report

3.2.1 Patient Image

PNG (Portable Network Graphics) is an image compression file format. Different patient images from the camera or scan are taken with size N*N. The suggested system is effective under certain circumstances, which are as follows:

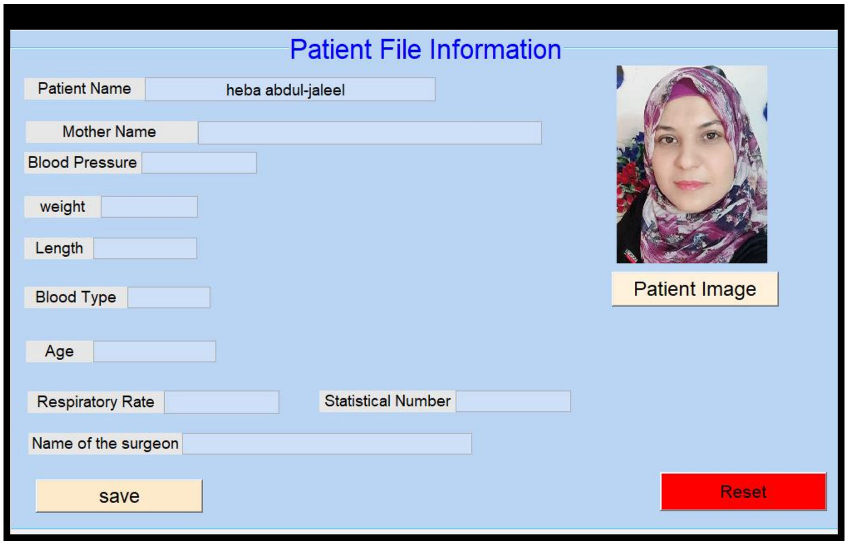
1. The proposed system is utilized with the png and jpg styles of human images, as shown in Figure(3.2).

2. There are almost 20 people represented in the database's pictures.

3. Camera system that is fixed in place (fixed acquiring image system) that has an RGB picture model and a resolution of ((N*N).

4. All images are read in the MatLab program and converted to resolution 180*180.

5. These images are subject to the face detection subsystem to extract the face information that needs in the program.



Patient File Information

Patient Name: heba abdul-jaleel
Mother Name:
Blood Pressure:
weight:
Length:
Blood Type:
Age:
Respiratory Rate:
Statistical Number:
Name of the surgeon:

Figure (3.2): Operation of entering the information

3.2.2 Face Detection

The capacity to discern faces from non-facial items in an image or video is known as face detection. The Viola-Jones algorithm is durable, robust, and quicker despite being obsolete.

Human faces can detect with this technique. The algorithm is divided into four stages:

1. Selection of Haar-like characteristics.

2. Creating a whole image.

3. Training on the Adaboost

4. Classifiers that are stacking on top of each other.

Vision.CascadeObjectDetector comes with many pre-trained classifiers for detecting frontal faces, profile faces, noses, eyes, and the upper body. These classifiers, however, are not always enough for a given application. The computer vision toolbox may train a custom classifier on an image database.

Figure(3.3) depicts the outcome of the face detection step on a random sample picture, which is used to illustrate the operation of the proposed system in more detail.

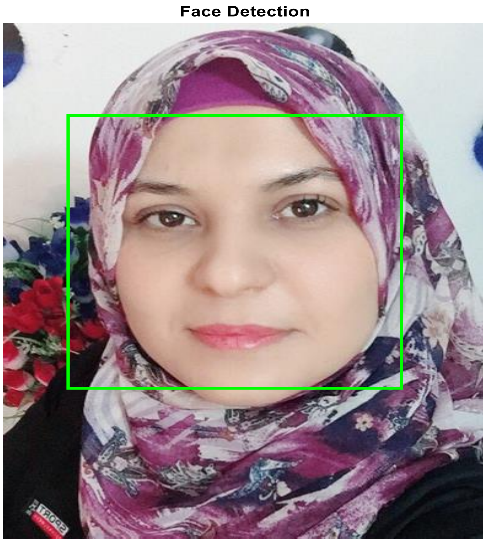


Figure (3.3): The effect of the face detection stage on the sample image

3.2.3 Cropping and Resized Image

Cropping is a technique used in the photography, film processing, broadcasting, graphic design, and printing industries. Cropping is the process of removing undesired parts from a photograph or illustration. The procedure typically draws some of the image's peripheral areas to remove unnecessary rubbish, improve framing, adjust. The cropping of the sample image is shown in figure (3.4). After cropping it, the image is resized to the 180 *180 resolution in the system.

Figure (3.4): Cropping and resizing of the sample image

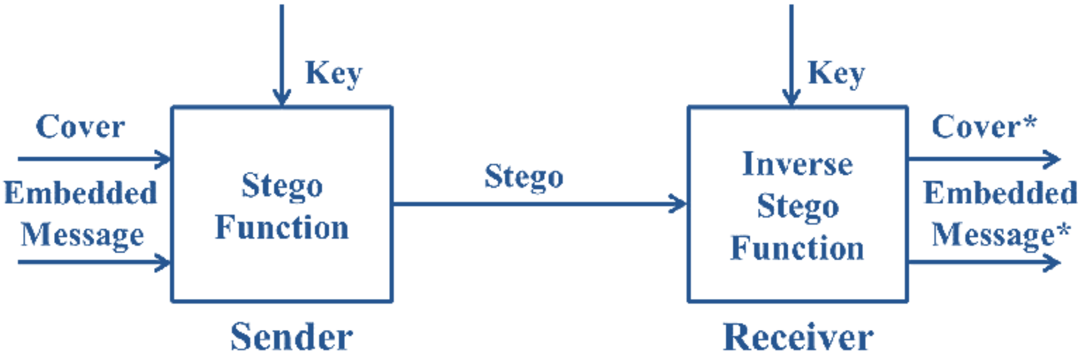
3.2.4 Steganography System

Everything is possible when it comes to that "something." it is the art of hiding a secret message inside (or even on top of) a non-secret item called steganography. These days, many instances of steganography include concealing a bit of text inside an image. Alternatively, you may conceal a secret message or script inside a Word or Excel document.

The term "data concealment" refers to a kind of data hiding that may be accomplished in several ways. The term "covert communication" refers to a form of communication in which communications are concealed utilizing any medium; This is accomplished via steganography.

Steganography is a practice that enables secrecy – and deception – in the same way, that cryptography is a science that mainly allows privacy.

Within a cover file, steganography hides many forms of data.; images, texts, videos, and other messages can be used as input. Although it is nearly identical to the cover file, the generated stego file contains secret information. Steganography exploits human perception. Human senses are not trained to hunt for files with information concealed inside them, even though algorithms can perform what is known as Steganalysis (Detecting the use of steganography). The block diagram of a safe steganographic system is shown in Figure (3.5).



Figure(3.5): A generic Steganography System

The following are the components of a steganographic system:

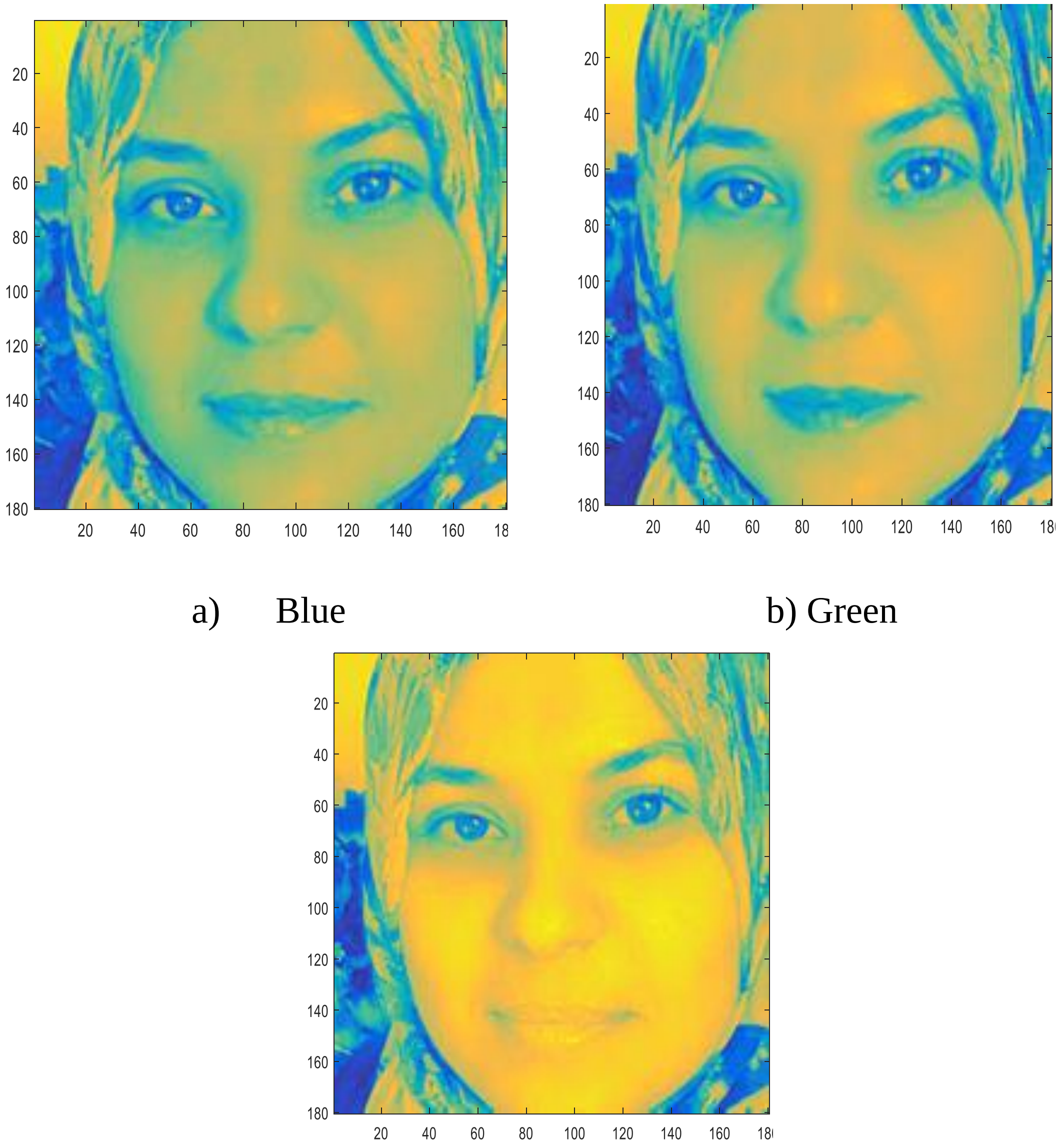
The secret message: or information to be kept hidden.

The data/ medium masked the private message (cover file/digital medium).

- **Stego file:** A reworked version of the cover with the hidden message.
- **Key:** Both the sender and recipient must know additional confidential data for the embedding and extracting processes.
- **Steganographic function:** A steganography function accepts cover, secret message, and key as inputs, while the outputs are stego files.
- **Steganographic inverse function:** A steganography function with the inputs stego file and key output a secret message; this is the inverse procedure employed in the embedding process. The result of the extraction process is identical to the input of the embedding process.

The steganography algorithm varies depending on the application; in this thesis, the medical application is used, and the procedures are made on the cover image produced from the previous steps as follows:

1-Extract the colors of the cover image that cropped in the last step to red, green, and blue, as shown in figure(3.6)

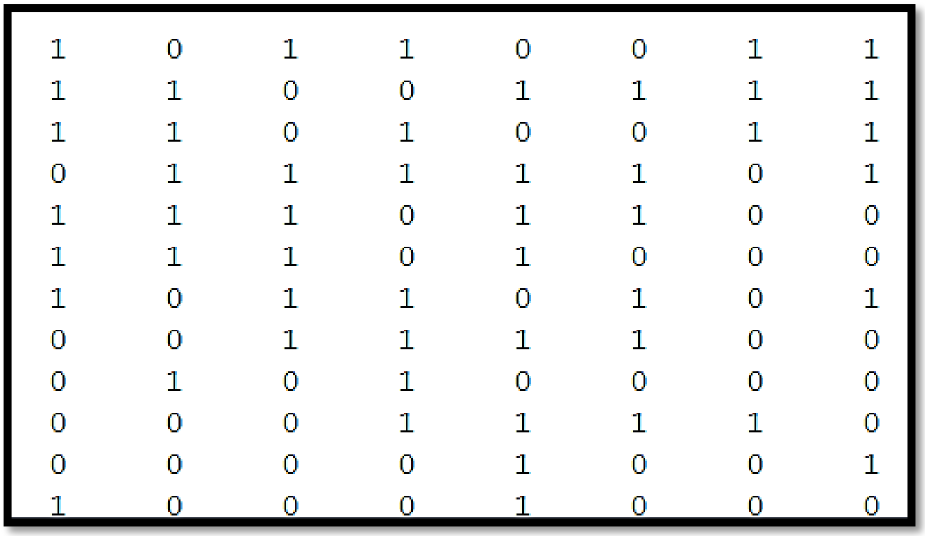


a) Blue b) Green

c) Red

Figure (3.6): The colors of the sample image

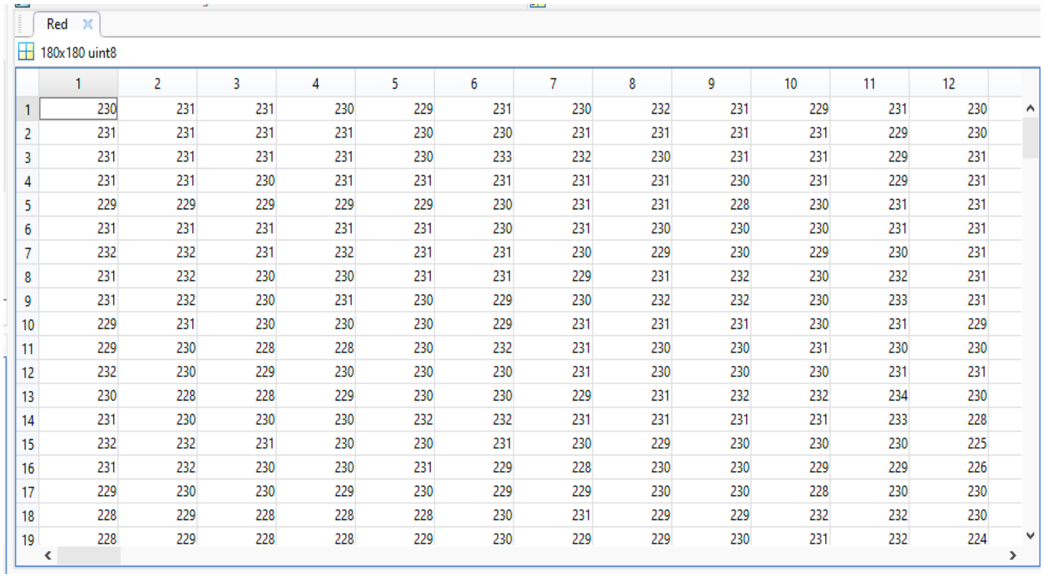
2. In digital image processing, binary pictures are frequently used as masks, thresholding, and dithering. Simple run-length compression algorithms work effectively for most binary images. Binary images can be thought of as two-dimensional integer lattice subsets. Figure (3.7) shows a simple sample of the binary representing.



```
1   0   1   1   0   0   1   1
1   1   0   0   1   1   1   1
1   1   0   1   0   0   1   1
0   1   1   1   1   1   0   1
1   1   1   0   1   1   0   0
1   1   1   0   1   0   0   0
1   0   1   1   0   1   0   1
0   0   1   1   1   1   0   0
0   1   0   1   0   0   0   0
0   0   0   1   1   1   1   0
0   0   0   0   1   0   0   1
1   0   0   0   1   0   0   0
```

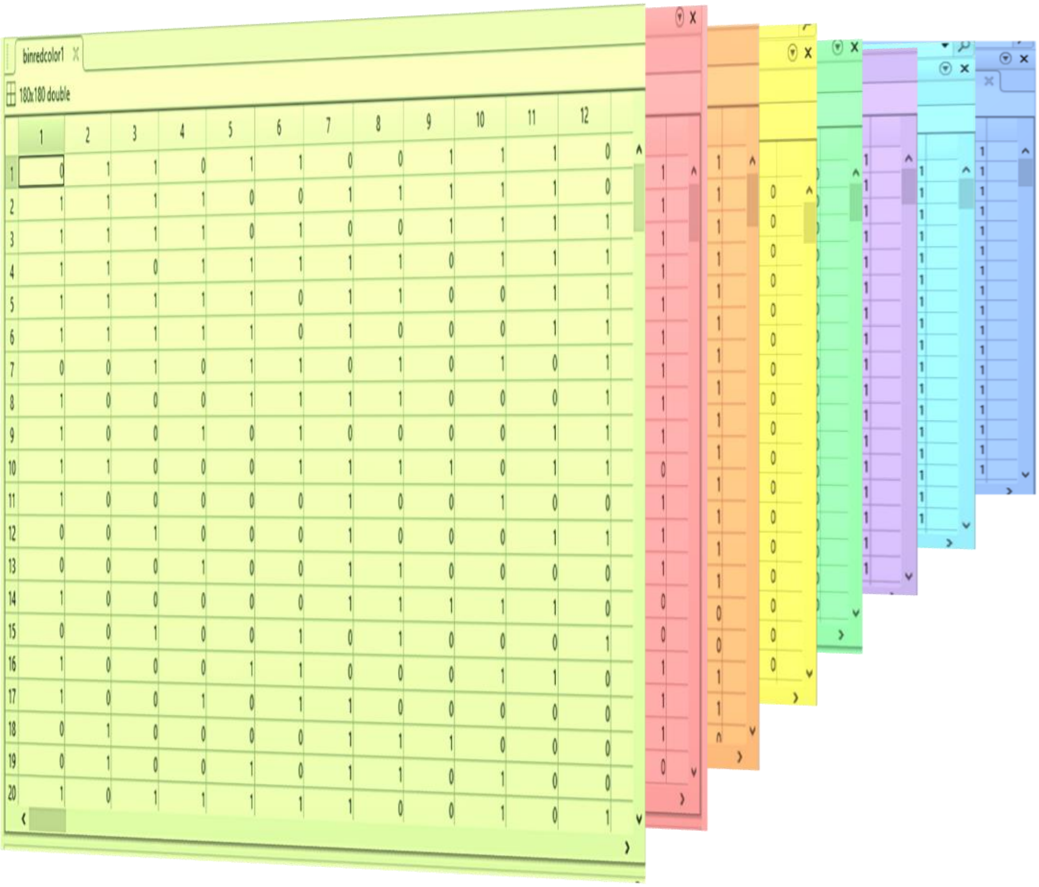
Figure (3.7) Simple sample of the binary representing.

3. Here, the system converts the green color from matrix 180*180 decimal (3.8) to 180*180 *8 binary as in Figures(3.8)& (3.9) respectively and takes the first dimension to access with it.



	1	2	3	4	5	6	7	8	9	10	11	12
1	230	231	231	230	229	231	230	232	231	229	231	230
2	231	231	231	231	230	230	231	231	231	231	229	230
3	231	231	231	231	230	233	232	230	231	231	229	231
4	231	231	230	231	231	231	231	231	230	231	229	231
5	229	229	229	229	229	230	231	231	228	230	231	231
6	231	231	231	231	231	230	231	230	230	230	231	231
7	232	232	231	232	231	231	230	229	230	229	230	231
8	231	232	230	230	231	231	229	231	232	230	232	231
9	231	232	230	231	230	229	230	232	232	230	233	231
10	229	231	230	230	230	229	231	231	231	230	231	229
11	229	230	228	228	230	232	231	230	230	231	230	230
12	232	230	229	230	230	230	231	230	230	230	231	231
13	230	228	228	229	230	230	229	231	232	232	234	230
14	231	230	230	230	232	232	231	231	231	231	233	228
15	232	232	231	230	230	231	230	229	230	230	230	225
16	231	232	230	230	231	229	228	230	230	229	229	226
17	229	230	230	229	230	229	229	230	230	228	230	230
18	228	229	228	228	228	230	231	229	229	232	232	230
19	228	229	228	228	229	230	229	229	230	231	232	224

Figure (3.8): Sample from the values of green color



binredcolor1

180x180 double

	1	2	3	4	5	6	7	8	9	10	11	12
1	0	1	1	0	1	1	0	0	1	1	1	0
2	1	1	1	1	0	0	1	1	1	1	1	0
3	1	1	1	1	0	1	0	0	1	1	1	1
4	1	1	0	1	1	1	1	1	0	1	1	1
5	1	1	1	1	1	0	1	1	0	0	1	1
6	1	1	1	1	1	0	1	0	0	0	1	1
7	0	0	1	0	1	1	0	1	0	1	0	1
8	1	0	0	0	1	1	1	1	0	0	0	1
9	1	0	0	1	0	1	0	0	0	0	1	1
10	1	1	0	0	0	1	1	1	1	0	1	1
11	1	0	0	0	0	0	1	0	0	1	0	0
12	0	0	1	0	0	0	1	0	0	0	1	1
13	0	0	0	1	0	0	1	1	0	0	0	0
14	1	0	0	0	0	0	1	1	1	1	1	0
15	0	0	1	0	0	1	0	1	0	0	0	1
16	1	0	0	0	1	1	0	0	0	1	1	0
17	1	0	0	1	0	1	1	0	0	0	0	0
18	0	1	0	0	0	0	1	1	1	0	0	0
19	0	1	0	0	1	0	1	1	0	1	0	0
20	1	0	1	1	1	1	1	0	0	1	0	1

Figure (3.9) Eight dimensions binary image of green color

The image is read as different pixel data in the Matlab program depending on the image's color, which ranges from white (value 255) to black (value 0). The color gradation of the image is through these two values. The green color chosen in this program contains a set of different pixels from color to show the gradient.

After reading these values in Figure (3.8), turn them to the binary numeric array. This conversion is not like any other, which converts an array from decimal to binary values in the same length and a certain number of bits, such as 8 bits or more or less, depending on the values present. The entire array has converted from a two-dimensional one array

180 * 180 to 8 arrays with two dimensions 180 * 180. These matrices denote in Figure (3.9) use various colors to differentiate them.

The values and placements of the matrices result from the transformation and vary depending on the position of the pixels from which they are changing.

3.2.5 Two Dimension Cubic Spline Interpolation

Piecewise cubic convolution (PCC) introduces picture interpolation in two-dimensional (2-D), non-separable space. PCC has traditionally been implemented using a one-dimensional (1-D) derivation with a two-dimensional separable generalization. However, the traditional method is ineffective because typical situations and imaging systems are indistinguishable.

Using the least-square method and a cubic-spline algorithm, the (2-D) cubic-spline interpolation scheme recalculates the sampled values from the image data. Revisiting the standard 1-D derivation of the separable kernel is helpful to introduce both definitions and notation.

The roots of the 2D-cubic spline interpolation derive from the dimension of the cover image and the length of the patient file information, as shown in table (3.1).

Table (3.1). Control Point Choices for Spline Curve Construction.

Cover image vector	**1**	**988**	**3410**	**8090**
Information(secret)	1	39	150	200

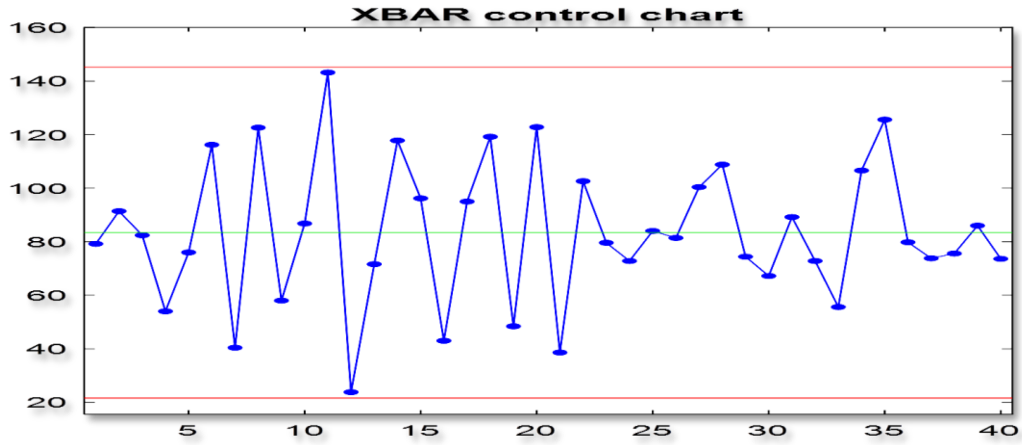
The particular points used in the 2D cubic spline interpolation shown in the table (3.1) are not chosen at random, but rather according to a unique system that relies on determining the length of the image used, which was 180 * 180, as well as determining the size of the data used (the text data to be encoded) and choosing points from the image length and the data length representing primary roots. So that eight roots determine the 2D cubic spline interpolation and its shape, the reasonable possibilities for extracting the roots from among those lengths must devising.

The 2D cubic spline interpolation, whose roots were determined and drawn according to the following equation (3.1), is depicted in Figure(3.10).

$$S(x,y) = \mathrm{S(x)}.\,\mathrm{S(y)}$$

$$= (S_0(x){+}\propto\ S_1(x))(S_0(y){+}\propto\ S_1(y))$$

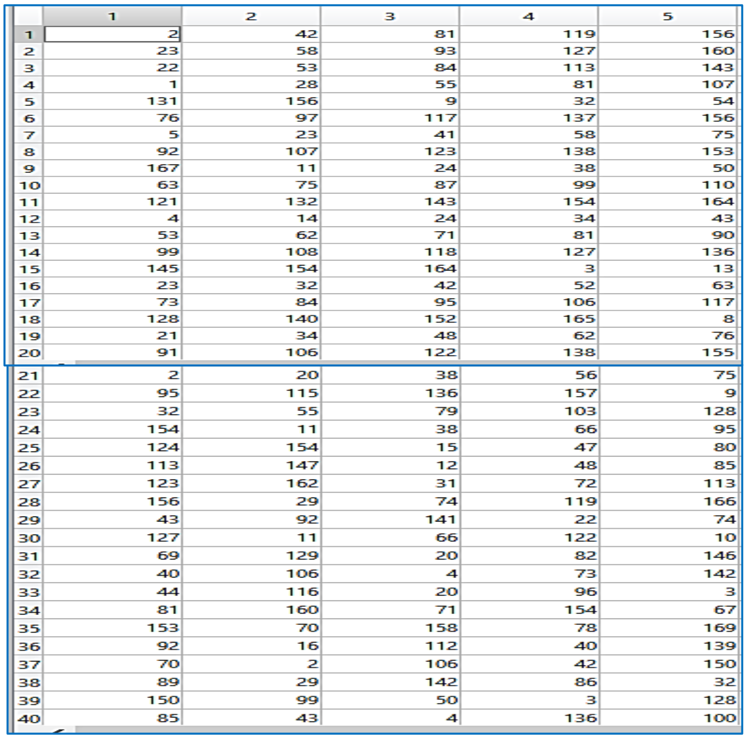
$$= S_0(x)\,S_0(y) +\propto (S_0(x)\,S_1(y) + S_1(x)\,S_0(y)) +\propto^2 S_1(x)\,S_1(y) \quad (3.1)$$



Figure(3.10): The roots of 2D cubic spline interpolation

Selecting the roots, creating the cubic function, and extracting its values are all steps in the process. According to the proposed program, these values were taken and transformed to precise spots in the previously acquired and specified cover image. The 2D cubic spline interpolation values are adjusted to include all of the image's positions. The method for doing so is determined by the size of the cover picture that has been applied and the number of binary data required to encode the bits through it. The highest image length value regards 170 instead of 180, where the remaining ten values hiding the data.

As a result, MOD 170 is chosen as the primary root of the cubic spline interpolation values, resulting in a two-dimensional array with values containing all of the data encoded, as shown in Figure(3.11).



	1	2	3	4	5
1	2	42	81	119	156
2	23	58	93	127	160
3	22	53	84	113	143
4	1	28	55	81	107
5	131	156	9	32	54
6	76	97	117	137	156
7	5	23	41	58	75
8	92	107	123	138	153
9	167	11	24	38	50
10	63	75	87	99	110
11	121	132	143	154	164
12	4	14	24	34	43
13	53	62	71	81	90
14	99	108	118	127	136
15	145	154	164	3	13
16	23	32	42	52	63
17	73	84	95	106	117
18	128	140	152	165	8
19	21	34	48	62	76
20	91	106	122	138	155
21	2	20	38	56	75
22	95	115	136	157	9
23	32	55	79	103	128
24	154	11	38	66	95
25	124	154	15	47	80
26	113	147	12	48	85
27	123	162	31	72	113
28	156	29	74	119	166
29	43	92	141	22	74
30	127	11	66	122	10
31	69	129	20	82	146
32	40	106	4	73	142
33	44	116	20	96	3
34	81	160	71	154	67
35	153	70	158	78	169
36	92	16	112	40	139
37	70	2	106	42	150
38	89	29	142	86	32
39	150	99	50	3	128
40	85	43	4	136	100

Figure(3.11): Location matrix of 2D-cubic spline interpolation

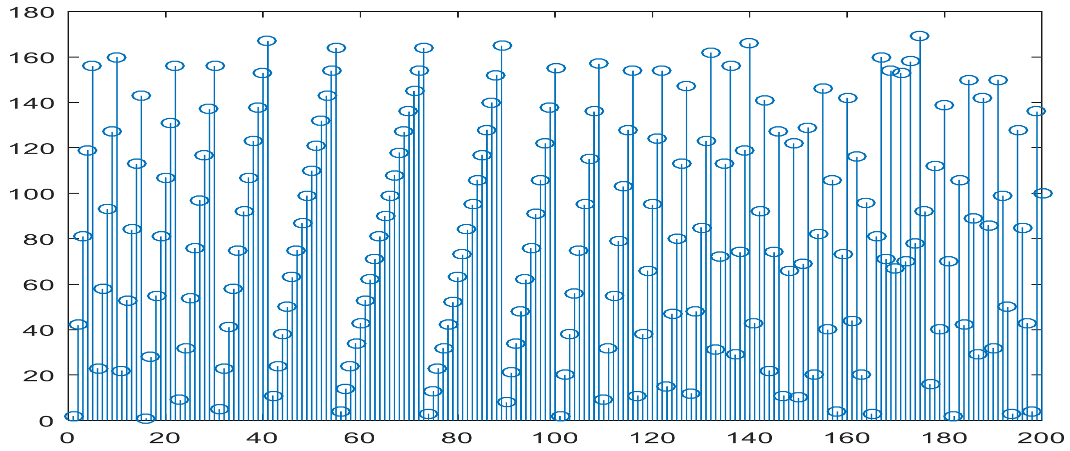


Figure (3.12): The diagram of the 2D-cubic spline interpolation values

One of the specifications of these resulting values is that the decimal value is not repeating during one row of the matrix; the matrix here is the first matrix selected from the eight matrices that resulted from converting the green color into binary data. For more focusing on the value of the location, Figure (3.12) can explain all matters with the cover image height and width of patient file length.

3.2.6 Chaotic Encryption Technology (Logistic Map)

When a chaotic system behaves, it is characterized by the following characteristics: In normal circumstances, the loss of connectivity points between one group and its condition cannot be anticipated. Finally, it is very reliant on the initial starting position. Even if a pair of chaotic appliances start with identical states, they will quickly develop into totally different systems if their starting points are slightly different.

The majority of chaotic encryption technology investigations are now based on one and two dimensions. According to several studies, low-dimension secrecy is insufficient. Many low-dimensional chaotic encryption solutions have been developed in recent years, but they all have some level of secrecy flaws. It is widely assumed that many contemporary chaotic encryption techniques contain security flaws.

(1) Improved security may be achieved via the use of the following strategies. Using quasi-chaotic sequences, you may create sequences with a longer duration. Consequently, to build a robust chaotic encryption system, it is necessary to establish a multi-dimensional chaotic cryptography system. To develop a high-quality chaotic encryption system, the design of "high-quality chaotic" arrangements is essential.

(2) To encrypt an image step by step, you may combine the pixel cryptographic algorithm with a pixel position encryption approach to encrypt a picture in stages. This encryption technique is suited for usage in scenarios with higher security requirements due to its superior security performance. Because the encryption process scrambles both image pixel positions and pixel values, decrypting a cipher becomes much more difficult, improving security.

(3) Combine the methods of encryption with data concealment. Image encryption methods have advanced significantly in recent years, and a range of attacks against encrypted photos have emerged in the meantime. Encrypting a picture and transmitting the resultant unidentifiable image are two examples of image manipulation. Across the internet may inadvertently reveal the image's value, increasing the likelihood of hostile

assaults. Transfer of the photograph over the internet will be significantly safer when paired with data concealing techniques.

There are many well-known chaotic maps. The logistic map is one of the most straightforward and visible systems for displaying order to chaos transition.

Referring to the logistic equation that is used in this program as in equation (3.2), noting that it is necessary to choose the basic root *r* and the starting initial value x_iI.e., the zero value, to generate a chaotic situation.

$$x_{i+1} = rx_i(1 - \mathrm{x_i}) \qquad (3.2)$$

The values are chosen as r=4, and the initial value x_0 =0.94281. The bifurcation of the logistic map is shown in Figure (3.13).

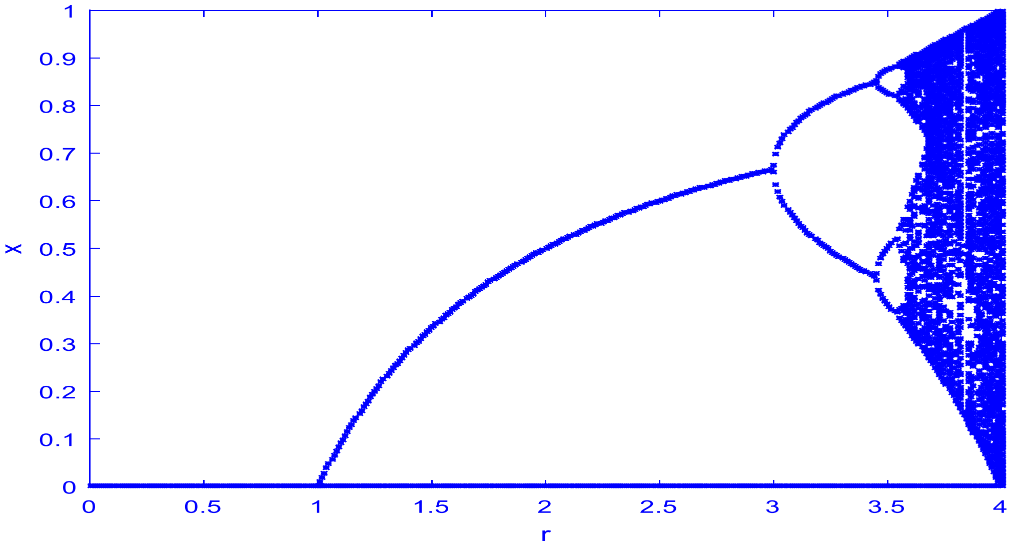


Figure (3.13): The bifurcation of the logistic map.

The purpose of generating the logistic function is to encode the entered information (patient information), so the length of this function was chosen equal to the length of the patient's data. It considers the amount of an inevitable increase that could happen due to the different lengths of the entered information according to its types. The assumed primitiveness value from this map is drawn as in Figure(3.14).

Logistic map matrix= [22 68 88 44 98 6 23 72
81 62 94 21 67 88 42 98 9 34 89
38 94 21 66 89 39 95 20 64 92 28
80 63 93 27 79 67 88 42 98 10 35
91 34 89 39 95 19 62 94 21 66 89
39 95 19 63 94 24 73 79 67 88 42]

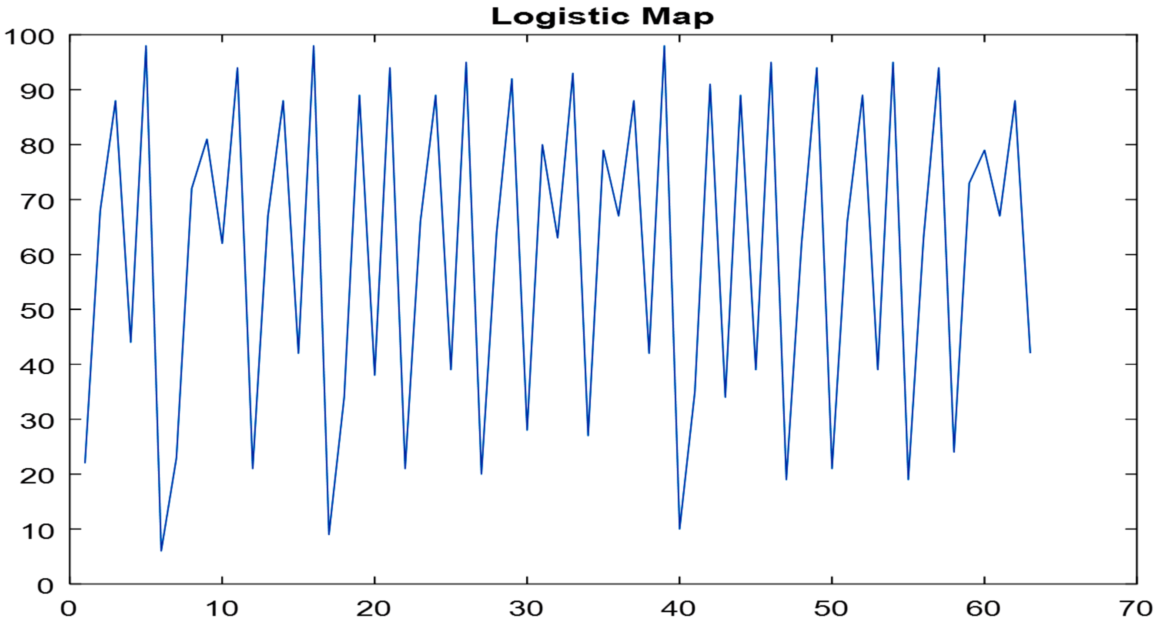


Figure (3.14): The results values of the logistic map.

3.2.7 Patient File Information

The secret information is encrypted in the cover image related to the patient. All the information that is needed to protect and save the privacy of the patient such as patient mother name, age, weight, patient number, blood pressure, blood type, Respiratory rate, length, Statistical number, and name of the surgeon are entered as texts under a file named the patient file. Figure (3.15) shows a sample of this information in the patient file.

Patient File
Patient number: 100
name: Heba Abdul-Jaleel
age:32
blood pressure: 120/80.
Blood type:+O
Respiratory rate:normal
weight: 68
Length: 160
Statistical number: 11
Name surgeon: Dr. Suham Ahmed

Figure (3.15): The encrypted text for the same person in the cover image

All this information is read in MatLab as ASCII code and converted to the strings values (numbers) as shown in Figure (3.16). So as easily treated and encrypted in the logistic map to provide the required security for the patient's information and finally converted to the binary digits so as encrypted in the selected sites from the cubic spline interpolation.

```
Patient File=[49   48   48   32   104  101  98   97   32
97   98   100  117  108  45   106  97   108  101  101
108  32   51   51   32   49   50   48   47   56   48
32    43    111   32    56    56    32    55    48    32    49
54    48    32    49    49    32    100   114   46    115   117
104   97    109   32    97    104   109   101   100   32]
```

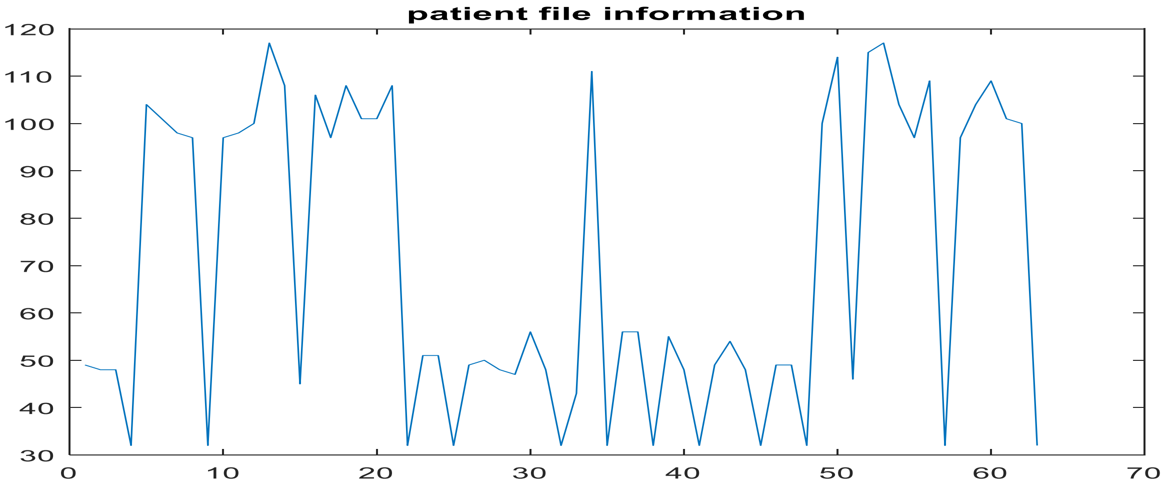


Figure (3.16): The patient file information

3.2.8 The Encryption Algorithm

Many academics presented several picture encryption techniques based on chaotic theories, employing chaotic systems capable of generating enormous, Chaotic sequences that are not linked to one another, seem like noise, and the recyclable sequences of this kind are impossible to reverse. Model or forecast making them even more challenging to crack.

One of the basic assumptions for any picture encryption system is that there is no such thing as 100% security. In most cases, a system for encrypting data is considered secure if the costs of fracturing a particular encryption technique surpass the price of data encryption. If the time spent cracking a specific algorithm exceeds the data confidentiality period, that algorithm can also be considered secure. Furthermore, if the amount of data required to crack an algorithm is more significant than that required to crack a secret key encryption method, the algorithm is considered secure.

A few aspects of the image should be addressed before encrypting it, high data density, considerable redundancy, and high pixels correlated. As a result, The following principles should be followed while developing an algorithm. The encryption method should use the most fundamental operation type that is feasible. Because a picture includes a large amount of data, it is called a data image; encrypting it with a complicated technique will be computationally expensive. A designer should also use a parallel processing approach when considering encryption time. The pixels of an image should be jumbled to create more significant encryption effects. It is preferable to employ an encryption solution that combines compression and encryption to provide more image redundancy.

The process of encryption algorithms can be divided into three algorithms the first algorithm for encrypted the patient file information in the logistic map to produce the secure patient file information and the second part for encrypting the secure patient file information the specific locations of the eighth dimension of binary green color matrices, and finally the algorithm for encrypting the length of the patient file in the green color.

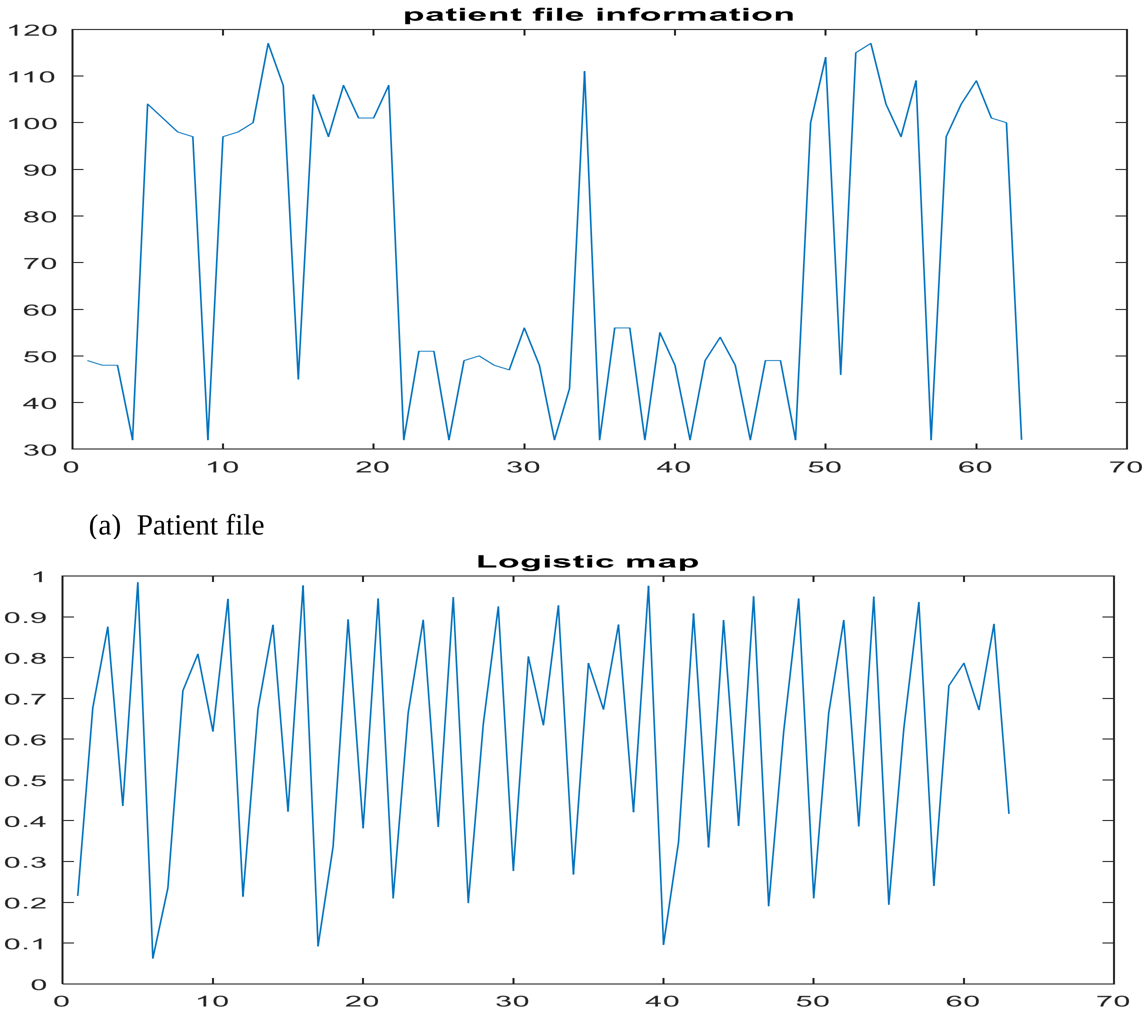
Algorithm1: encrypted the patient file information in the logistic map. The matrix result from converting the ASCII code to the numbers

are added to the matrix of the logistic map matrix after rounding it and converting to the integer values as in the steps bellow:

Secure patient file= [22 68 88 44 98 6 23 72
81 62 94 21 67 88 42 98 9 34 89
38 94 21 66 89 39 95 20 64 92 28
80 63 93 27 79 67 88 42 98 10 35
91 34 89 39 95 19 62 94 21 66 89
39 95 19 63 94 24 73 79 67 88
42]+
[49 48 48 32 104 101 98 97 32 97 98
100 117 108 45 106 97 108 101 101 108 32
51 51 32 49 50 48 47 56 48 32 43
111 32 56 56 32 55 48 32 49 54 48
32 49 49 32 100 114 46 115 117 104 97
109 32 97 104 109 101 100 32]

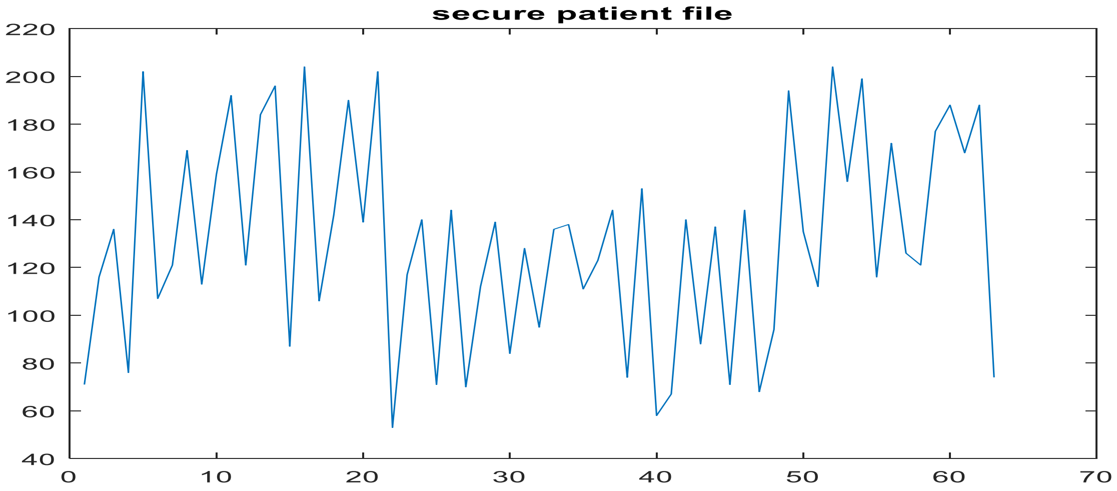
Secure patient file= [71 116 136 76 202 107 121 169
113 159 192 121 184 196 87 204 106 142 190
139 202 53 117 140 71 144 70 112 139 84
128 95 136 138 111 123 144 74 153 58 67
140 88 137 71 144 68 94 194 135 112 204
156 199 116 172 126 121 177 188 168 188 74]

All values of the patient file are changed to another value because of the wide variation of the logistic map values. The representing of the patient file matrix are shown in Figure(3.17a), the logistic map matrix shown in Figure(3.17b), and the encryption result secure patient file is shown in Figure(3.17c), which is the result from the combination of figures (3.16) and (3.14) to represent the first encryption algorithm



(a) Patient file

(b) logistic map

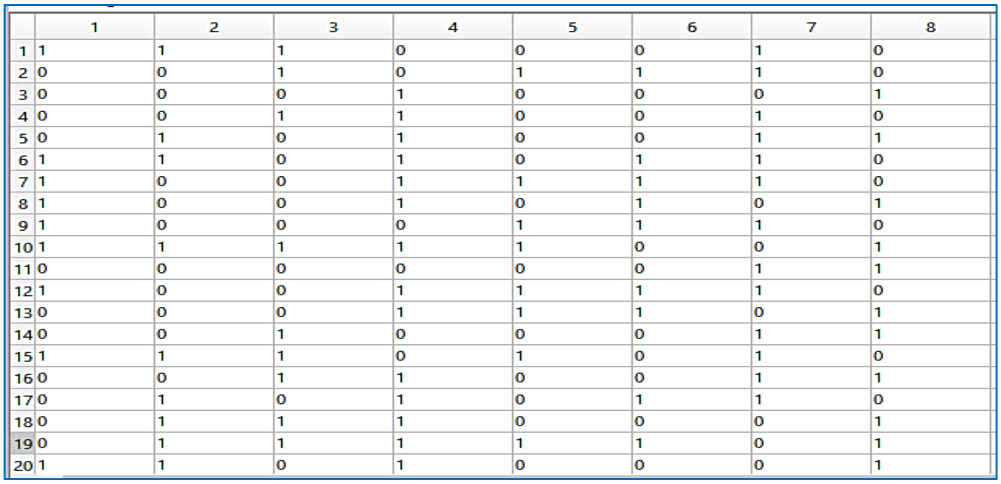


(c) Secure Patient file

Figure (3.17) :The first encryption between patient file and logistic map

Algorithm 2: the second encryption algorithm is related to encrypting the secure patient file with the cover image.

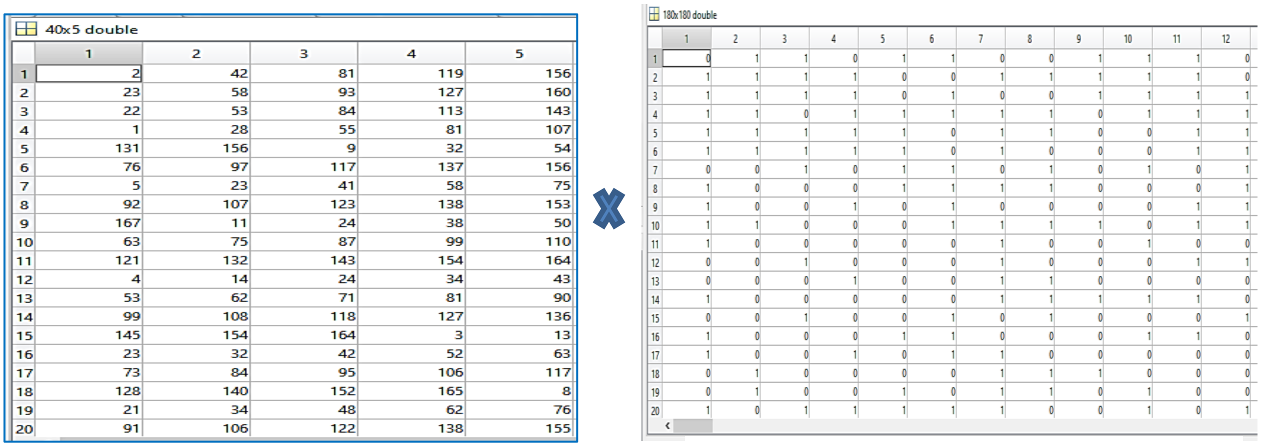
All information of the secure patient file is converted to binary values with eight bits for each symbol (byte). Note that this length (eight bits) varies according to the values of information. Still, here, the length has been identified and restricted in the MOD(170) as taking in the logistic map steps, so the lengths are limited in eight bits as result matrix of n*8 dimension shown in figure (3.18), where n is the length of patinent file.



	1	2	3	4	5	6	7	8
1	1	1	1	0	0	0	1	0
2	0	0	1	0	1	1	1	0
3	0	0	0	1	0	0	0	1
4	0	0	1	1	0	0	1	0
5	0	1	0	1	0	0	1	1
6	1	1	0	1	0	1	1	0
7	1	0	0	1	1	1	1	0
8	1	0	0	1	0	1	0	1
9	1	0	0	0	1	1	1	0
10	1	1	1	1	1	0	0	1
11	0	0	0	0	0	0	1	1
12	1	0	0	1	1	1	1	0
13	0	0	0	1	1	1	0	1
14	0	0	1	0	0	0	1	1
15	1	1	1	0	1	0	1	0
16	0	0	1	1	0	0	1	1
17	0	1	0	1	0	1	1	0
18	0	1	1	1	0	0	0	1
19	0	1	1	1	1	1	0	1
20	1	1	0	1	0	0	0	1

Figure (3.18): Sample of the binary values of the secure patient file

After the conversion of the patient file to the binary, applying the location matrix result from 2D cubic spline matrix Figure (3.19a) on the first dimension of the binary green color Figure (3.19b) (first dimension from initially eight dimensions). Figure (3.19) show the sample of these two matrices.



40x5 double

	1	2	3	4	5
1	2	42	81	119	156
2	23	58	93	127	160
3	22	53	84	113	143
4	1	28	55	81	107
5	131	156	9	32	54
6	76	97	117	137	156
7	5	23	41	58	75
8	92	107	123	138	153
9	167	11	24	38	50
10	63	75	87	99	110
11	121	132	143	154	164
12	4	14	24	34	43
13	53	62	71	81	90
14	99	108	118	127	136
15	145	154	164	3	13
16	23	32	42	52	63
17	73	84	95	106	117
18	128	140	152	165	8
19	21	34	48	62	76
20	91	106	122	138	155

180x180 double

	1	2	3	4	5	6	7	8	9	10	11	12
1	0	1	1	0	1	1	0	0	1	1	1	0
2	1	1	1	1	0	0	1	1	1	1	1	0
3	1	1	1	1	0	1	0	0	1	1	1	1
4	1	1	0	1	1	1	1	1	0	1	1	1
5	1	1	1	1	1	0	1	1	0	0	1	1
6	1	1	1	1	1	0	1	0	0	0	1	1
7	0	0	1	0	1	1	0	1	0	1	0	1
8	1	0	0	0	1	1	1	1	0	0	0	1
9	1	0	0	1	0	1	0	0	0	0	1	1
10	1	1	0	0	0	1	1	1	1	0	1	1
11	1	0	0	0	0	0	1	0	0	1	0	0
12	0	0	1	0	0	0	1	0	0	0	1	1
13	0	0	0	1	0	0	1	1	0	0	0	0
14	1	0	0	0	0	0	1	1	1	1	1	0
15	0	0	1	0	0	1	0	1	0	0	0	1
16	1	0	0	0	1	1	0	0	0	1	1	0
17	1	0	0	1	0	1	1	0	0	0	0	0
18	0	1	0	0	0	0	1	1	1	0	0	0
19	0	1	0	0	1	0	1	1	0	1	0	0
20	1	0	1	1	1	1	1	0	0	1	0	1

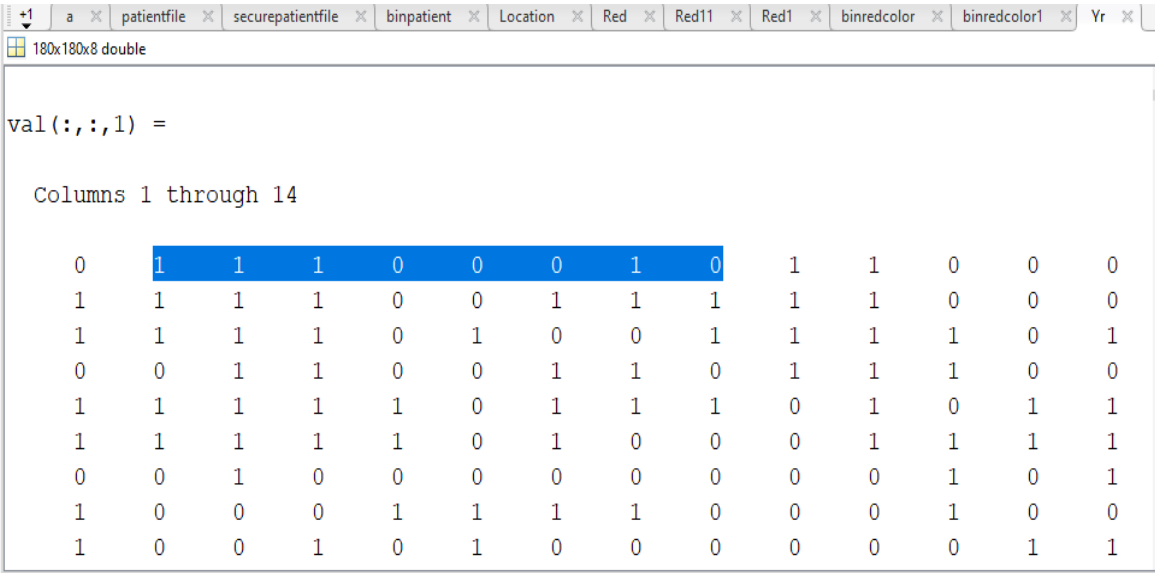
b) 2D cubic spline matrix

a) First dimension matrix

Figure (3.19) Sample of two matrices: a) 2D cubic spline matrix and b) First dimension matrix

The process of using the 2D cubic spline to locate the position of encrypting in the green cover matrix is as follows: the first value of location has "2" from the Figure (3.19a), this value means the second position in the first row from the Figure (3.19b) of the green cover matrix is selecting, So this bit in this position and seventh bits after it is using to hide the **"first byte"** of the binary secure patient file from the Figure (3.19). These seventh positions are from the first matrix and all eight matrices of the binary green color to say the z plane operation.

The hiding process uses the least significant bit method, where every bit of the binary patient file is replaced with the last bit of z- plain matrices of the binary green color. The result of the hiding operation shows that the patient bits are arranged in the same manner as in the binary patient file bits. Figure (3.20) show the result of the hiding step for one byte as a sample of operation, where the shadow blue color represents the first byte of patient file information.



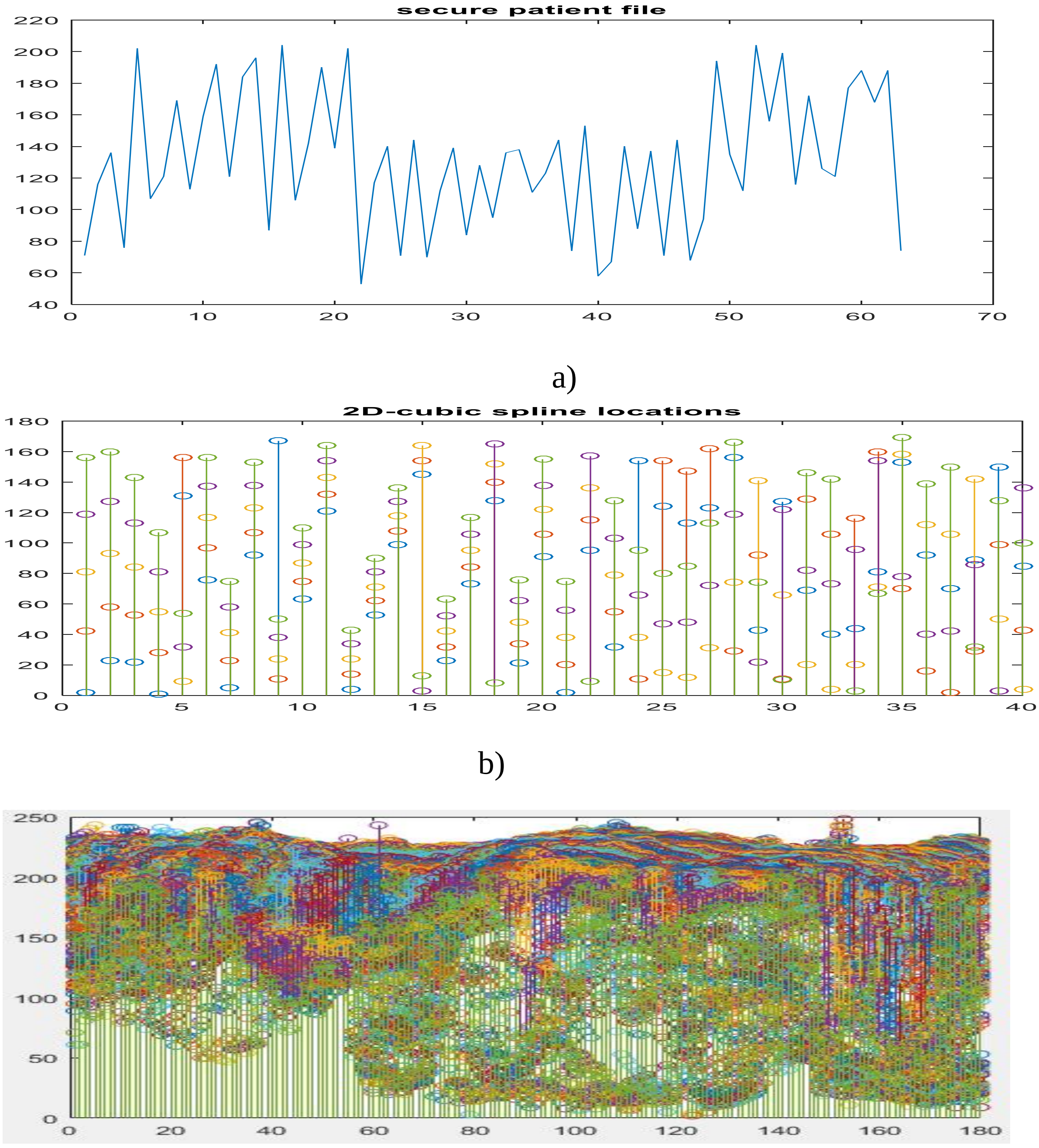
```
val(:,:,1) =

  Columns 1 through 14

     0     1     1     1     0     0     0     1     0     1     1     0     0     0
     1     1     1     1     0     0     1     1     1     1     1     0     0     0
     1     1     1     1     0     1     0     0     1     1     1     1     0     1
     0     0     1     1     0     0     1     1     0     1     1     1     0     0
     1     1     1     1     1     0     1     1     1     0     1     0     1     1
     1     1     1     1     1     0     1     0     0     0     1     1     1     1
     0     0     1     0     0     0     0     0     0     0     0     1     0     1
     1     0     0     0     1     1     1     1     0     0     0     1     0     0
     1     0     0     1     0     1     0     0     0     0     0     0     1     1
```

Figure (3.20): First byte of patient file information in the green color

Here, Figure (3.21) below can summarize the second encryption algorithm



a)

b)

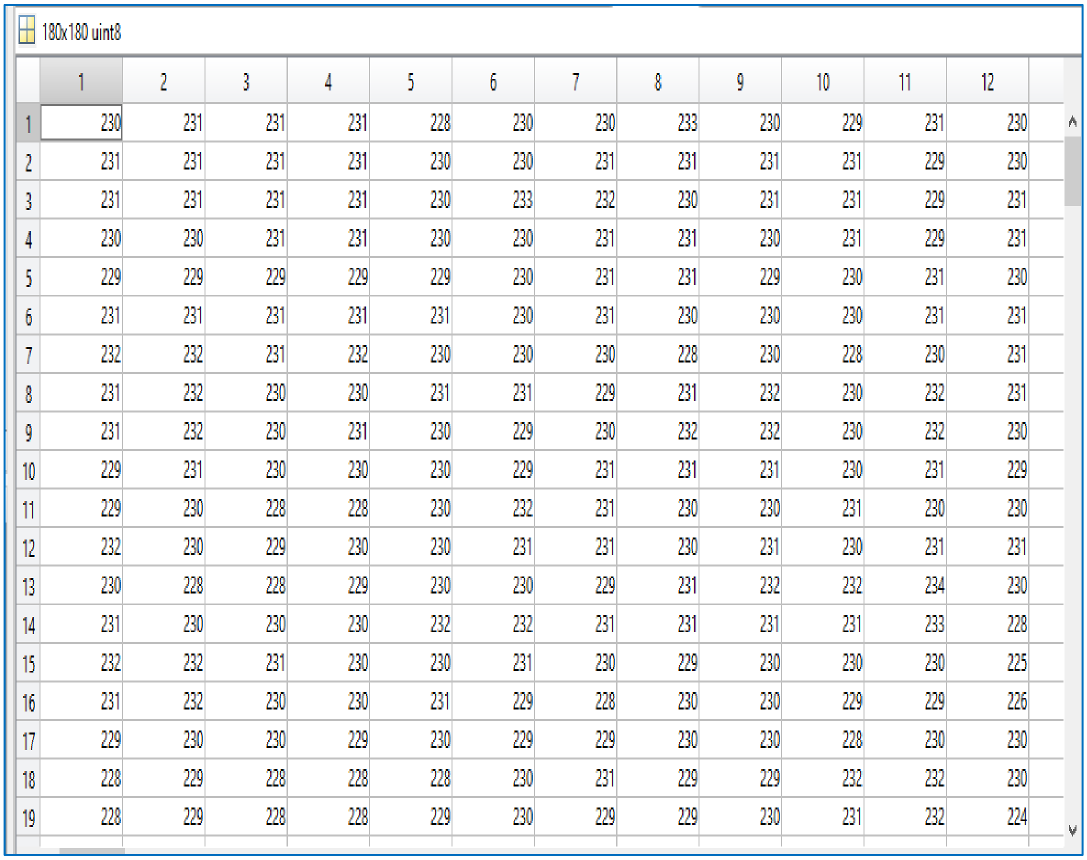
c)

Figure (3.21): The second encryption steps between patient file and logistic map a) secure patient file b) locations of cover image c) Hiding in the red of cover image

Algorithm3: in this algorithm, the length of patient file information is converted to binary and hidden in the red color of the image after converting it to binary. The process of hiding is the same that used in algorithm2 which is the least significant bit

3.2.9 Reconstructed The Cover Image

The green color is constructed from binary by converting the bytes to decimal values, as in figure (3.22). After encrypting the desired information of the patient file in the green color, the green color becomes the steganography plain. It contains all the desired information that need to protect them and hide from unauthorized people.



180x180 uint8

	1	2	3	4	5	6	7	8	9	10	11	12
1	230	231	231	231	228	230	230	233	230	229	231	230
2	231	231	231	231	230	230	231	231	231	231	229	230
3	231	231	231	231	230	233	232	230	231	231	229	231
4	230	230	231	231	230	230	231	231	230	231	229	231
5	229	229	229	229	229	230	231	231	229	230	231	230
6	231	231	231	231	231	230	231	230	230	230	231	231
7	232	232	231	232	230	230	230	228	230	228	230	231
8	231	232	230	230	231	231	229	231	232	230	232	231
9	231	232	230	231	230	229	230	232	232	230	232	230
10	229	231	230	230	230	229	231	231	231	230	231	229
11	229	230	228	228	230	232	231	230	230	231	230	230
12	232	230	229	230	230	231	231	230	231	230	231	231
13	230	228	228	229	230	230	229	231	232	232	234	230
14	231	230	230	230	232	232	231	231	231	231	233	228
15	232	232	231	230	230	231	230	229	230	230	230	225
16	231	232	230	230	231	229	228	230	230	229	229	226
17	229	230	230	229	230	229	229	230	230	228	230	230
18	228	229	228	228	228	230	231	229	229	232	232	230
19	228	229	228	228	229	230	229	229	230	231	232	224

Figure (3.22): Sample from the green color matrix after constructing it

And finally, construct the color cover image with three-dimension in Figure (3.23), where the cover image is saved and ready to upload to the database.

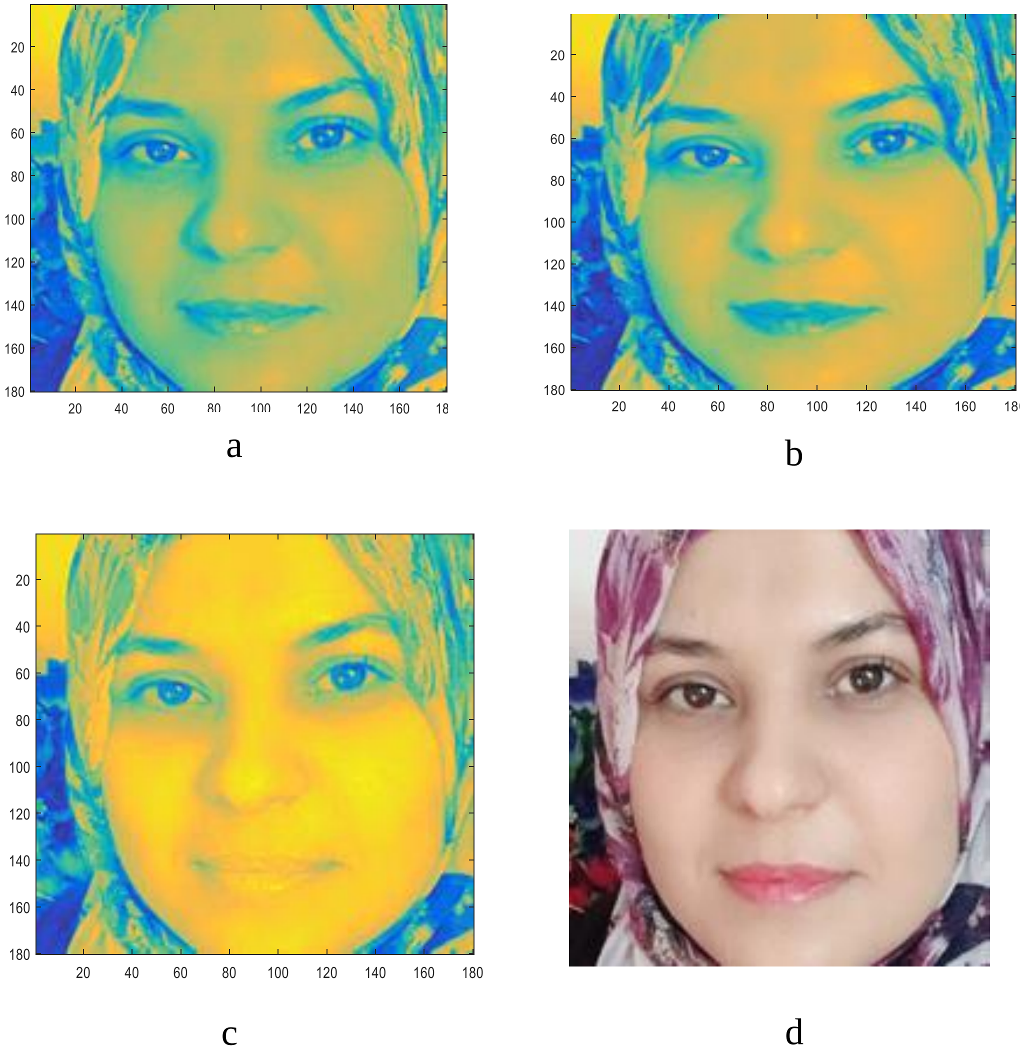


figure (3.23): Reconstructed the cover Image steps a) blue color b)encrypt green c) encrypt red d) encrypt the cover image

3.2.10GUI of Encryption Subsystem

The program will do all the encryption requirements internally and give the final image that contains the encrypted information. All the steps mentioned previously of the encryption subsystem are converted to the graphical user interface to facilitate the work on the encoder and give the result quickly, as shown in Figure (3.24), Which only asks to enter the patient's information to encrypt it. The essential buttons in this GUI after entering the information are:

Patient image: to choose the patient image from desired folder or camera.

Save: to execute the encrypting algorithms.

Reset: to delete the current information for a new operation.

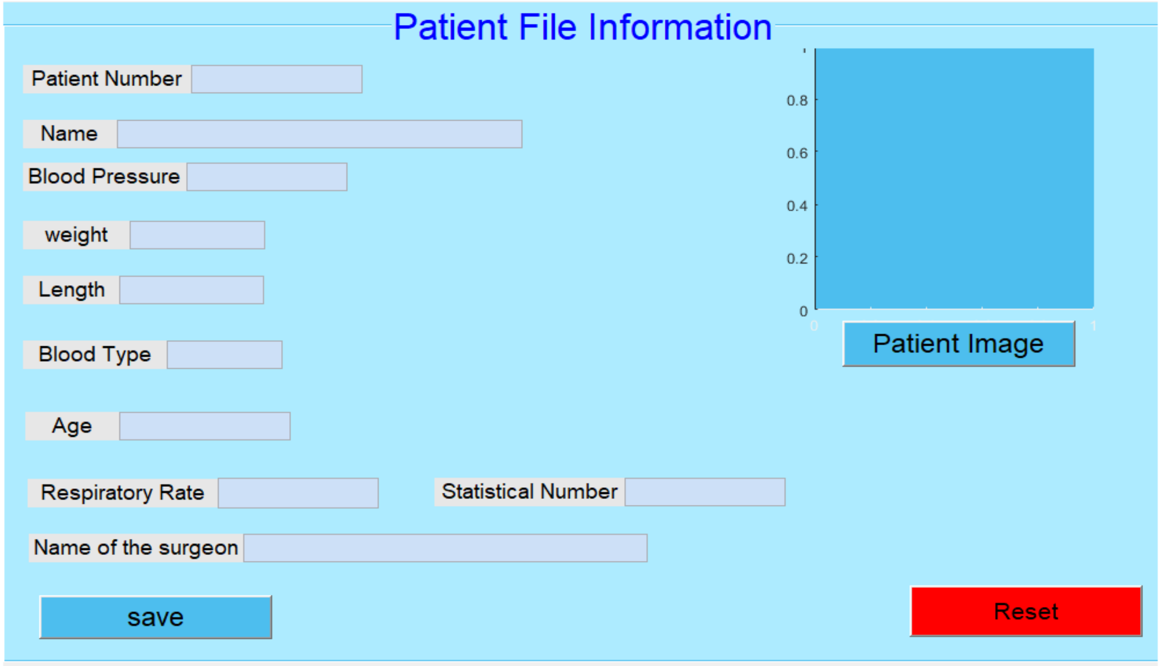


Figure (3.24): GUI of Encryption Subsystem

3.2.11 Clouding And Data-Based Subsystem(Web Design)

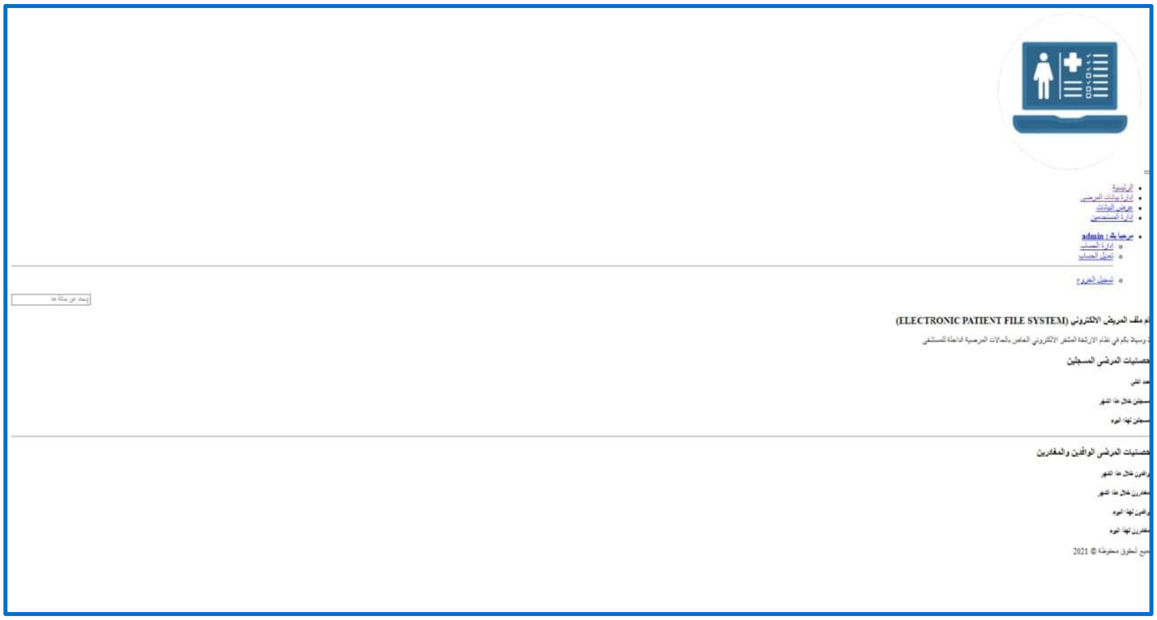
The idea of cloud computing is storing data and information away from our physical location and accessing it via the internet. Thus the data and information are not bound to any area. How did a straightforward explanation become known as "cloud computing"? as discussed in the previous chapter, clouds can be seen somewhere in the sky, regardless of the geographical position. Data and information are available whenever connected to the internet, regardless of location.

After completing the encryption process, the images are uploaded via the internet to store them in the cloud and make a database for it to give the ability to reach and access them (the patient information) from any place but not for everyone.

The design of this web is divided into two parts. The first part is related to web page designing, which is the interfacing of the information to the users. The second part is related to the database part. In the first part, different languages are used for building it, such as:

1. HyperText Markup Language(HTML): This describes the web page's structure, headings, and paragraphs, as shown in figure (3.25).

2. Cascading Style Sheets(CSS): It is the language assistant for coordinating the Internet page, arranging colors, fonts, images, and page shape, as shown in figure (3.26).



- الرئيسية
- ادارة بيانات المرضى
- عرض البيانات
- ادارة المستخدمين
- مرحبا بك : admin
  - ادارة الحساب
  - تعديل الحساب
  - تسجيل الخروج

ابحث عن حالة هنا

ام ملف المريض الالكتروني (ELECTRONIC PATIENT FILE SYSTEM)

 وسهلا بكم في نظام الارشفة المشفر الالكتروني الخاص بالحالات المرضية الداخلة للمستشفى

حصئيات المرضى المسجلين

عدد الكلي

مسجلين خلال هذا الشهر

مسجلين لهذا اليوم

حصئيات المرضى الوافدين والمغادرين

وافدين خلال هذا الشهر

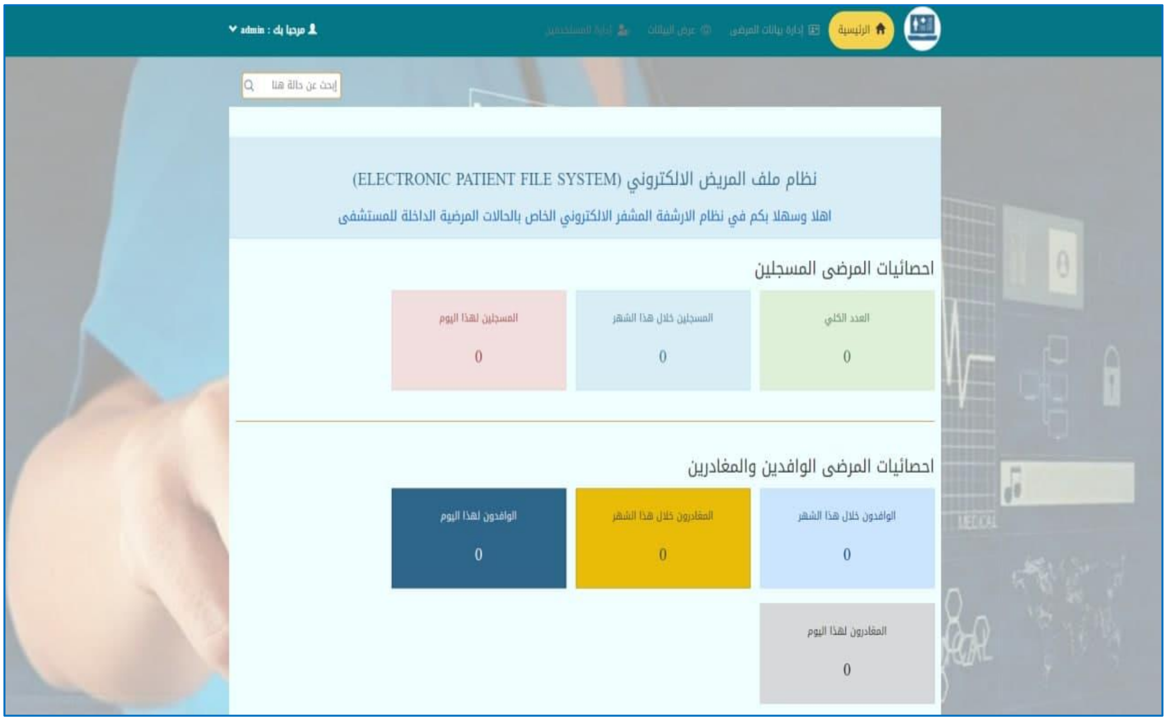
مغادرين خلال هذا الشهر

وافدين لهذا اليوم

مغادرين لهذا اليوم

جميع الحقوق محفوظة © 2021

Figure (3.25): The Web page design using HTML only



إبحث عن حالة هنا

نظام ملف المريض الالكتروني (ELECTRONIC PATIENT FILE SYSTEM)

اهلا وسهلا بكم في نظام الارشفة المشفر الالكتروني الخاص بالحالات المرضية الداخلة للمستشفى

احصائيات المرضى المسجلين

العدد الكلي	المسجلين خلال هذا الشهر	المسجلين لهذا اليوم
0	0	0

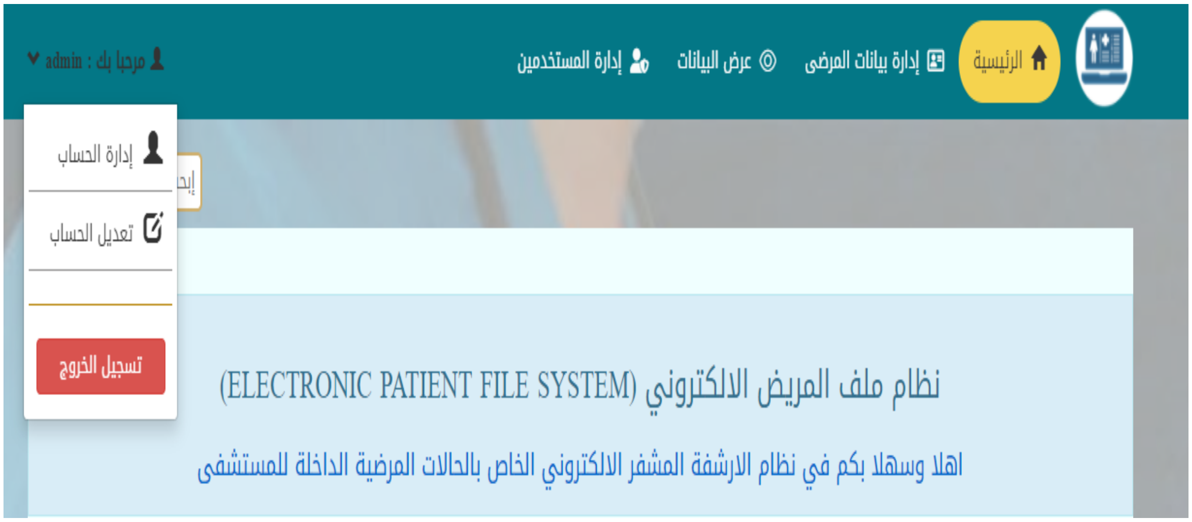
احصائيات المرضى الوافدين والمغادرين

الوافدون خلال هذا الشهر	المغادرون خلال هذا الشهر	الوافدون لهذا اليوم
0	0	0

المغادرون لهذا اليوم
0

Figure (3.26): The Web page design using HTML and CSS.

3. Javascript for page designing: to add different layouts and comments to the site, such as sliding menus as shown in figure(3.27).



نظام ملف المريض الالكتروني (ELECTRONIC PATIENT FILE SYSTEM)

اهلا وسهلا بكم في نظام الارشفة المشفر الالكتروني الخاص بالحالات المرضية الداخلة للمستشفى

figure(3.27): The design using Javascript for page.

4. Model View Controller (MVC): to create a highly efficient web page where:

a - It gives the ability to display and enter data and configure the user interface

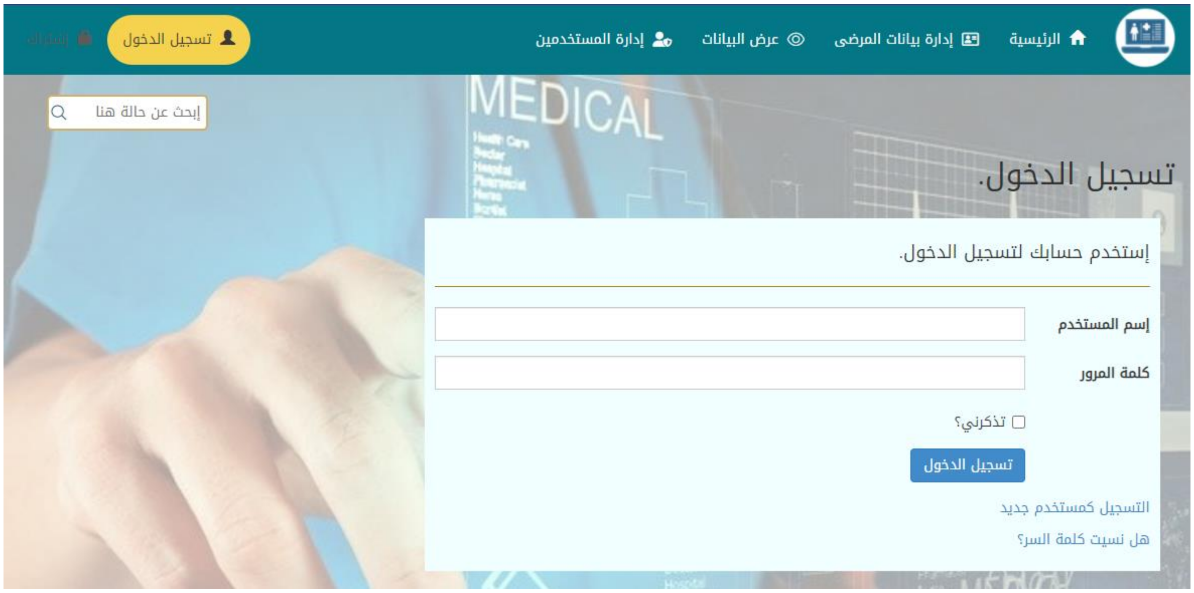
b- Giving the control unit to enter data, process it, or read it from the database, controlling sessions, links, and others.

C- Giving the form for the database that deals with the presentation directly or controls entering data directly. It consists of several classes built using a language. For more details, see Appendix A.

In the second part, Databases are built using Structured Query Language (SQL). Each table in a relational database has a required field that uniquely identifies each row. These key fields can be used to link two tables of information together.

The whole system of clouding interfacing is shown in figure (3.28), where the cover images are uploaded after the steganography process is complete.

Suppose the user is the owner-manager or responsible for the page or a data entry or familiar with it. In that case, When entering the page, the program asks for a user name and password, as shown in figure (3.28), so it is not possible to enter anyone who is not authorized to enter and the type of this user. Therefore, each type of these users is determined, as each person has points of tolerance that differ from the other.



تسجيل الدخول.

إستخدم حسابك لتسجيل الدخول.

إسم المستخدم

كلمة المرور

□ تذكرني؟

تسجيل الدخول

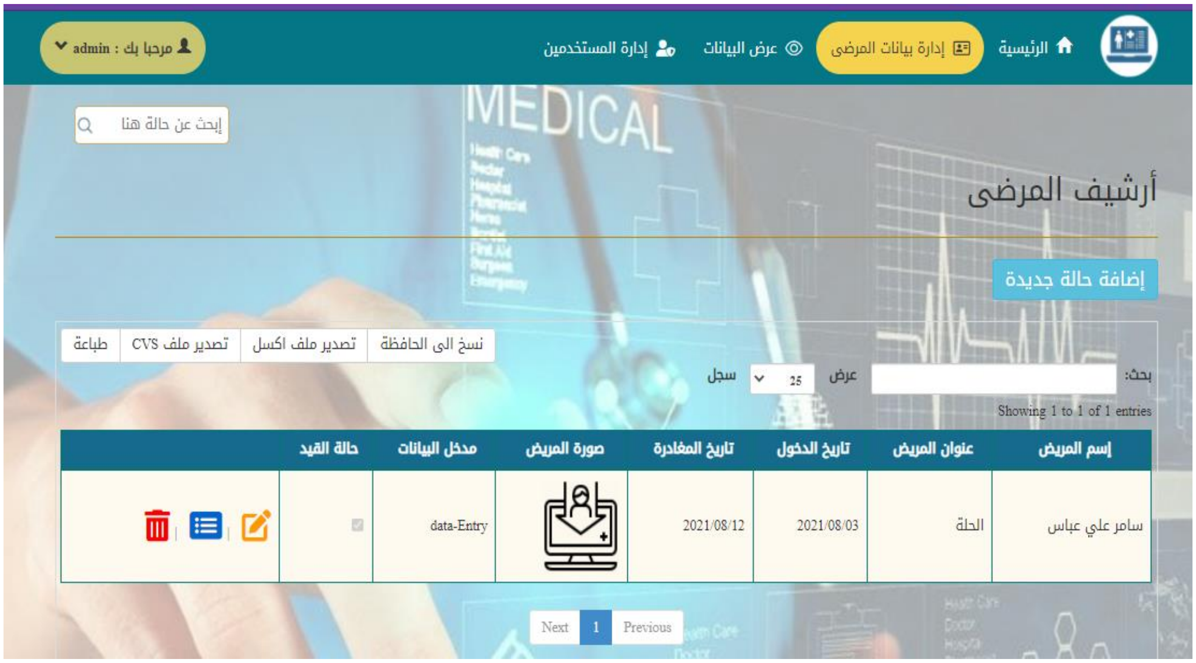
التسجيل كمستخدم جديد

هل نسيت كلمة السر؟

Figure(3.28): Web page design

Figure (3.26) page contains several menus in the address bar. The first list is the main page list that displays the welcome message with statistics such as the statistics of registered patients in terms of the total number, the number of registered persons for this month, the number of those registered for this day, and the statistics of arrivals and departures for the month.

In the list of patient data management (second list), there is the archive for patients, where it contains searches, additions, a display of the existing record according to the numbers, and the current list is exported to a file for printing or saving or to an excel sheet file, followed by the patient table that contains information such as the patient's name, profile picture, patient address and date his entry and exit from the hospital, the name of the data entry, the control of information in terms of scanning or modification and content restriction as in the Figure (3.29). In this list, all the information entered or edited is protected. It has a specific authority, as it is by the data entry only and the main administrator on the page, and no one who does not have this authority is allowed to access or change it.



أرشيف المرضى

بحث: عرض 25 سجل

Showing 1 to 1 of 1 entries

إسم المريض	عنوان المريض	تاريخ الدخول	تاريخ المغادرة	صورة المريض	مدخل البيانات	حالة القيد	
سامر علي عباس	الحلة	2021/08/03	2021/08/12		data-Entry	☑	

Figure (3.29): Patient data management list page

When clicking on Add a new case, the window related to entering the required data will appear, such as name, date of entry and departure, loading the encrypted personal picture, and saving the data in the database, as shown in figure(3.30).

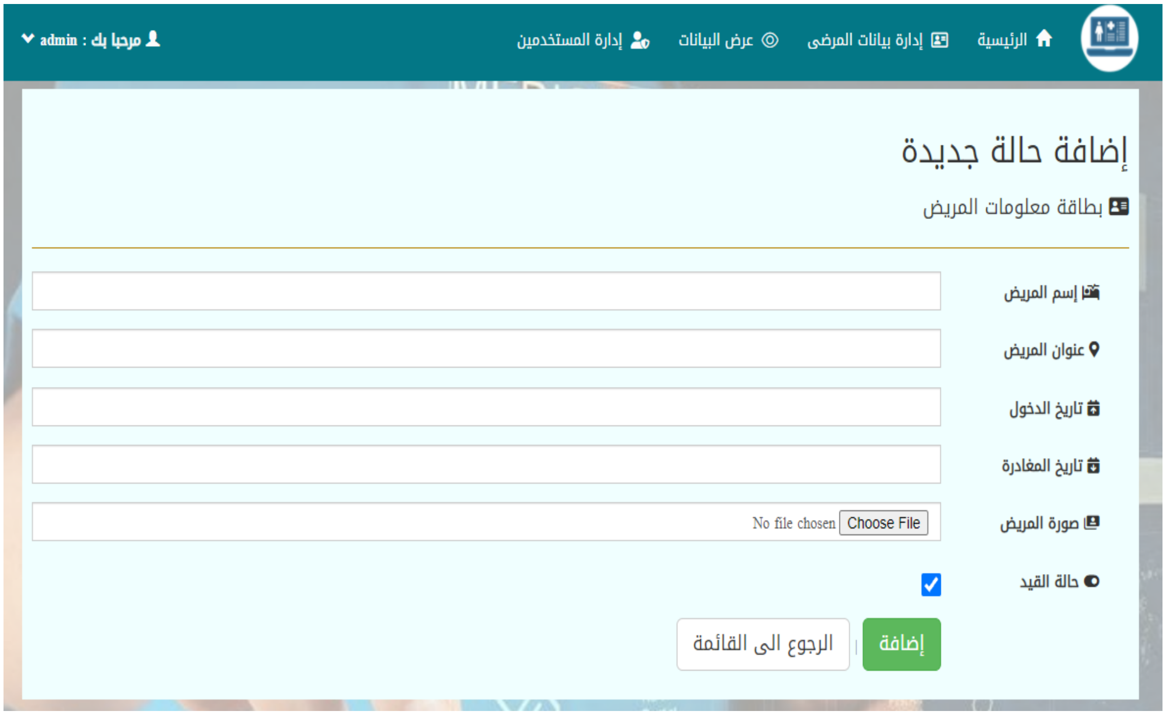
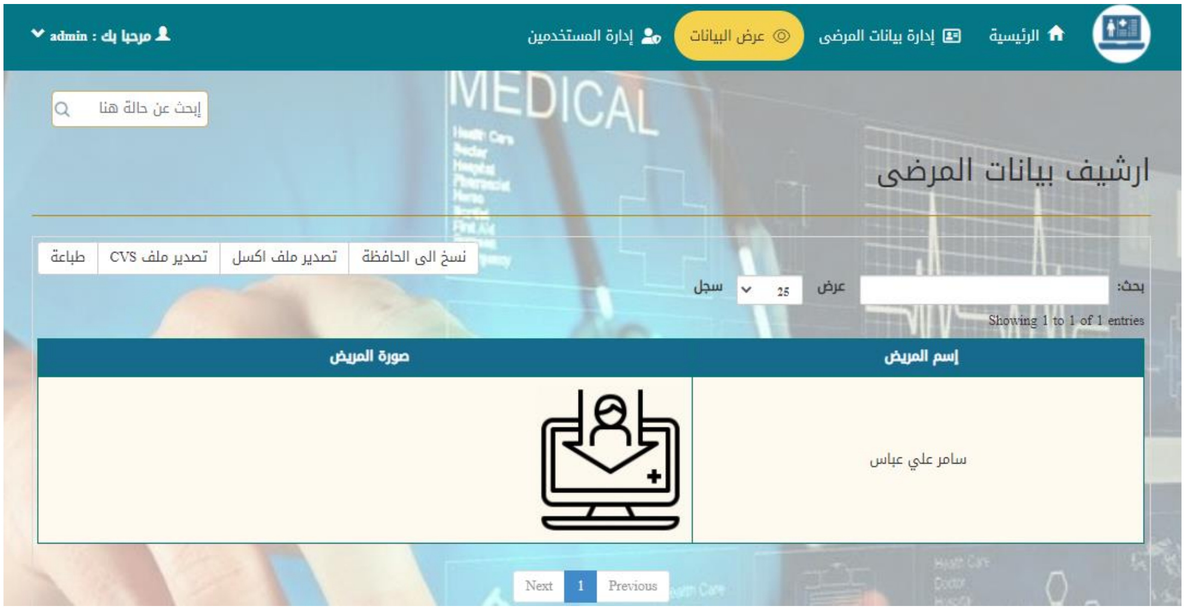


Figure (3.30): Add a new case page

In the third list, the data display list, the patient's data is displayed in terms of name and photo only. This list is displayed to anyone who does not have the options to access and control this page and search on a case. No other information is shown in addition to searches and export to excel sheets, printing, or saving the data as in Figure (3.31).



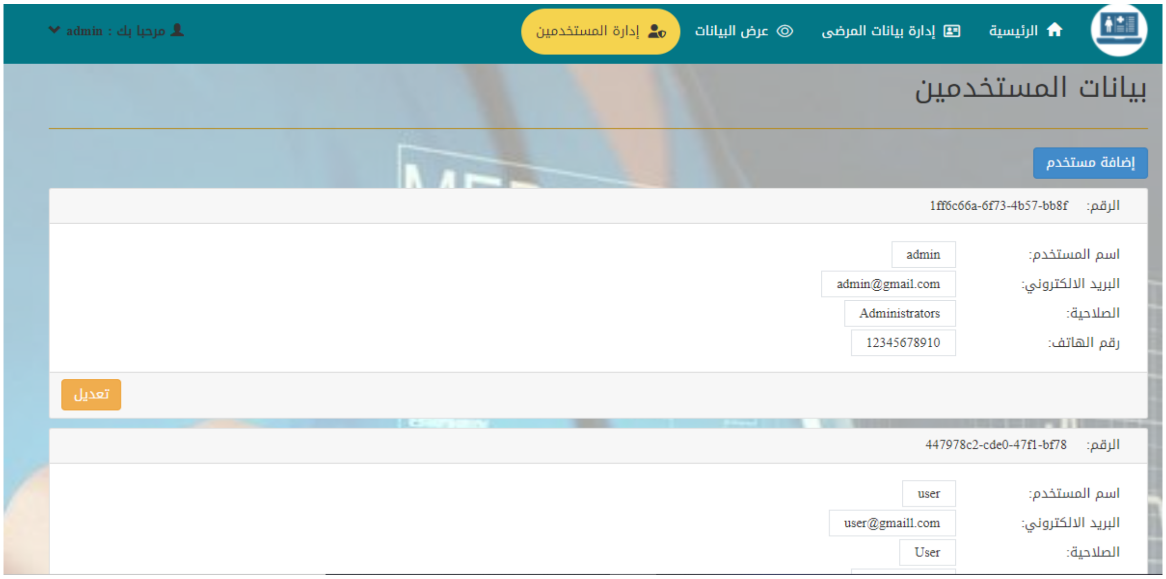
ارشيف بيانات المرضى

Showing 1 to 1 of 1 entries

إسم المريض	صورة المريض
سامر علي عباس	

Figure (3.31): Data display page

In the fourth list, which is the list of user data management, where access is controlled, and the number of people allowed to enter to head, enter, and process data, where an account and a specific password are created, and the accounts are modified or changed as shown in the Figure (3.32).



بيانات المستخدمين

الرقم: 1ff6c66a-6f73-4b57-bb8f

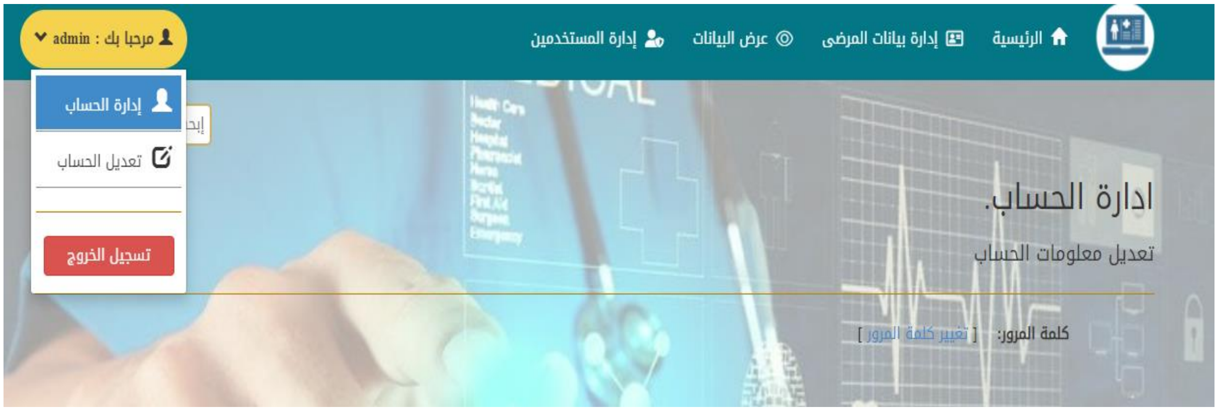
اسم المستخدم: admin
البريد الالكتروني: admin@gmail.com
الصلاحية: Administrators
رقم الهاتف: 12345678910

الرقم: 447978c2-cde0-47f1-bf78

اسم المستخدم: user
البريد الالكتروني: user@gmaill.com
الصلاحية: User

Figure (3.32): User management page

In the final list, which is for the user that contains account management information and account modification, in addition to logging out, when clicking on Manage Account, a window will appear to control changing the account password as in Figure (3.33).



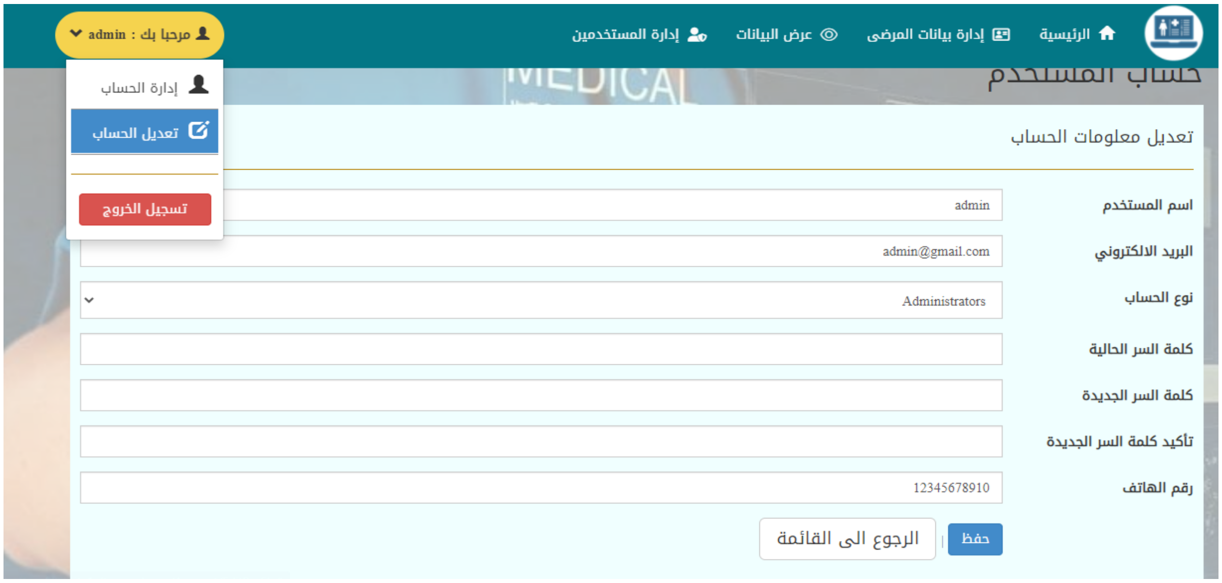
ادارة الحساب.

تعديل معلومات الحساب

كلمة المرور: [تغيير كلمة المرور]

Figure (3.33): Account modification page

When clicking on the Edit account, a window will appear to modify information in terms of the current password and change it to another, add an email, add the user's phone number and save the data or return to the main menu as in Figure (3.34)



حساب المستخدم

تعديل معلومات الحساب

اسم المستخدم admin

البريد الالكتروني admin@gmail.com

نوع الحساب Administrators

كلمة السر الحالية

كلمة السر الجديدة

تأكيد كلمة السر الجديدة

رقم الهاتف 12345678910

Figure (3.34):Edit account page

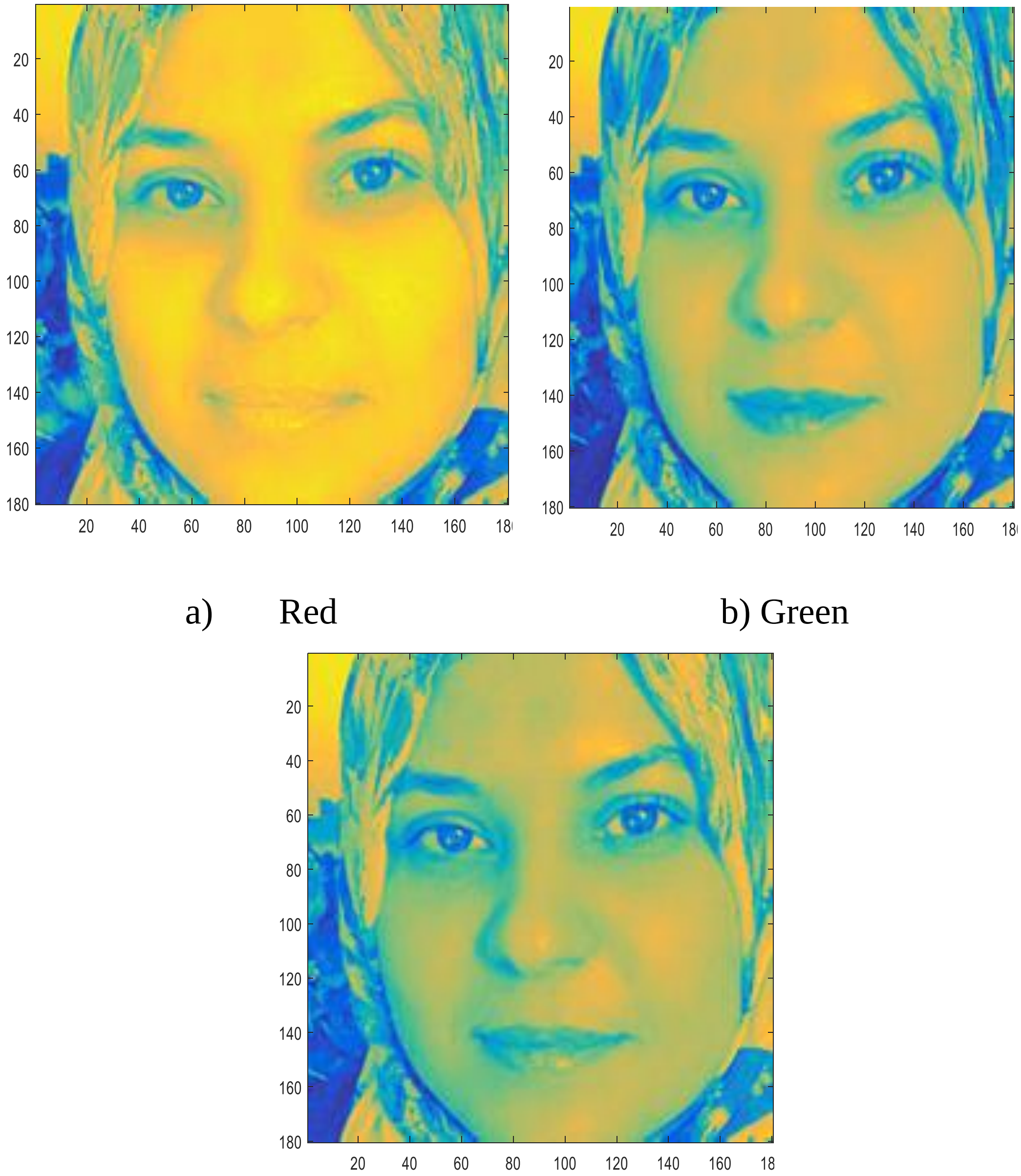
3.2.12Decryption and Extraction Process

If the key is known and decryption is possible, the secret (patient file) encrypted by a key in the embedding system can be extracted. This is the same key that is used during the embedding. However, they secrete information that must be encrypted before embedding, making it nearly hard for hackers to erase the encrypted data. Another essential aspect of information encryption is that the information energy is evenly dispersed over the host signal.

The process of the decryption algorithm consisting of many steps will be explained in detail as follows: After reading the image from the specific user in the web page and the need to extract the information, the image exports for saving at the administer computer to read it in the extraction program. The extraction program uses Mat lab language as in figure (3.35).

Figure (3.35): Patient image from the webserver

After reading the image in Matlab its extracted to the three colors as it contained (Red, Green, and Blue colors) as shown in Figure (3.36)

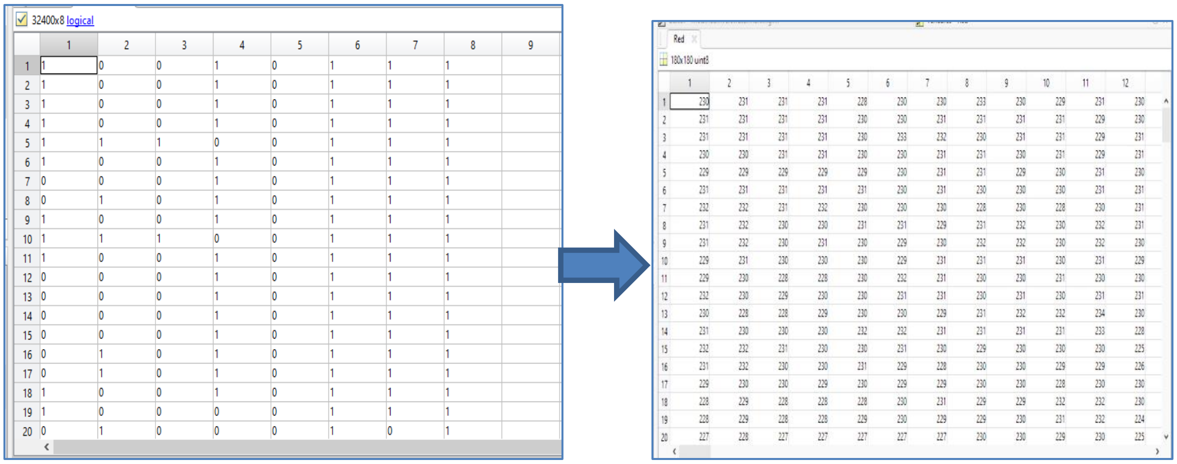


a) Red b) Green

c) Blue

Figure(3.36): The colors of the patient image

The pixels of red color are converted to one vector and then converted to the binary values, as shown in figure(3.37). The length of patient file information is stored in the least significant bit of the binary red color matrix.



☑ 32400x8 logical

	1	2	3	4	5	6	7	8	9
1	1	0	0	1	0	1	1	1	
2	1	0	0	1	0	1	1	1	
3	1	0	0	1	0	1	1	1	
4	1	0	0	1	0	1	1	1	
5	1	1	1	0	0	1	1	1	
6	1	0	0	1	0	1	1	1	
7	0	0	0	1	0	1	1	1	
8	0	1	0	1	0	1	1	1	
9	1	0	0	1	0	1	1	1	
10	1	1	1	0	0	1	1	1	
11	1	0	0	1	0	1	1	1	
12	0	0	0	1	0	1	1	1	
13	0	0	0	1	0	1	1	1	
14	0	0	0	1	0	1	1	1	
15	0	0	0	1	0	1	1	1	
16	0	1	0	1	0	1	1	1	
17	0	1	0	1	0	1	1	1	
18	1	0	0	1	0	1	1	1	
19	1	0	0	0	0	1	1	1	
20	0	1	0	0	0	1	0	1	

Red

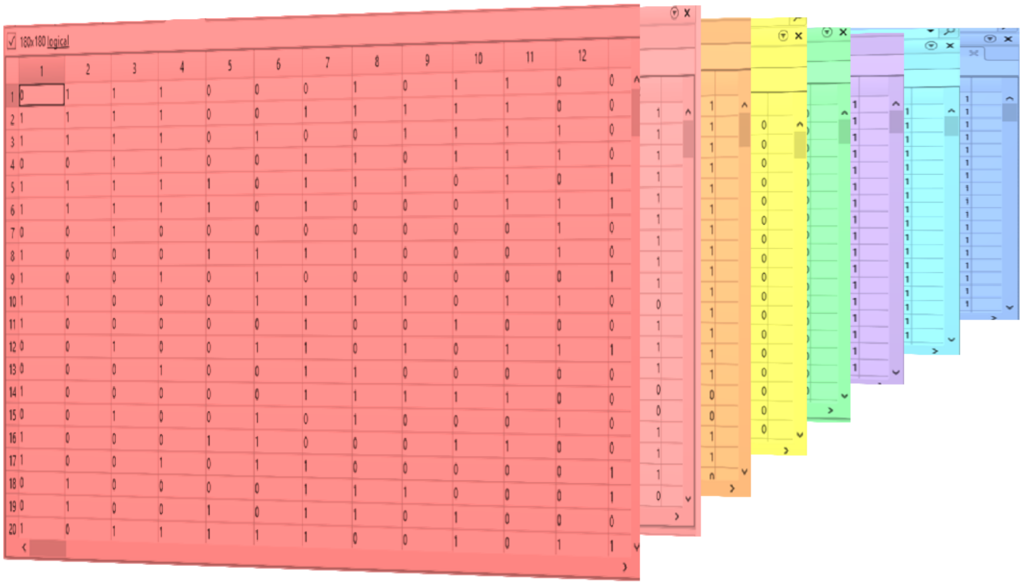
180x180 uint8

	1	2	3	4	5	6	7	8	9	10	11	12
1	230	231	231	231	228	230	230	233	230	229	231	230
2	231	231	231	231	230	230	231	231	231	231	229	230
3	231	231	231	231	230	233	232	230	231	231	229	231
4	230	230	231	231	230	230	231	231	230	231	229	231
5	229	229	229	229	229	230	231	231	229	230	231	230
6	231	231	231	231	231	230	231	230	230	230	231	231
7	232	232	231	232	230	230	230	228	230	228	230	231
8	231	232	230	230	231	231	229	231	232	230	232	231
9	231	232	230	231	230	229	230	232	232	230	232	230
10	229	231	230	230	230	229	231	231	231	230	231	229
11	229	230	228	228	230	232	231	230	230	231	230	230
12	232	230	229	230	230	231	231	230	231	230	231	231
13	230	228	228	229	230	230	229	231	232	232	234	230
14	231	230	230	230	232	232	231	231	231	231	233	228
15	232	232	231	230	230	231	230	229	230	230	230	225
16	231	232	230	230	231	229	228	230	230	229	229	226
17	229	230	230	229	230	229	229	230	230	228	230	230
18	228	229	228	228	228	230	231	229	229	232	232	230
19	228	229	228	228	229	230	229	229	230	231	232	224
20	227	228	227	227	227	227	227	230	230	229	230	225

a) b)

Figure(3.37): The conversion of the matrix to binary value (a) red color matrix (b) binary value matrix

The next step of the extraction process is to convert the green color to the binary matrix with eight dimensions, as shown in figure(3.38)

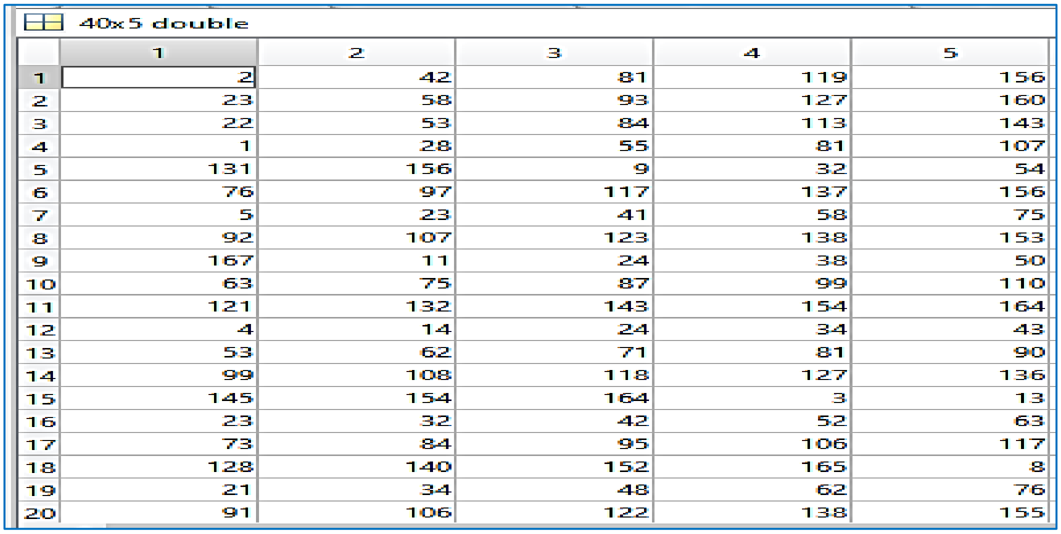


☑ 180x180 logical

	1	2	3	4	5	6	7	8	9	10	11	12	
1	0	1	1	1	0	0	0	1	0	1	1	0	0
2	1	1	1	1	0	0	1	1	1	1	1	0	0
3	1	1	1	1	0	1	0	0	1	1	1	1	0
4	0	0	1	1	0	0	1	1	0	1	1	1	0
5	1	1	1	1	1	0	1	1	1	0	1	0	1
6	1	1	1	1	1	0	1	0	0	0	1	1	1
7	0	0	1	0	0	0	0	0	0	0	0	1	0
8	1	0	0	0	1	1	1	1	0	0	0	1	0
9	1	0	0	1	0	1	0	0	0	0	0	0	1
10	1	1	0	0	0	1	1	1	1	0	1	1	0
11	1	0	0	0	0	0	1	0	0	1	0	0	0
12	0	0	1	0	0	1	1	0	1	0	1	1	1
13	0	0	0	1	0	0	1	1	0	0	0	0	0
14	1	0	0	0	0	0	1	1	1	1	1	0	0
15	0	0	1	0	0	1	0	1	0	0	0	1	0
16	1	0	0	0	1	1	0	0	0	1	1	0	0
17	1	0	0	1	0	1	1	0	0	0	0	0	1
18	0	1	0	0	0	0	1	1	1	0	0	0	1
19	0	1	0	0	1	0	1	1	0	1	0	0	0
20	1	0	1	1	1	1	1	0	0	1	0	1	1

Figure (3.38): Eight dimensions of binary green color

At this point, the program generates the 2D cubic spline interpolation with a length equal to the patient file length to specify the locations on the hiding data in Figure (3.39). The information and root of the cubic interpolation must be the same as roots used on the encryption side. If they differ, the values generated will vary, so the data and information cannot return correctly.

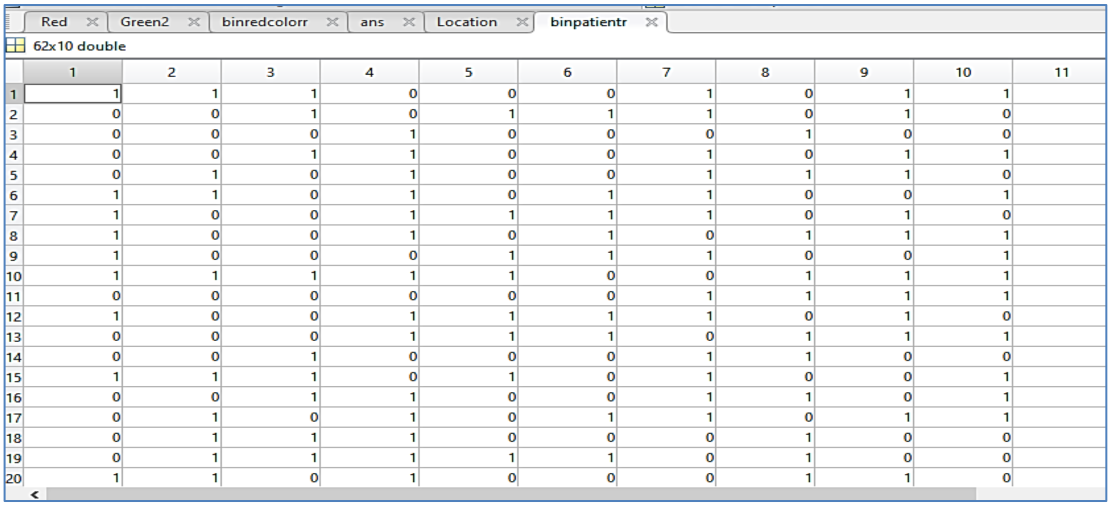


40x5 double

	1	2	3	4	5
1	2	42	81	119	156
2	23	58	93	127	160
3	22	53	84	113	143
4	1	28	55	81	107
5	131	156	9	32	54
6	76	97	117	137	156
7	5	23	41	58	75
8	92	107	123	138	153
9	167	11	24	38	50
10	63	75	87	99	110
11	121	132	143	154	164
12	4	14	24	34	43
13	53	62	71	81	90
14	99	108	118	127	136
15	145	154	164	3	13
16	23	32	42	52	63
17	73	84	95	106	117
18	128	140	152	165	8
19	21	34	48	62	76
20	91	106	122	138	155

Figure (3.39): The sample 2D cubic spline in the reviser side

In generating a 2D cubic spline, specify the hiding data location. The data is extracted in the inverse rule of encryption from this location as a binary value with eight bits to produce the secure patient information see Figure (3.40).



	1	2	3	4	5	6	7	8	9	10	11
1	1	1	1	0	0	0	1	0	1	1	
2	0	0	1	0	1	1	1	0	1	0	
3	0	0	0	1	0	0	0	1	0	0	
4	0	0	1	1	0	0	1	0	1	1	
5	0	1	0	1	0	0	1	1	1	0	
6	1	1	0	1	0	1	1	0	0	1	
7	1	0	0	1	1	1	1	0	1	0	
8	1	0	0	1	0	1	0	1	1	1	
9	1	0	0	0	1	1	1	0	0	1	
10	1	1	1	1	1	0	0	1	1	1	
11	0	0	0	0	0	0	1	1	1	1	
12	1	0	0	1	1	1	1	0	1	0	
13	0	0	0	1	1	1	0	1	1	1	
14	0	0	1	0	0	0	1	1	0	0	
15	1	1	1	0	1	0	1	0	0	1	
16	0	0	1	1	0	0	1	1	0	1	
17	0	1	0	1	0	1	1	0	1	1	
18	0	1	1	1	0	0	0	1	0	0	
19	0	1	1	1	1	1	0	1	0	0	
20	1	1	0	1	0	0	0	1	1	0	

Figure (3.40) :Sample of binary secure patient information

This secure patient information converts to decimal values to apply the second decryption algorithm.

Secure patient file=[71 116 136 76 202 107 121 169
113 159 192 121 184 196 87 204 106 142 190
139 202 53 117 140 71 144 70 112 139 84
128 95 136 138 111 123 144 74 153 58 67
140 88 137 71 144 68 94 194 135 112 204
156 199 116 172 126 121 177 188 168 188]

At this time, the logistic map is generated with a length equal to the patient file length and root same that on the encryption side (r=4 and x0= 0.94281) as shown in Figure (3.41) and subtract the results values (logistic map and secure patient information) to get the final report.

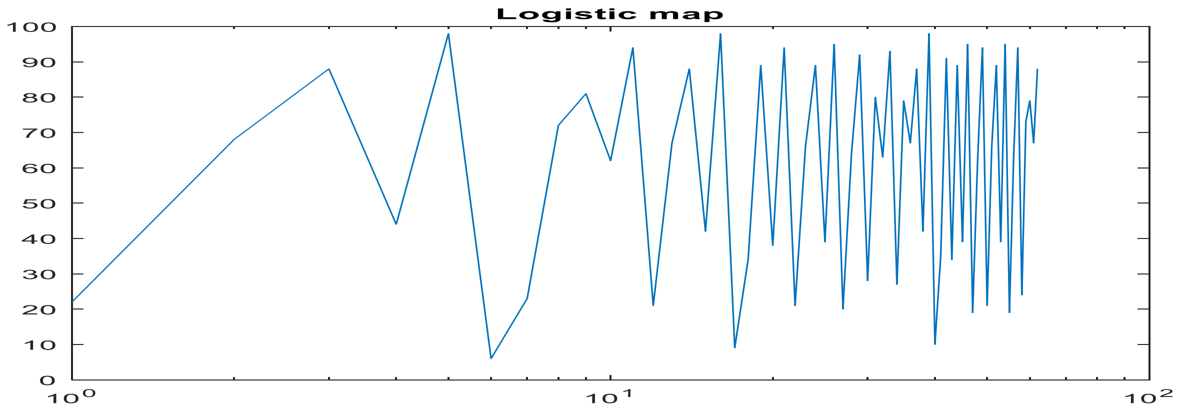


Figure (3.41):Logistic map in the receiver side

```
patient file=[ 71   116   136   76    202   107   121   169   113   159
          192   121   184   196   87    204   106   142   190   139   202
          53    117   140   71    144   70    112   139   84    128   95
          136   138   111   123   144   74    153   58    67    140   88
          137   71    144   68    94    194   135   112   204   156   199
          116   172   126   121   177   188   168   188]-[ 22    68    88
          44    98    6     23    72    81    62    94    21    67    88
          42    98    9     34    89    38    94    21    66    89    39
          95    20    64    92    28    80    63    93    27    79    67
          88    42    98    10    35    91    34    89    39    95    19
          62    94    21    66    89    39    95    19    63    94    24
          73    79    67    88]

patient Data=[ 49   48    48    32    104   101   98    97    32    97
          98    100   117   108   45    106   97    108   101   101   108
          32    51    51    32    49    50    48    47    56    48    32
          43    111   32    56    56    32    55    48    32    49    54
```

48 32 49 49 32 100 114 46 115 117 104
97 109 32 97 104 109 101 100].

This patient data matrix is then converted to the string value to extract the information as text. The result of conversion is as follows:

Patient no:100

Patient name: Heba Abdul-Jaleel

Age:32

Blood pressur:120/80

Blood type:+o

Respiratory rate:88

Weight: 70

Length: 160

Statistical number: 11
Name surgeon: dr. suham Ahmed

It tests different types of attacks on the cover image, such as Salt & Pepper Noise, Additive White Gaussian Noise (AWGN), Poisson noise, and Speckle noise. Performance Parameters are calculated in terms of The bit error rate (BER), Similarity, "Signal to Noise Ratio (SNR)," "Peak Signal To Noise Ratio (PSNR)," and "Root Mean Square Value(RMS)" have a habit of assessing the quality of the correlation between the original and derived information according to the equations (3,4,5,6, and7). The results show that the program works well to extract the encrypted data.
The bit error rate can calculate by equation (3.3):

$$BER = \frac{B_{err}}{M * N} * 100\% \qquad (3.3)$$

$$SNR = \frac{Power_{signal}}{Power_{noise}} \tag{3.4}$$

Signal to noise ratio can calculate by equation (3.5):

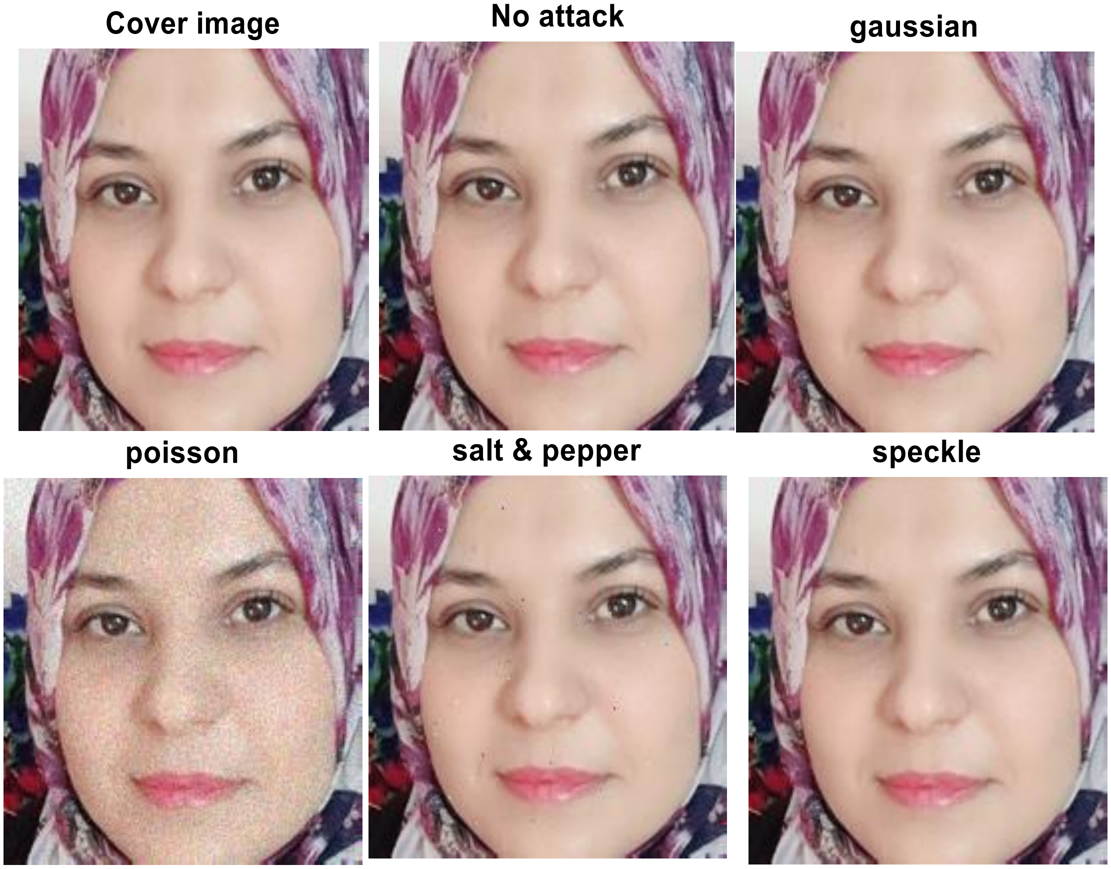
$$SNR = 10\log_{10}\left(\frac{\sum_{n=1}^{N} x^2(n)}{\sum_{n=1}^{N} \left(x(n) - x'(n)\right)^2} \right) \tag{3.5}$$

the root means the fair value of the quantity can also calculate by equation (3.6):

$$RMS = \sqrt{[MSE]^2} \tag{3.6}$$

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[x'(i,j) - x'(i,j)]^2 \tag{3.7}$$

The table below shows the image quality measurements with different types of attacks. The effect of the episodes (Gaussian, Poisson, Salt &pepper, and Speckle) on the cover image is shown in figure (3.42).



Cover image

No attack

gaussian

poisson

salt & pepper

speckle

Figure(3.42): Different status for the effect of the attack on the cover image

Tables (3.2): The impact of various watermarking attacks for the image

Type of attack	SSIM	SNR	MSE	PSNR	RATE	RMS
No attack	1	49.9152	0.0004	93.7543	0.0003	0.0212
Gaussian	0.9999	43.8347	0.0035	83.4827	0.0026	0.0592
Poisson	0.85060	2.0689	17.0773	41.0258	0.3689	4.1324
Salt &pepper	0.9912	12.9373	0.02953	72.8263	0.0003	0.1718
Speckle	0.9999	43.2697	0.00203	86.1959	0.00293	0.0451

The proposed algorithm interphase the pixel position of the host (cover)image using 2D- cubic spline interpolation and embedded information using the (LSB) technique in the eight binary planes of the green color from covers images. The proposed steganography algorithm is effective and has been proven to be resistant to a variety of attacks. Figure (3.40) shows the resolution (180*180) of the host color image with different attacks, such as Gaussian noise, Poisson noise, Salt and Pepper noise, and finally speckle noise. Table (3.2) depicts the impact of these attacks are excellent results prove that the proposed algorithm is resistant to a wide range of attacks. Gaussian noise has the most significant impact on the steganography image, as does the addition of salt noises, which lowers the image's quality.

Chapter Four

CHAPTER FOUR
LABORATORY RESULTS AND DISCUSSION

4.1 Introduction

The results of the proposed system finding in this chapter come from software created in Matlab 2016 utilizing a computer "Dell-8NFVKIE, Intel(R)" with an Intel Core i7 CPU and 4.00 GHz SSD RAM running Windows 10. The results are presented in two classifications, one for the Database subsystem and the other for encryption subsystems.

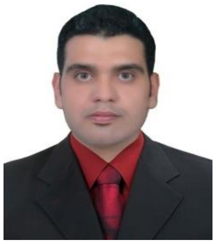
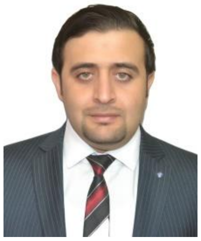
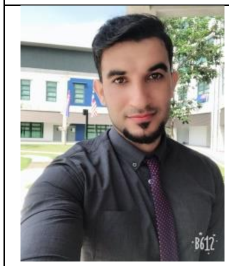
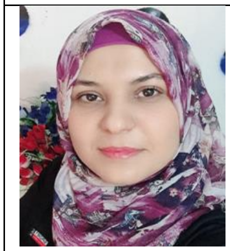
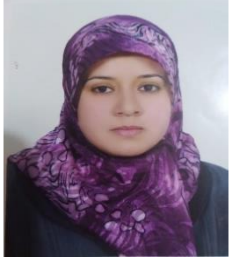
4.2The Encryption System

The algorithm of the encryption system consists of many processes explained in chapter three, where the cover image of the patient is loaded to it and passed through different encryption operations. The 2D cubic spline interpolation, the chaotic algorithm, and the least significant bits are types of encryption subsystems used in the proposed steganography system.

Since there are different image formats, two types of these formats are taken in the experiments study to check the algorithm's robustness. JPG is a lossy image compression format, meaning there is a difference between reading and writing the matrices and lossless PNG format. More details are in appendix B.

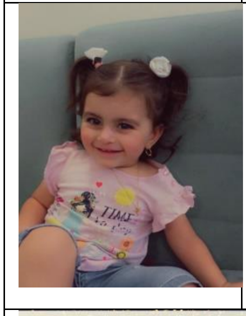
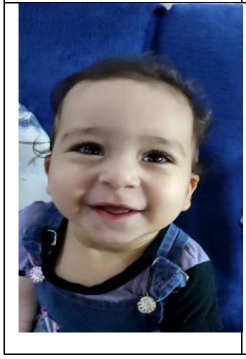
To study the effectiveness and robustness of the encryption algorithm, many cases are studied and subject to different image attacks such as Gaussian, salt and pepper, Poisson, and Speckle noise. As explained in chapter three, the robustness is measured in terms of PSNR, RMS values, and the number of errors. Here Table (4.1) depicts the images with specific data used in the encryption program.

Table (4.1): Images with specific information as experiment information.

Patient image	Patient name	age	Weight	length	Blood pressure	Blood type	Heart rate
	Ibrahim Hassan	36	93	178	120/80	O +	normal
	Mohammed Ihsan	32	90	173	110/70	B+	normal
	Alaa Nihad Tuama	33	88	185	120/70	B+	normal
	Heba Abdul-Jaleel	33	70	160	120/80	O +	normal
	Dilshad Abdul-Sada	39	62	150	110/80	B+	normal

	Ali Kadhim	26	65	173	120/80	O +	normal
	Gada Qanber Ali	34	49	150	120/80	O+	normal
	Ahmed Fouad	32	121	182	140/90	O+	normal
	Dhafer Thamir	33	88	173	120/80	AB+	normal
	Kassim Jumah Ali	35	67	167	120/80	O+	normal

	Mohammed Amir	38	92	180	120/80	**A-**	normal
	Laith Hussain Jasim	25	90	166	120/80	AB+	normal
	Ramy Riad Hussian	31	95	174	120/80	AB+	normal
	Balqees Abdul-Jaleel	25	55	153	120/80	O+	normal
	Mohammed Ganim Abas	32	66	176	120/80	O-	normal

	Salam Jabar Ali	30	88	185	120/80	O+	normal
	Hassan Falah Mohsen	34	89	176	120/80	A+	normal
	Sama Hussain Ali	2	11	76	120/80	B+	normal
	Ahmed Hussain Ali	6	22	127	120/80	B+	normal
	Fadl Mohammed Ganim	11 m	8	60	120/80	O+	normal

	Luma Hameed Abd	34	50	150	120/80	O-	normal
	Ali Abdul-jaleel	26	70	176	120/80	O+	normal

4.3 Case Study

Here, different images are taken and tracked from capturing to uploading on the webserver and finally downloading to extract the information.

4.3.1 Encryption System

Three images are taken as a case study to illustrate the program's work and test its durability against attacks on images if they were jammed during transmission.

These images are characterized in spite of differences in size, accuracy, and type, where some are of a PNG, and others are of JPEG formats. As for the quality, some of them are high, medial, and the other weak quality. Pictures that were randomly taken from the total donors in the program test whose information is mentioned in Table (4.1) as follows

The first case is taking (Fadl Mohammed Ganim) child image, Medium resolution with the size 732 KB (749,568 bytes) and 561*941 dimension with PNG format as shown in figure(4.1).

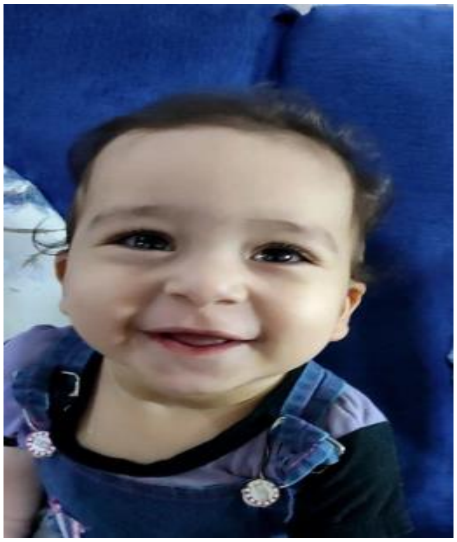


Figure (4.1): The first case (Fadl Mohammed Ganim) image

The second case is taking (Hassan Falah Mohsen) image, high-resolution photography with 2.11 MB (2,220,032 bytes), 1523*1541 dimension, and JPG format, as shown in figure (4.2).

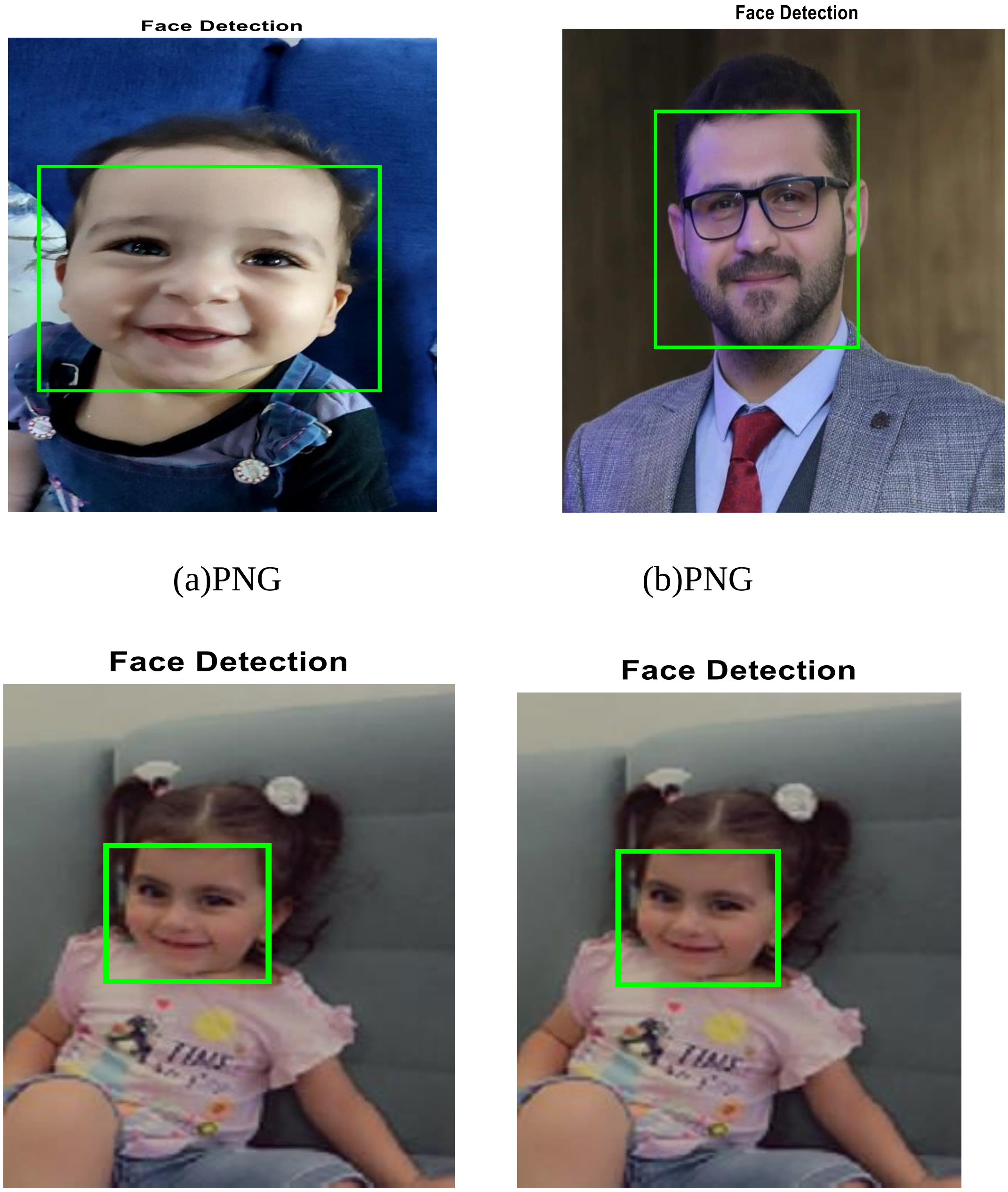
Figure (4.2): The second case (Hassan Falah Mohsen) image

The third case is taking (Sama Hussain Ali) child image, low resolution with 120 KB (122,880 bytes), and 200*267 dimensions with PNG and JPEG formats as shown in figure (4.3).

(a) (b)

Figure (4.3): The third case is taking (Sama Hussain Ali) image a) PNG and b) JPEG

Here the tracking procedure of the proposed system on these images, from capturing the image to uploading it to the server, is discuses. The first step is to read the image in the matlab program. Then, the algorithm resizes the image to the 180*180 resolution to make all images uniform. After resizing the image, enter the face detection algorithm to detect the patient face only, as shown in figure(4.4).



(a)PNG (b)PNG

(c)PNG (d)JPEG

Figure(4.4): Face detection step on the images after resizing them.

The second step is cropping the face only for all images to decrease the size of the data uploading to the webserver, as shown in Figure (4.5), and make this image a cover to encrypt the information in it.

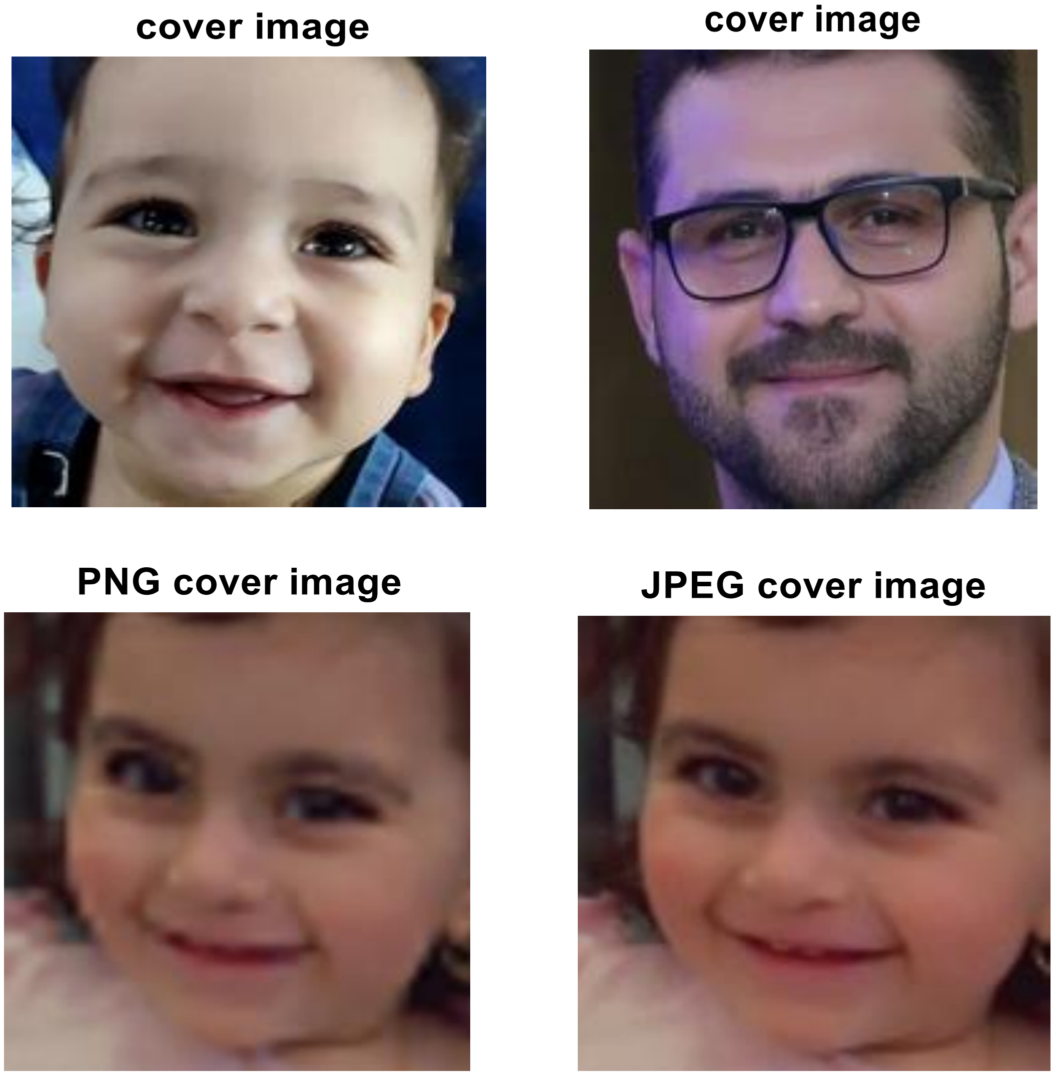
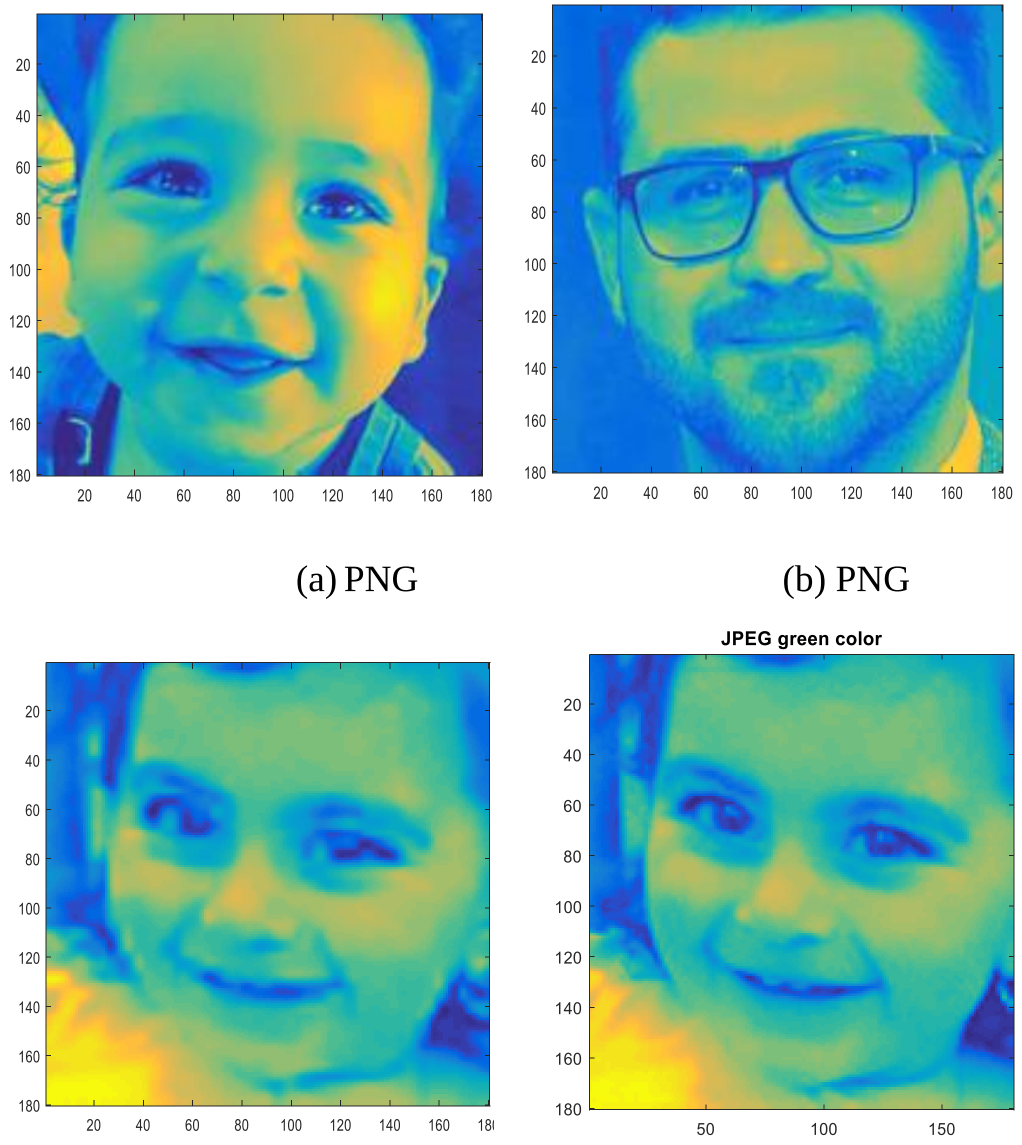


Figure (4.5): The cropping step on the cover images

When completing the cropping degree, the cover images extract the three colors (Red, Green, and Blue) for using the Green color and Red in the next encryption steps, as shown in figure(4.6).



(a) PNG (b) PNG

(c) PNG (d) JPEG

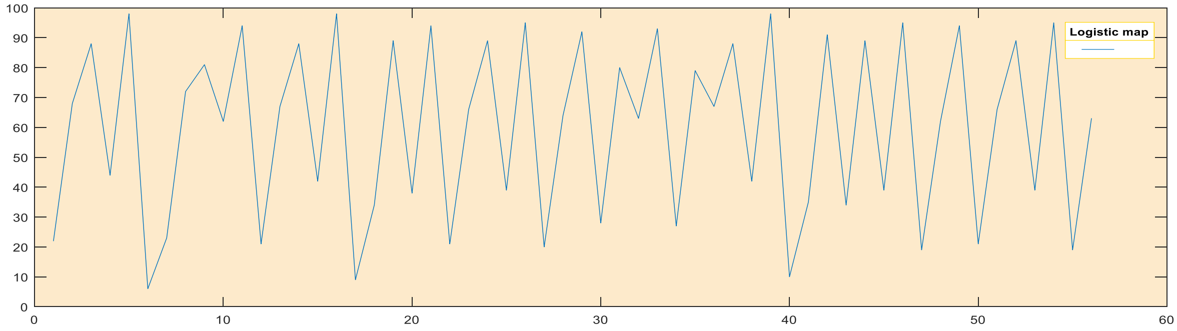
Figure(4.6): Green colors for the images

After preparing the Green color of the cover image. The third step is the program asking for entering the patient information, which is entered as ASCII code as in Table (4.2)

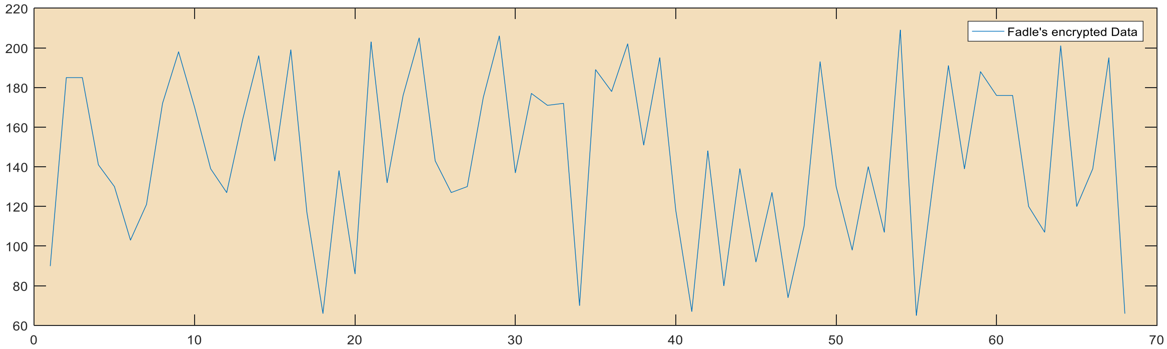
Table (4.2): Specific information for the three images

Patient name	age	Weight	length	Blood pressure	Blood type	Heart rate
Fadl Mohammed Ganim	11month	8	60	120/80	O+	normal
Hassan Falah Mohsen	34	89	176	120/80	A+	normal
Sama Hussain Ali	2	11	76	120/80	B+	normal

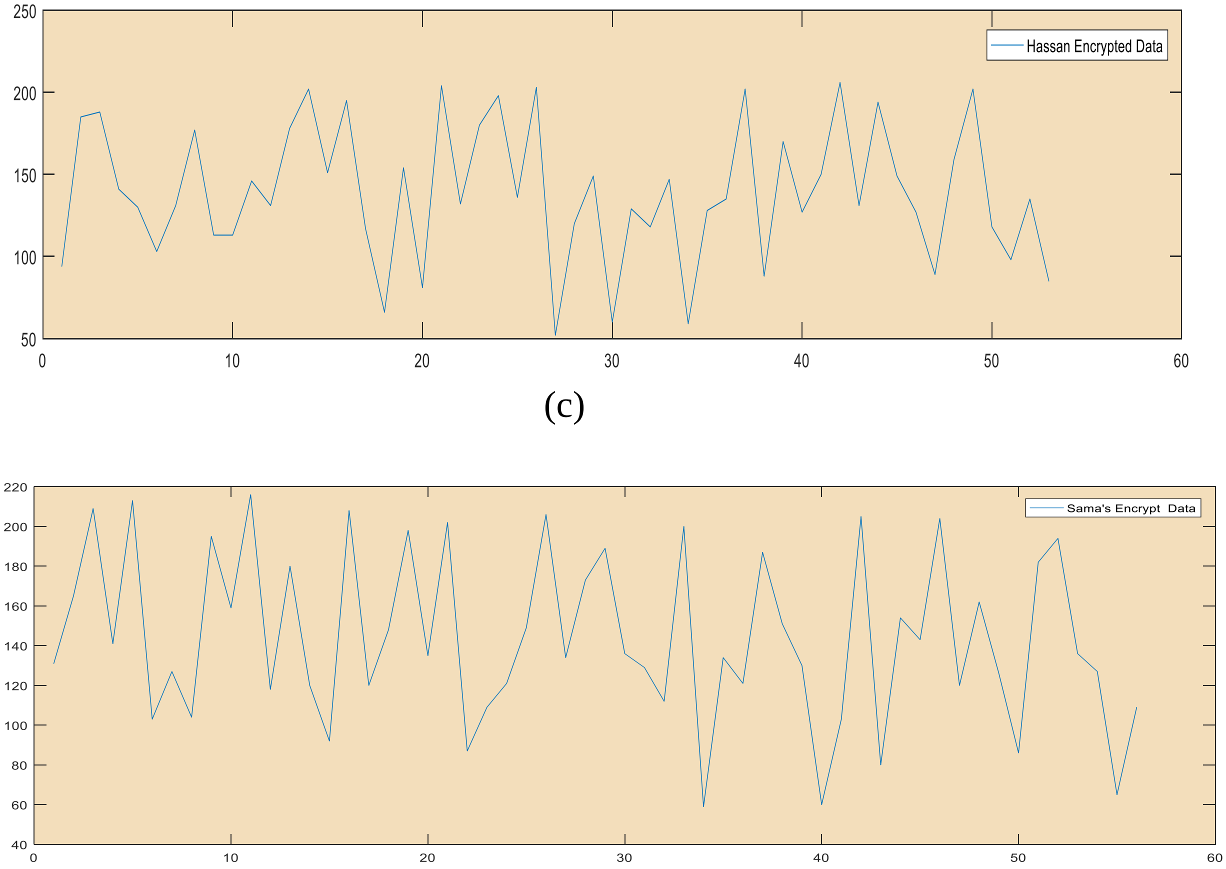
In the fourth step, the program generates the chaotic map (logistic map) with specific determinants mentioned in chapter three and encrypts the patient information. The logistic map diagram and the results of the encrypting patient information are depicted in figure(4.7).



(a)



(b)



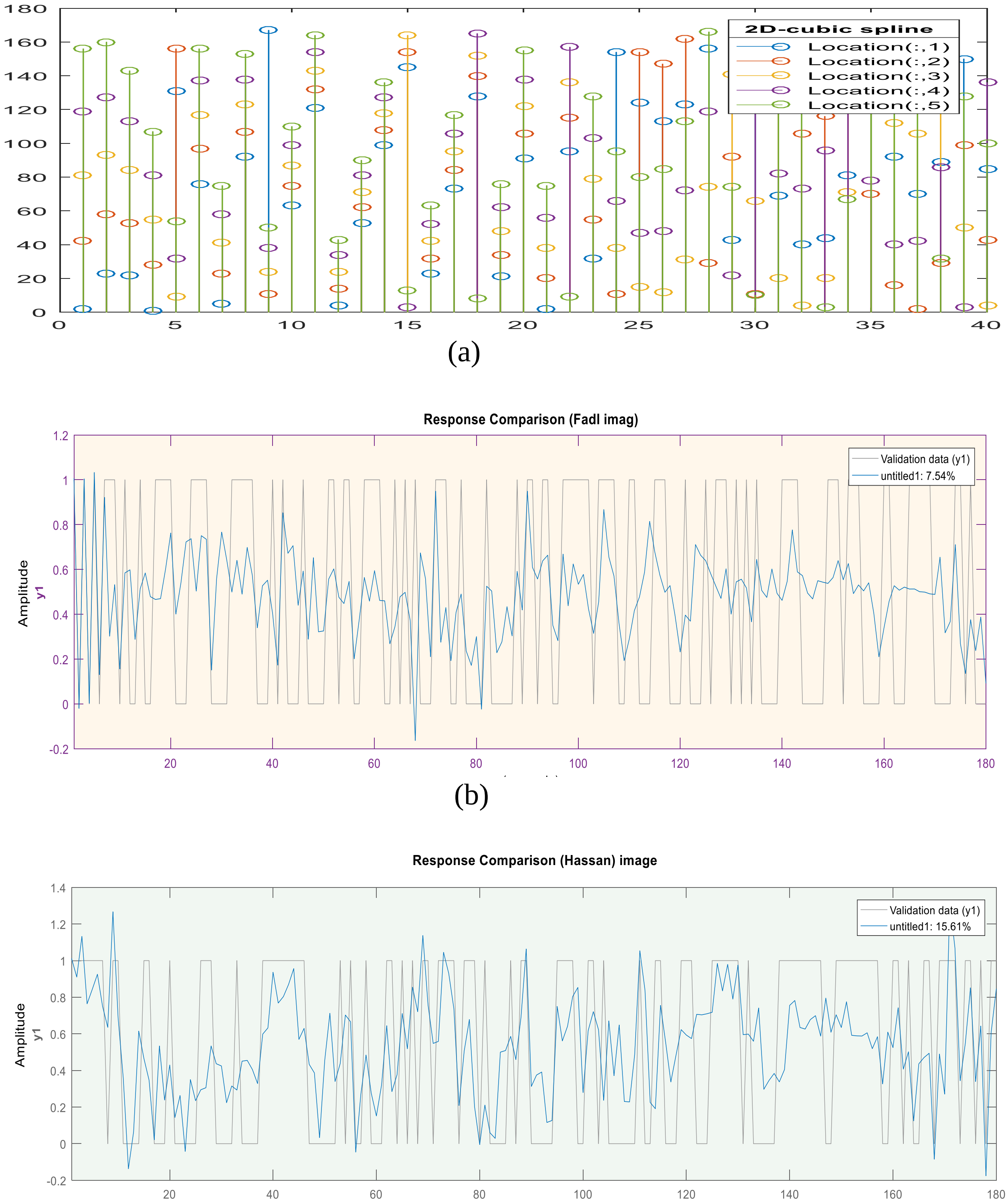
(c)

(d)

Figure(4.7): the encrypted patient information with logistic map encrypted part (a) logistic map, (b) Fadl's encrypted information (c) Hassan's encrypted information (d) Sama's encrypted information

The above figure shows the difference in the lengths of the data entered according to the different data for each person, thus giving a difference in the value and length, which gave a clear difference in the waveform of each person after encoding it using the logistic function.

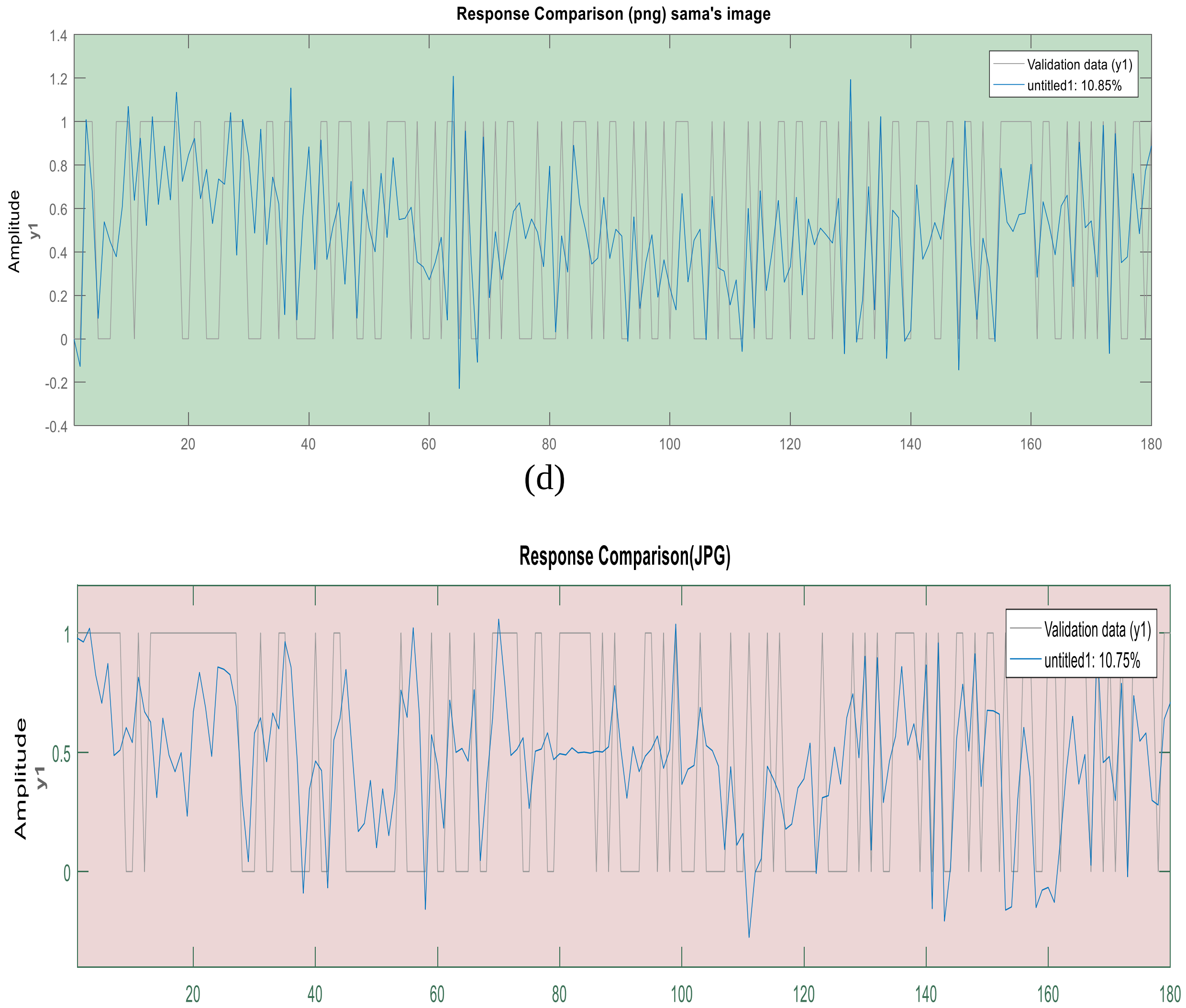
Fifth, after completing the first part of the coding, starting with the second part. Generate the 2D-cubic spline interpolation to locate the specific location on the green image to encrypt the secure patient information in it. The results of encrypting information in green are shown in figure(4.8).


2D-cubic spline
Location(:,1)
Location(:,2)
Location(:,3)
Location(:,4)
Location(:,5)
0 20 40 60 80 100 120 140 160 180
0 5 10 15 20 25 30 35 40
Response Comparison (Fadl imag)
Validation data (y1)
untitled1: 7.54%
Amplitude
y1
-0.2 0 0.2 0.4 0.6 0.8 1 1.2
20 40 60 80 100 120 140 160 180
Response Comparison (Hassan) image
Validation data (y1)
untitled1: 15.61%
Amplitude
y1
-0.2 0 0.2 0.4 0.6 0.8 1 1.2 1.4
20 40 60 80 100 120 140 160 180

(a)

(b)

(c)



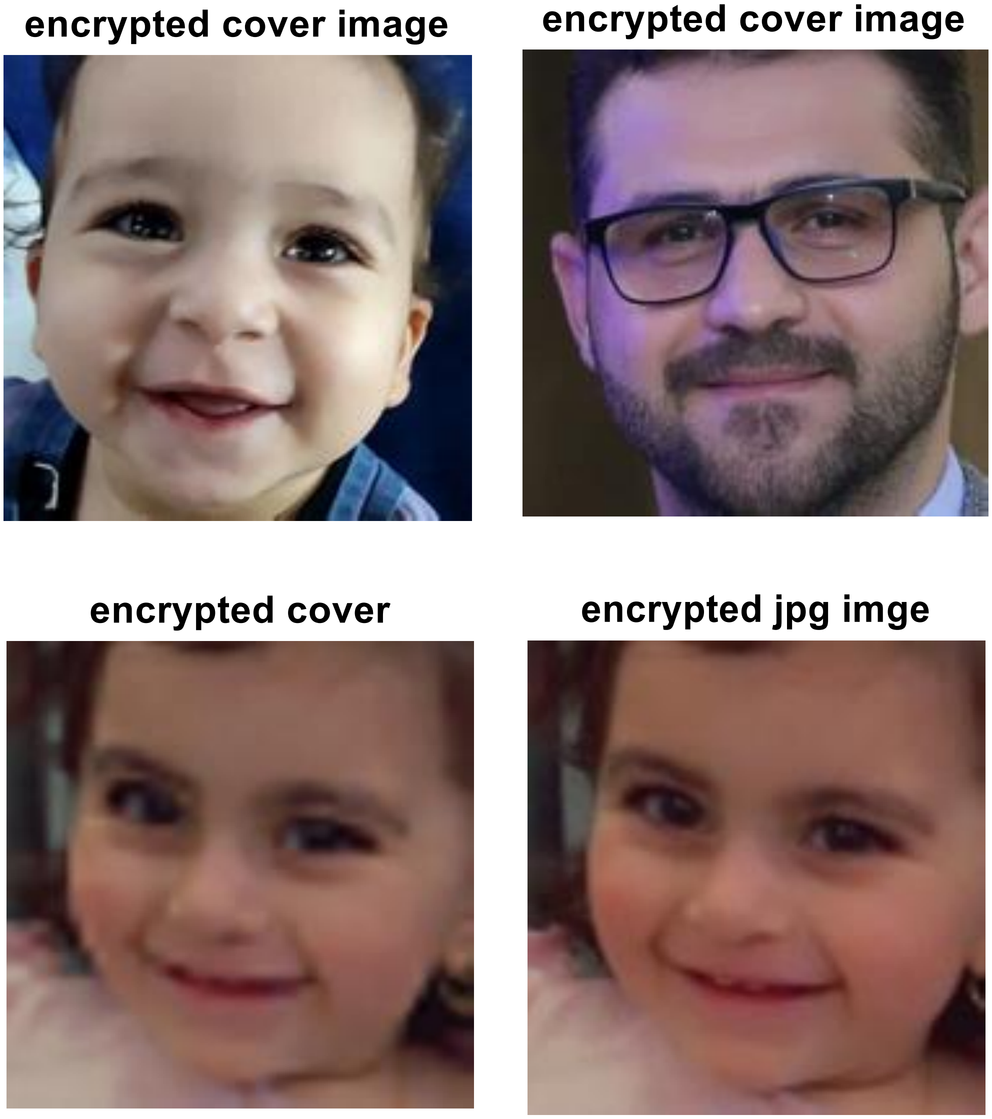
(d)

(e)

Figure(4.8): Green color at Encrypting information step for different images: (a)Cubic spline function,(b) green color of Fadl's image, (c) green color of Hassan's image, (d) green color of Sam's PNG image, (e) green color of Sam's JPG image,

The data distribution results from the first coding process on the sites almost randomly. According to the specific sites that appear in the above figure, four sites are identified that differ from the other row according to the two-dimensional cube spline function so that it absorbs all the data after converting it into binary numbers.

When completing the second encryption, the final encryption encrypts the length of the patient information in red colors with different images. Finally, the cover image is reconstructed from binary to decimal to the Green color combined with the rest of the colors to form a colorful image, as shown in figure (4.9).



encrypted cover image

encrypted cover image

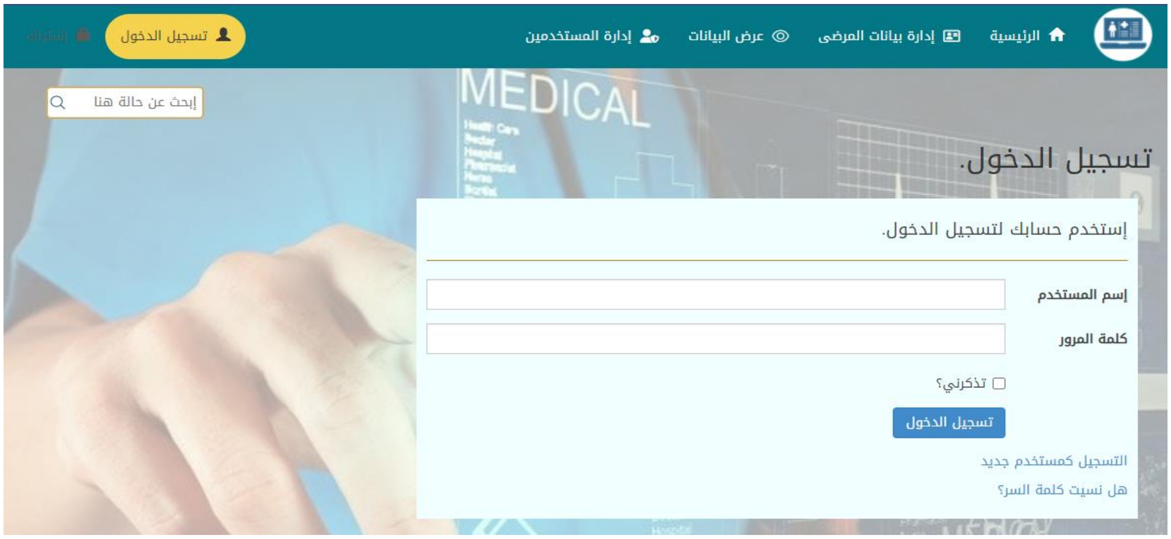
encrypted cover

encrypted jpg imge

Figure (4.9): Cover images in the final encryption step

4.3.2 Cloud And Database System

The patient image is uploaded to the cloud when completing the encryption process, and the case is added to the web to identify the patient card. The interfacing to the web page is shown in figure (4.10), and the patient card page is shown in figure (4.11).

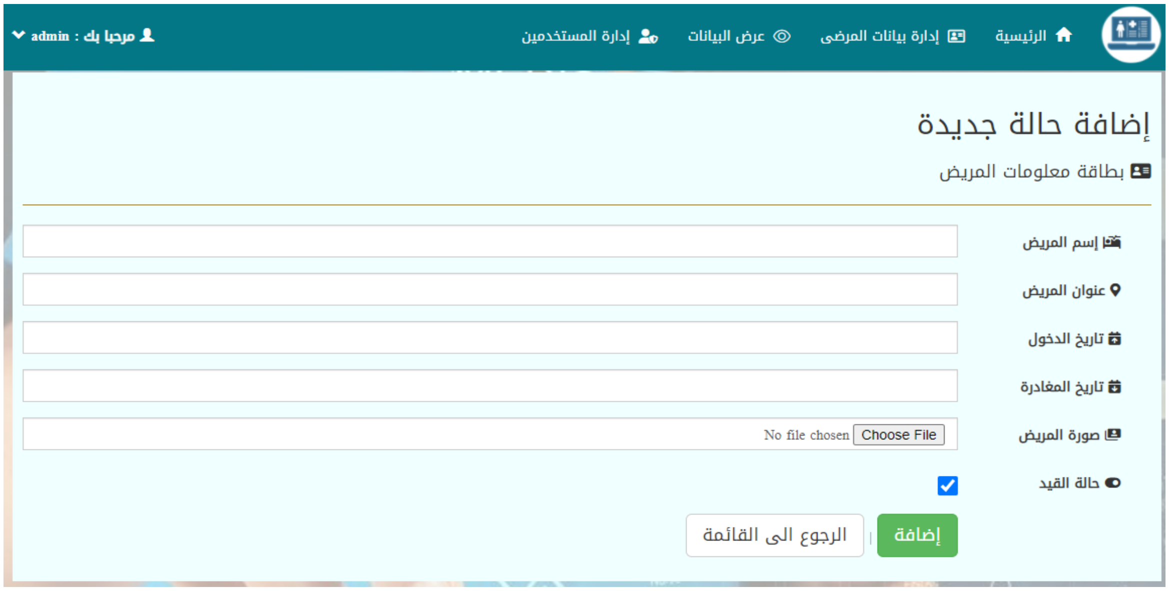


تسجيل الدخول.

إستخدم حسابك لتسجيل الدخول.

☐ تذكرني؟

Figure(4.10): Web page design



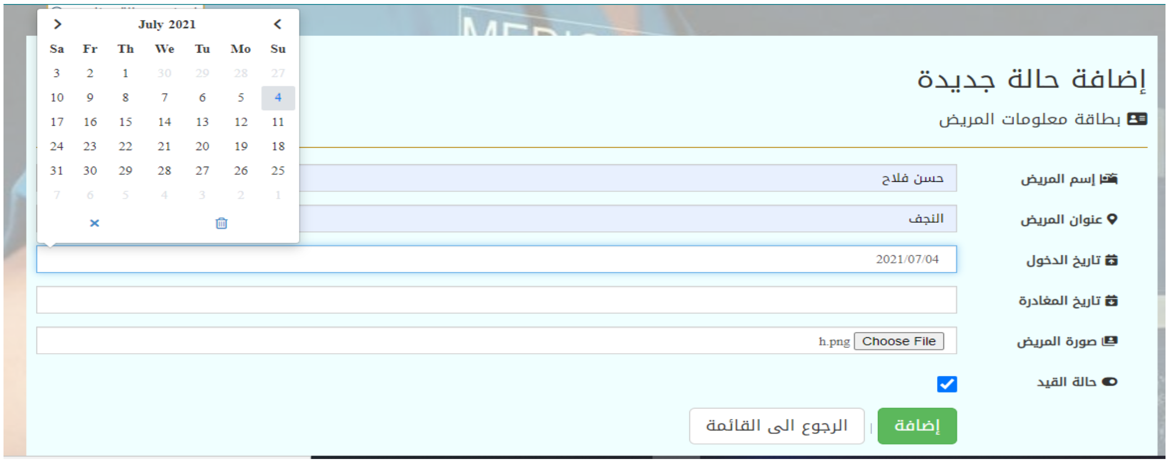
إضافة حالة جديدة

بطاقة معلومات المريض

حالة القيد ☑

figure (4.11): Entering a new case to the web.

The user completes the information needed, such as dating entry and leaving of the patient, which can be entered from the calendar or manually, address, and finally upload the image from the steganography part to archive it in the webserver as shown in figure (4.12). When entering information and clicking on added, the card is created for the patient and saved on the web as an archive. Many clients who have access to the patient web server can enter the patient information, and the web keeps them in the database.



July 2021

Sa	Fr	Th	We	Tu	Mo	Su
3	2	1	30	29	28	27
10	9	8	7	6	5	4
17	16	15	14	13	12	11
24	23	22	21	20	19	18
31	30	29	28	27	26	25
7	6	5	4	3	2	1

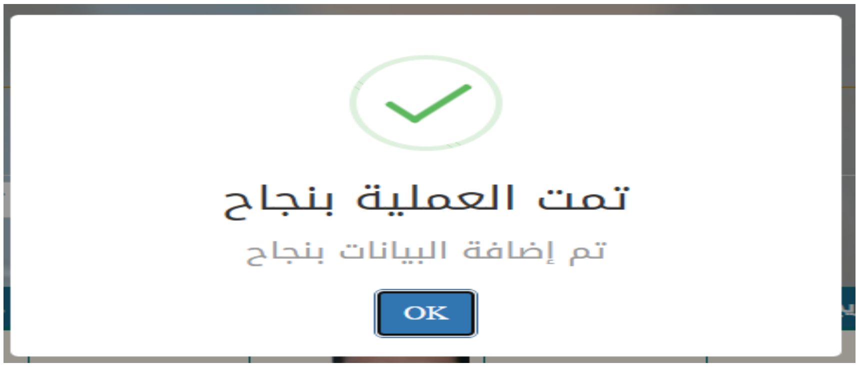
إضافة حالة جديدة

بطاقة معلومات المريض

إسم المريض	حسن فلاح
عنوان المريض	النجف
تاريخ الدخول	2021/07/04
تاريخ المغادرة	
صورة المريض	Choose File h.png
حالة القيد	☑

Figure (4.12): The page of entering Hasan's information in the webserver

A message appears when adding data is completed correctly and pressing the add button confirming that the addition has been completed successfully, as in Figure (4.13).

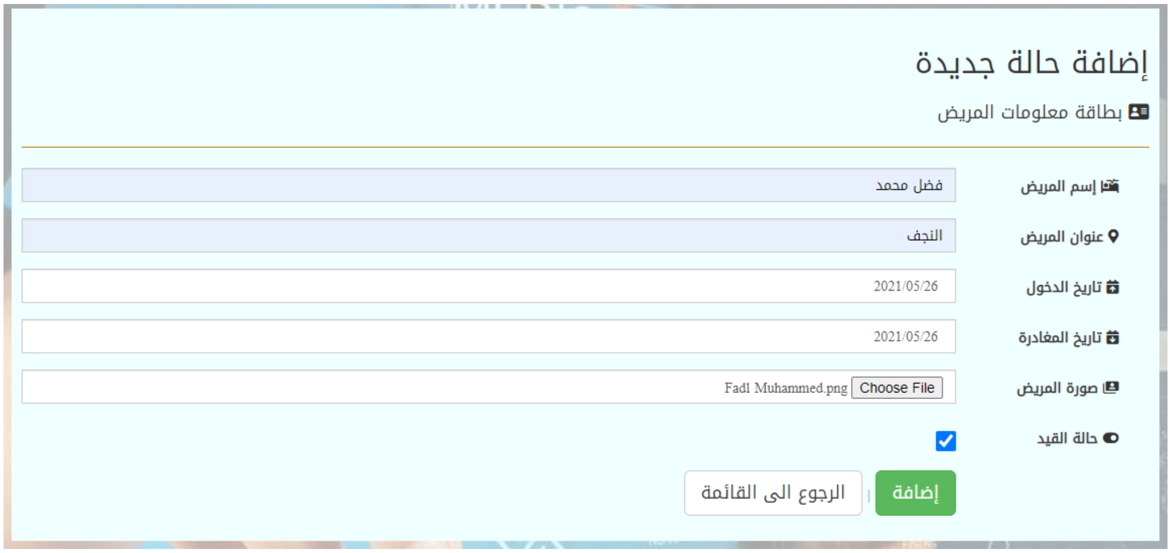


تمت العملية بنجاح

تم إضافة البيانات بنجاح

Figure (4.13): message of confirming of addition

The information of the other two cases adds to the webserver to save them in the database, as in Figures (4.14) and figure (4.15).

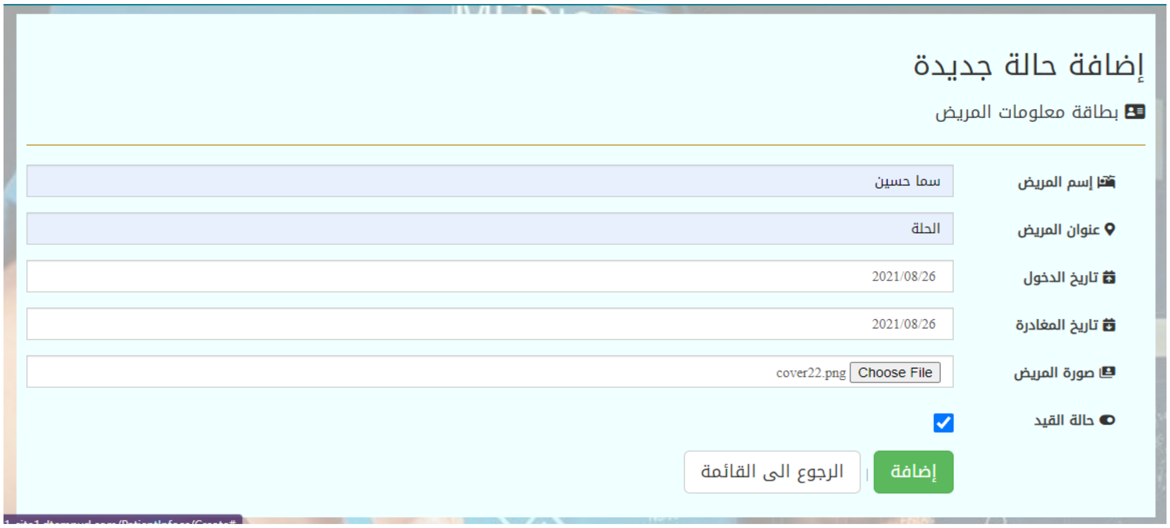


إضافة حالة جديدة

بطاقة معلومات المريض

إسم المريض	فضل محمد
عنوان المريض	النجف
تاريخ الدخول	2021/05/26
تاريخ المغادرة	2021/05/26
صورة المريض	Choose File Fadl Muhammed.png
حالة القيد	☑

Figure (4.14): The page of entering Fadl's information in the webserver



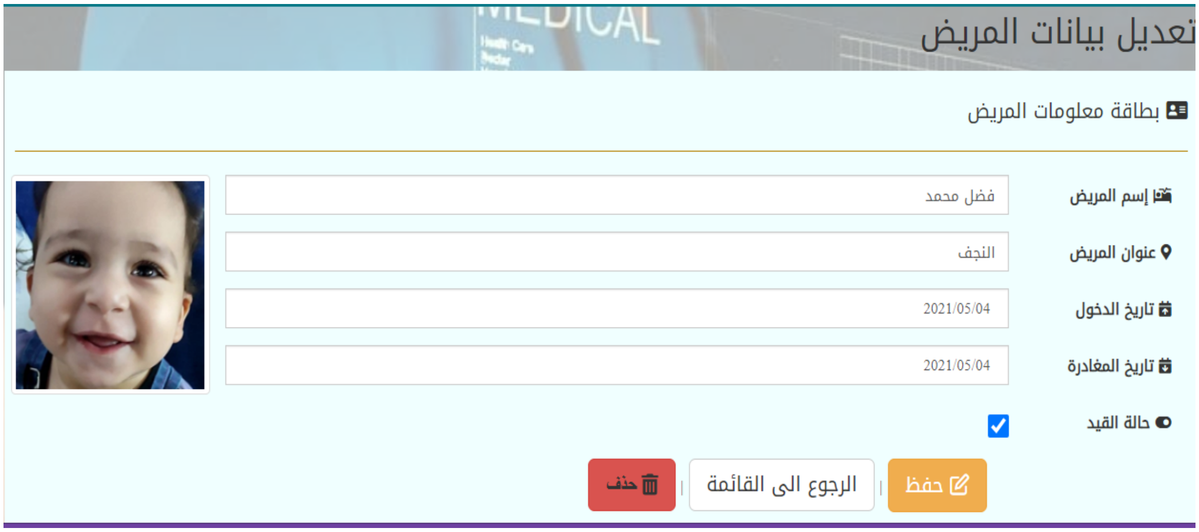
إضافة حالة جديدة

بطاقة معلومات المريض

إسم المريض	سما حسين
عنوان المريض	الحلة
تاريخ الدخول	2021/08/26
تاريخ المغادرة	2021/08/26
صورة المريض	Choose File cover22.png
حالة القيد	☑

Figure (4.15): The page of entering Sama's information in the webserver

Suppose the database needs to edit the patient information. In that case, the window will appear in Figure (4.16) containing the data entry information, leaving, address, saving, returning to home, and deleting on the news. Note here that the web saves the data entered, which appears on the patient details page.



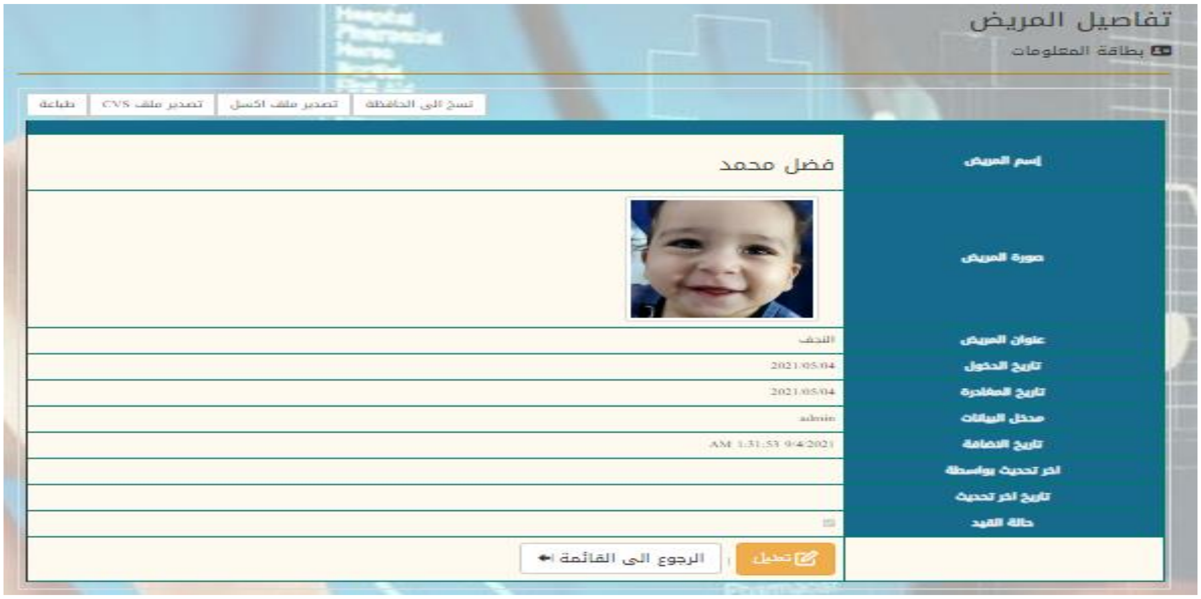
تعديل بيانات المريض

بطاقة معلومات المريض

إسم المريض	فضل محمد
عنوان المريض	النجف
تاريخ الدخول	2021/05/04
تاريخ المغادرة	2021/05/04
حالة القيد	☑

Figure(4.16): The editing page of patient information

When entering the patient's details, the information list will be shown in figure(4.17) and then save the data. The admin with the extraction program can save the image to his computer and run after reading the image to extract the patient file information.



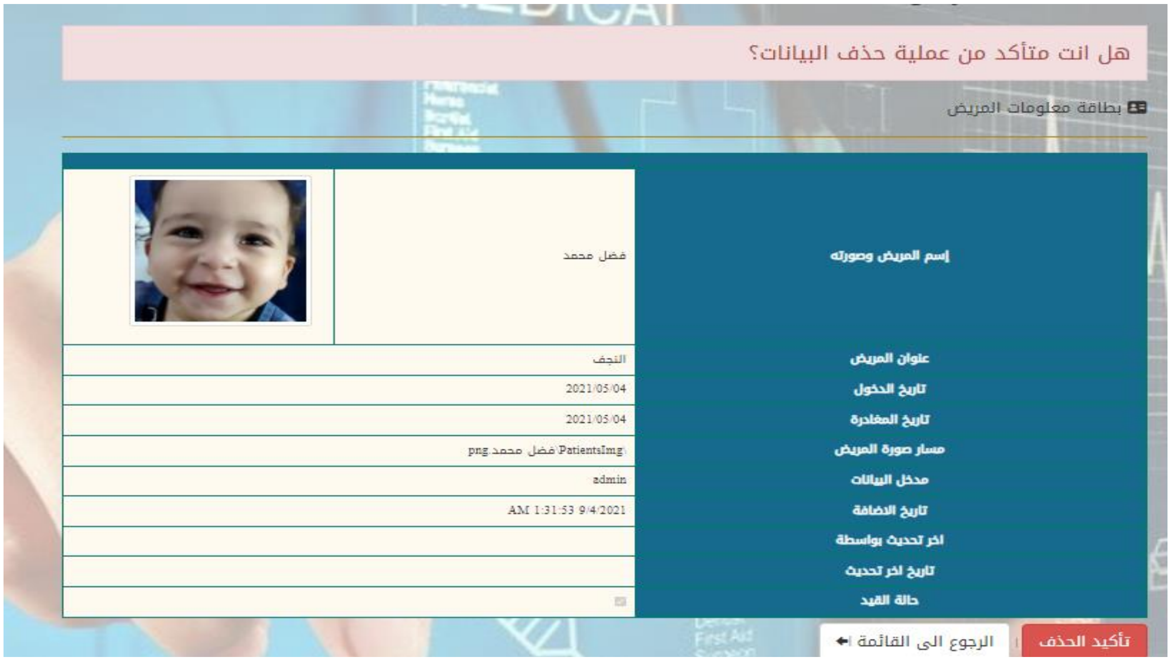
تفاصيل المريض

بطاقة المعلومات

إسم المريض	فضل محمد
صورة المريض	
عنوان المريض	النجف
تاريخ الدخول	2021/05/04
تاريخ المغادرة	2021/05/04
مدخل البيانات	admin
تاريخ الاضافة	AM 1:31:53 9/4/2021
اخر تحديث بواسطة	
تاريخ اخر تحديث	
حالة القيد	☐

figure (4.17): The details of patient information

Suppose the admin deletes the patient information and pushes it on the recycle bin. In that case, the deleting confirmation message appears on the screen as in figure (4.18), confirming the deleting or undoing it.



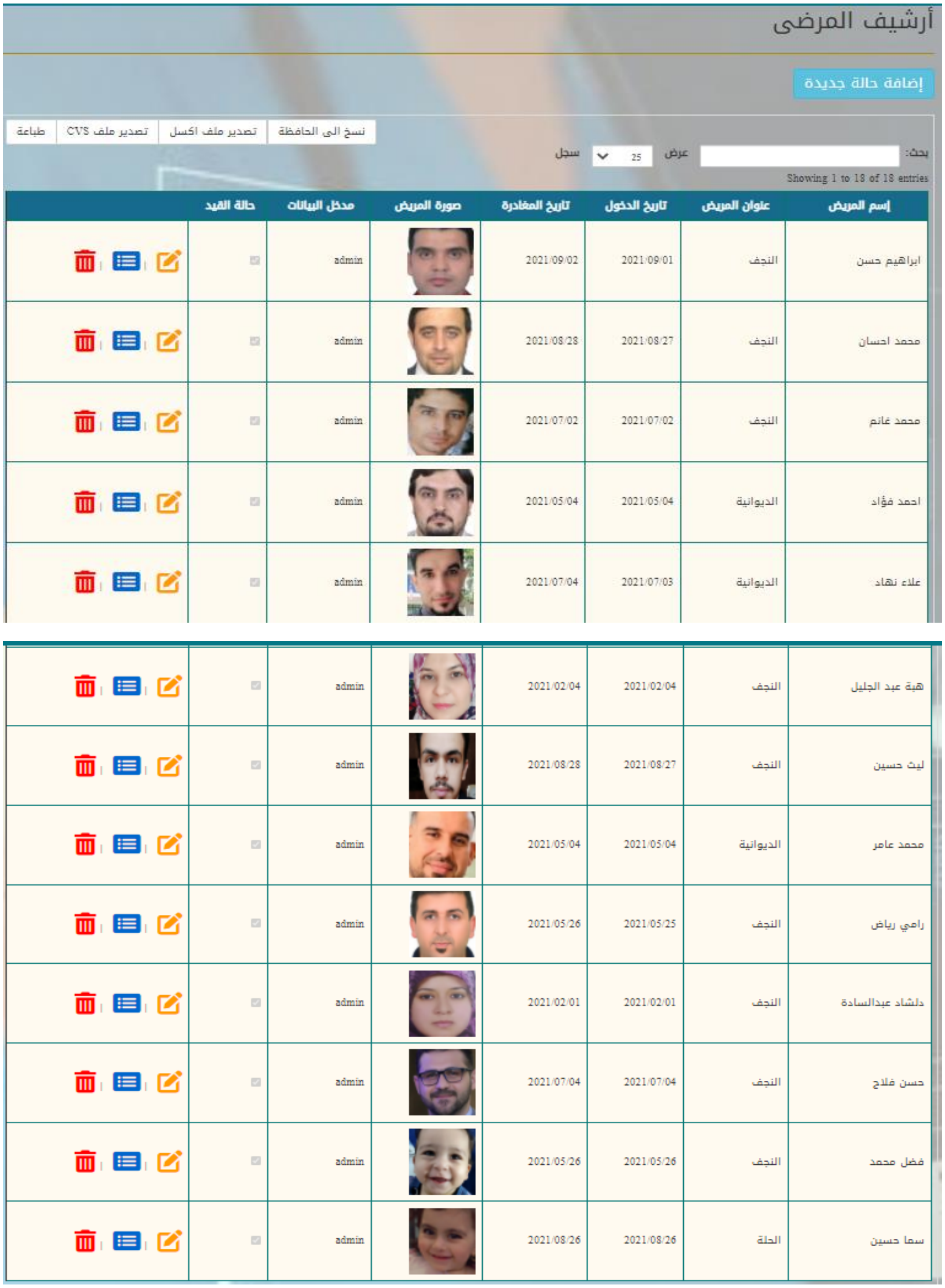
هل انت متأكد من عملية حذف البيانات؟

بطاقة معلومات المريض

إسم المريض وصورته	فضل محمد
عنوان المريض	النجف
تاريخ الدخول	2021/05/04
تاريخ المغادرة	2021/05/04
مسار صورة المريض	png.فضل محمد\PatientsImg\
مدخل البيانات	admin
تاريخ الاضافة	AM 1:31:53 9/4/2021
اخر تحديث بواسطة	
تاريخ اخر تحديث	
حالة القيد	☐

Figure (4.18): The confirmation of deleting information

Finally, all this process makes for 20 people to make the database to check it to search for information. Figure (4.19) View a sample from the archive.



أرشيف المرضى

Showing 1 to 18 of 18 entries

إسم المريض	عنوان المريض	تاريخ الدخول	تاريخ المغادرة	صورة المريض	مدخل البيانات	حالة القيد	
ابراهيم حسن	النجف	2021/09/01	2021/09/02		admin	☑	
محمد احسان	النجف	2021/08/27	2021/08/28		admin	☑	
محمد غانم	النجف	2021/07/02	2021/07/02		admin	☑	
احمد فؤاد	الديوانية	2021/05/04	2021/05/04		admin	☑	
علاء نهاد	الديوانية	2021/07/03	2021/07/04		admin	☑	
هبة عبد الجليل	النجف	2021/02/04	2021/02/04		admin	☑	
ليث حسين	النجف	2021/08/27	2021/08/28		admin	☑	
محمد عامر	الديوانية	2021/05/04	2021/05/04		admin	☑	
رامي رياض	النجف	2021/05/25	2021/05/26		admin	☑	
دلشاد عبدالسادة	النجف	2021/02/01	2021/02/01		admin	☑	
حسن فلاح	النجف	2021/07/04	2021/07/04		admin	☑	
فضل محمد	النجف	2021/05/26	2021/05/26		admin	☑	
سما حسين	الحلة	2021/08/26	2021/08/26		admin	☑	

Figure (4.19): Sample from the archive

In the case of searching for a specific case, suppose searching on the patient's full name (the triple name) the patient's name appears with his picture as shown in figure (4.20). Still, in the case of searching for a name only without mentioning his full name, all results bearing this name will appear, as shown in Figure (4.21).

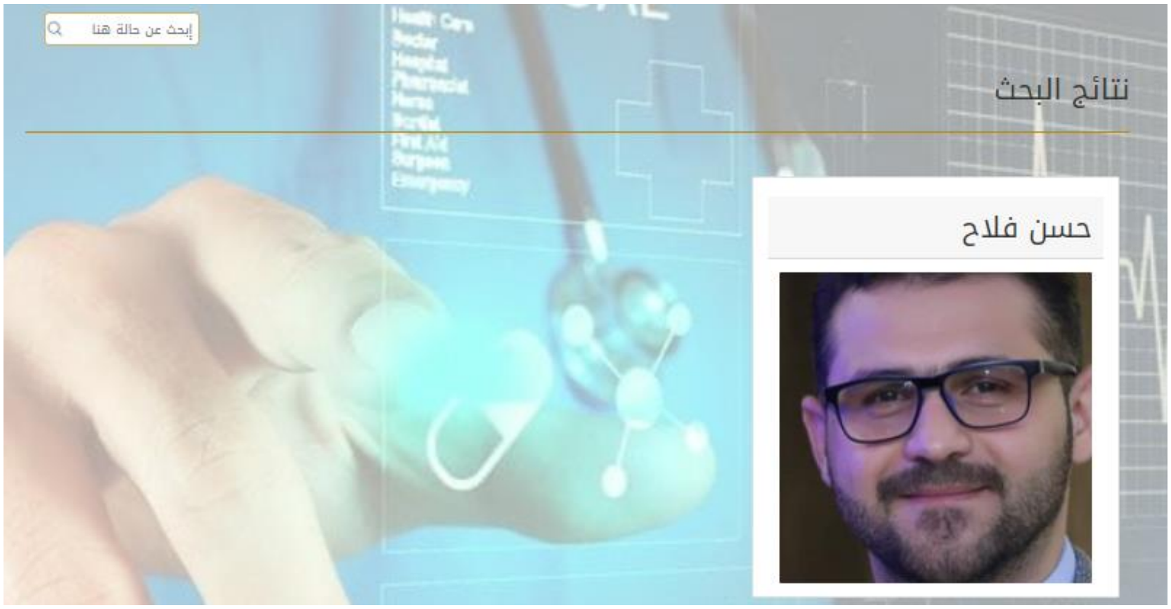


Figure (4.20): Search about Hasan Falah name

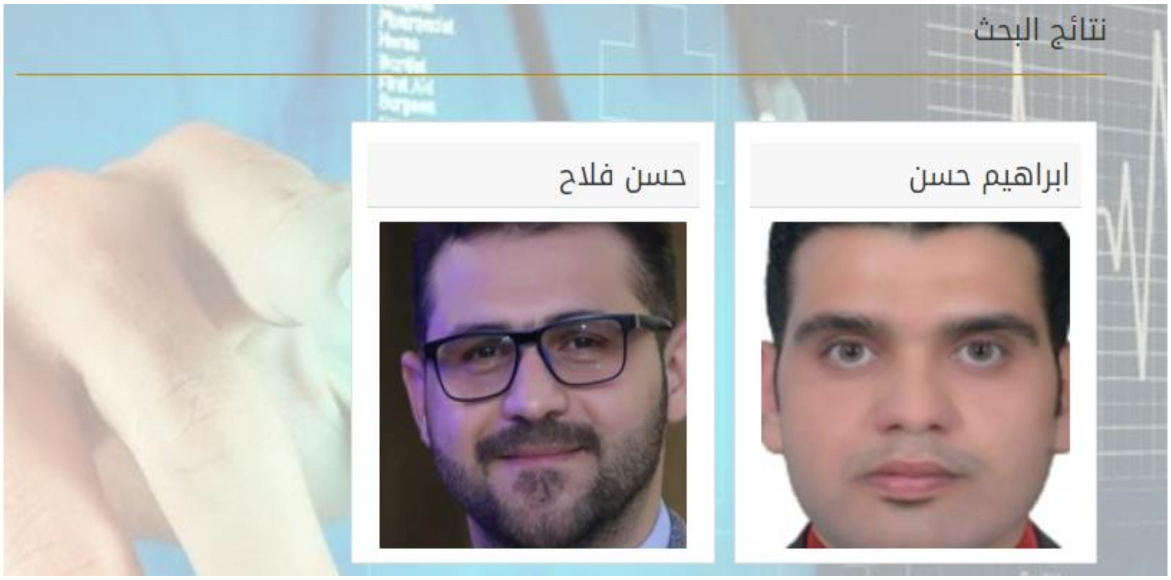


Figure (4.21): Search about Hasan name only

4.4 System's Quality

As shown in the previous chapter, the proposed system has high durability due to the combination of steganography and cryptography technologies. The system's strength lies in the encryption method, which is at a high level of confidentiality and does not affect the quality of the image, so it is not possible to distinguish between the encrypted image and the original image by the human visual perception system.

Suppose someone knows about the secret information inside the image and tries to access it. In that case, he must go beyond four levels of protection: the first level is the logistic map and its roots that require accuracy in its generation. The second level is represented by the 2D-cubic spline interpolation used for the first time in this work which performs a pseudo-random distribution of the embedding locations within the image. The third level is the binary data and its encryption; Finally, he must find the length of the data encoded through the images, on which the size of the logistic map depends.

In this section, the test of the system and the encryption algorithm under multiple noise systems produce to know the strength and robustness of the algorithm. Different attacks (Gaussian, salt and pepper, Poisson, and spackle) are applied on these cases studies of cover images, and performance parameters are measured to check the system's quality.

In the first case, the performance parameters are checked for all images at no attack in Table (4.3).

Table (4.3): The performance parameters of images at no attack.

Type of image	SSIM	SNR(dB)	MSE	PSNR(dB)	BER	RMS
Fadl's image	0.9999	49.1358	0.0004	93.7582	0.0003	0.0213
Hasan's image	0.9999	51.009	0.0003	94.5613	0.00025	0.0181
Sama's image(png)	0.9999	50.2745	0.00042	91.004	0.00029	0.0205
Sama's image(jpg)	0.9999	50.4250	0.0003	91.801	0.00028	0.0196

4.4.1 Salt& Pepper Noise

A fault in the camera's sensor, a software failure, or a hardware malfunction during the capture or transmission of an image is the most common cause of Salt & Pepper noise. Table(4.4) show the effect of the salts and pepper's noise on the studies images.

Table(4.4): The effect of the salts and pepper's noise on the studies images.

Type of image	SSIM	SNR(dB)	MSE	PSNR(dB)	RATE	RMS
Fadl's image	0.9786	10.4976	0.0486	70.413	0.0005	0.2204
Hasan's image	0.97221	10.6385	0.04886	69.5605	0.00056	0.22106
Sama's image(png)	0.9832	11.6922	0.04372	67.798	0.0005	0.20911
Sama's image(jpg)	0.9864	11.9208	0.04284	68.273	0.00048	0.20700

4.4.2 Gaussian Noise

The Additive White Gaussian Noise (AWGN) effect on the four images, which is familiar to every communication channel, is shown in Table (4.5).

Table (4.5): The effect of Gaussian noise on studies images.

Type of image	SSIM	SNR(dB)	MSE	PSNR(dB)	RATE	RMS
Fadl's image	0.9999	43.6324	0.0034	83.6115	0.0025	0.0589
Hasan's image	0.9999	43.6624	0.0036	82.5341	0.0027	0.0604
Sama's image(png)	0.9999	43.488	0.0038	80.018	0.0028	0.0616
Sama's image(jpg)	0.9999	43.4509	0.00382	80.3508	0.0028	0.0618

4.4.3 Poisson Noise

Table (4.6) shows the effect of the Poisson noise, which is caused by the quantitative nature of light and the autonomy of photon detections, and it is intrinsic to the measurement of light.

Table (4.6): The effect of Poisson noise on studies images

Type of image	SSIM	SNR(dB)	MSE	PSNR(dB)	RATE	RMS
Fadl's image	0.8240	2.9234	14.079	42.0708	0.34659	3.7522
Hasan's image	0.8362	4.35499	11.9825	42.05018	0.34841	3.46158
Sama's image(png)	0.8851	4.36001	12.2622	39.6167	0.34781	3.5017
Sama's image(jpg)	0.9096	4.2622	12.434	39.9204	0.3452	3.5262

4.4.4 Speckle Noise

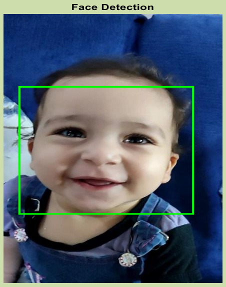
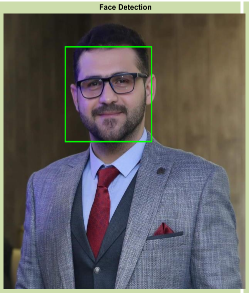
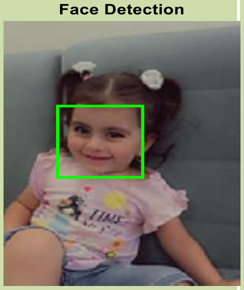
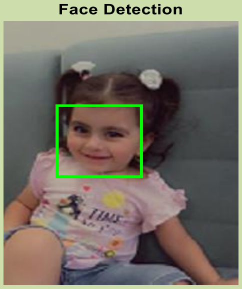
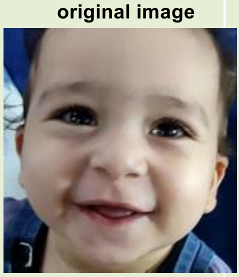
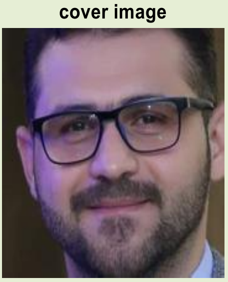
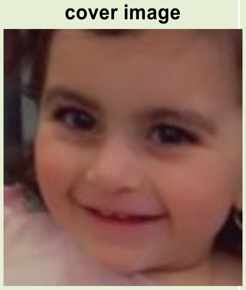
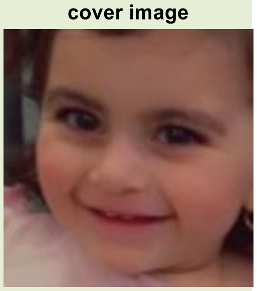
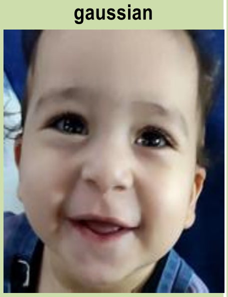
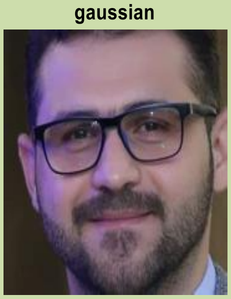
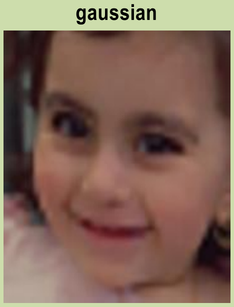
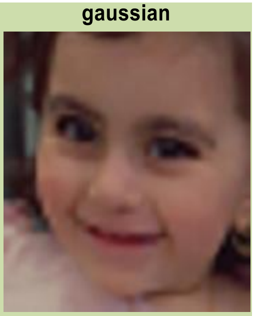
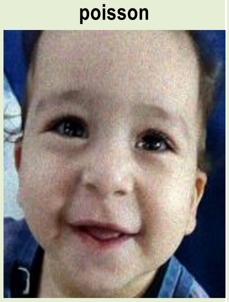
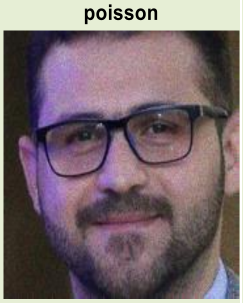
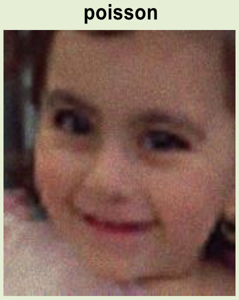
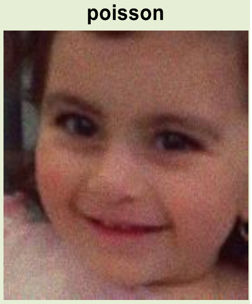
The dispersion of electromagnetic waves induced by the transducer, pictures of this form of noise has a granular pattern. When waves reflected on a rough texture interact with that texture, interferences are created, resulting in noise in the registered image. Table (4.7) show the effect of the Speckle noise on the images.

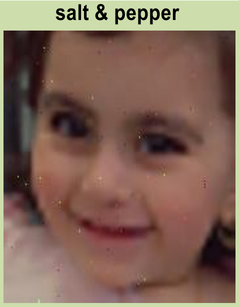
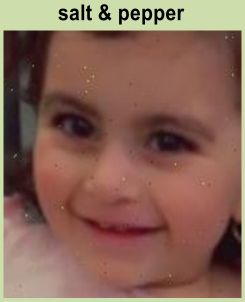
Table (4.7): The effect of Speckle noise on studies images.

Type of image	SSIM	SNR(dB)	MSE	PSNR(dB)	RATE	RMS
Fadl's image	0.9999	46.5577	0.00086	90.5430	0.0013	0.0294
Hasan's image	0.9999	62.1706	0.00003	105.8701	0.00003	0.0059
Sama's image(png)	0.9999	50.2745	0.00001	95.004	0.00001	0.00002
Sama's image(jpg)	1	50. 720	0.00001	96.004	0.00001	0.00001

The effect of attacks (Gaussian, salt and pepper, Poisson, and spackle) on the cover images are shown in Table (4.8), which represents four images (Fadl's image of 561*941 dimension with PNG format, Hasan's image of 1523*1541 dimension, and JPG format, and 200*267 sizes with PNG and JPEG formats).

Table(4.8): The effect of attacks on the images

Image Attack	Fadl's image	Hasan's image	Sama's image(png)	Sama's image(jpg
Face Detection				
Original image				
Gaussian noise				
Poisson noise				

Salt& pepper noise				
Speckle noise				

As noted that the program resizes the image to 180*180 resolution and processes it in the encryption system to check the system's quality under different attacks. The measuring of the performance parameters of the image **(Fadl Mohamed)** has PSNR reach to 93.7582dB at no attack and decrease slightly in speckle to reach 90.543 dB and so on to get 42.0708 dB in the Poisson attack.

In the image **(Hassan Falah Mohsen),** the values of PSNR reach 94.561dB at no attack and decrease slightly to get 42.05 in the Poisson attack, but in speckle-noise, the value of PSNR jump to 105.871dB because of the quality of this image where it has high resolution.

The third case is taking **(Sama Hussain Ali)** child image, low resolution with 120 KB (122,880 bytes), and 200*267 dimensions with PNG and JPEG format. The program resizes it to 180*180 resolution and processes it in the encryption system to check the system's quality under different attacks(Gaussian, salt and pepper, Poisson, and spackle). The same image is used with some accuracy, but with two different extensions (JPEG and PNG), encrypting and uploading operations are performed to the images. Then, the encrypted data was extracted.

But the bit error rate ranges from (0.0001 to 0.348) in Poisson noise; this value is minimal to affect the images, so the image still keeps its quality and robustness to attacks. All images after encryption are uploaded to the webserver to archive them in the central database. Some information such as date entry and leaving of the patient is recorded in the webserver to search the patient in the database. The data that encrypts in the cover image(patient file information) is extracted correctly after uploading it on the webserver and downloading it to the admin computer who has the decryption system to decrypt the image extract the data if needed.

The main idea is to test the efficiency of the system. Whether the images are from an extension JPEG or an extension PNG, and what are the results will change, but what have noticed is that the results vary with very few values that are almost impossible to take into account while maintaining the efficiency and strength of the system, where the image is read with a JPEG extension. The data is encrypted through operations, and algorithms encryption is then converted into a PNG image to eliminate data loss and losses that characterize the extended image. With this conversion and comparison between the values, finds that the efficiency of the system is very high and that the type of extension does not significantly affect the image

4.5 Discussion of The Result

The proposed algorithm interphase the pixel position of the host (cover)image using 2D-cubic spline interpolation and embedded information using the (LSB) technique in the eight binary planes of the green color from covers images. The proposed steganography algorithm is effective and proves to be resistant to various attacks. The result that gets can summarize in some points

1- The proposed algorithm consists of three sub-algorithms; chaotic algorithm, 2D- cubic spline interpolation algorithm, and the least robust algorithm.

2- The system operates on the color image. Green and red colors are used to encrypt some information to protect them from authorized people.

3- The main idea of generating two-dimension cubic spline interpolation is to specify the locations of the host media that encrypt the information in it and not only develop the sequence but encrypt the data with it.

4- The concatenations of the logistic map and 2D-cubic spline interpolation make the encryption system operates at high security to protect the data.

5- Since the archiving of patient files that not been used in the Iraq hospital yet, this proposed system gives the basics of archiving data with high security.

6- The system's robustness and effectiveness tests are made with different image attacks such as Gaussian, salt& pepper, poison, and speckle. The results in Table (4.3), Table (4.4), Table (4.5), Table

(4.6), Table (4.7), and Table (4.8) show the high robustness and quality of reconstructing the Data hiding.

7- All patient information is uploaded to the web and can reach from any other place. This step aims to store the data in the central computer.

8- The system works well and gives high confidence for the patient information.

9- Archiving and storing data on the Internet provides sufficient protection to eliminate the enormous amount of archiving paper data that can cause damage, loss, fire, and other harmful factors; it also provides storage space on the ground.

10- The information is fully protected by encrypting it and saving it in the personal image, and not allowing access to it or manipulating it, especially when people's lives are threatening in all forms.

11- Working with the system does not require time, paper, and equipment that causes losses due to its frequent use, especially the availability of computers and the Internet in all hospital corners. What is needed only is the camera that adds to take a picture of the patient. Therefore, the program designs to work on the computer.

12- The program has been converted into an application that installs on the computer without the need to install the Matlab program, where the program calls the Matlab environment (the virtual environment) directly from the Matlab website to perform all the required operations, and this saves a lot of storage space in addition to speed and accuracy.

13- The program works on both types of images alike (PNG and JPEG) with high efficiency. Using two format images, the encrypted data is extracted with very high efficiency after testing it on different attacks.

14- The program works on various types of imaging accuracy; whether it is high, medium, or weak precision, the result is the system's efficiency in encryption, data upload to the database, and decryption to extract the encrypted data in an excellent and high capacity.

15- There is a system currently operating in (Al-Adala Dispensary and Al-Numan Health Center) only in Najaf as a whole. The idea of the system is the (Health Visitor), which contains a complete file in the name of the head of the family having the information of individuals, and one of the officials enters the patient's data and transfers it from one doctor to another or directs it to the treating doctor depends on his health condition that requires treatment. Still, the system lacks images and data. They are not encrypted but are uploaded as they are to the central computer, and this causes an increase in the capacity of the uploaded data and thus requires additional volumes to store them. This matter was overcome in the proposed system, which has the novility of using the 2D-cubic spline algorithm for encrypting the data and using just the image capacity without needing the other space for patient information.

Chapter Five

CHAPTER FIVE
RESULTS OF PRACTICAL APPLICATION (FIELD IMPLEMENTATION)

5.1 Introduction

In this chapter, the practical field application of the program is proposed to see its practicality, response to work, and the extent to which patients and people respond to it.

It was supposed to manufacture a device consisting of a Panda-type microcomputer with the camera connected and programmed to install Windows 10 with Matlab to make a lightweight, portable computer, but the idea of manufacturing was dispensed with due to the presence of the movable and light tablet with more capabilities and a suitable design and a camera that meets the requirements of the program

To shorten the time that used to complete the manufacturing model and the expenses necessary to complete the appropriate model in terms of design, shape, and all the features needed for that, the application is installed on a Lenovo ThinkPad tablet with processor intel(R) Core(TM)-m7-6y75 CPU@1.2GHz of the 64-bit operating system for ease of work and implementation of the program with high efficiency.

The application is held in one of the health centers (Al-Nu'man health centers) of the Najaf governorate in Al-Hirah district (Al-Nu'man district), which is the second place after Al-Adala Health Center (located in Al-Adala district in Al-Najaf Al-Ashraf), which contains the health visitor program, but unfortunately, the installation and work was not completed for specific reasons

The previous visits were as follows: The first visit to Al-Adala health center, which found a response from the responsible gentlemen, especially Mr. Hussam Ajeel, who gave a detailed explanation of the health visitor program and how it works.

Then the second visit is to Al-Munadhera General Hospital with a book (facilitating the task of the postgraduate student), which welcomed, but unfortunately could not implement it because of the refusal of those accompanying patients to take pictures and patient information for a study application, as they say

The third visit was to Al Nu'man health center, as in the following parts of this chapter.

5.2 Al Adala Health Center

Meeting with Mr. Hussam Ajeel, who explained the health visitor program to us. Most of the courses related to teaching the health visitor program are held in it so far (I don't know the purpose, Including that the program was not completed in a health center and has not been implemented!) As mentioned earlier, the first visit was to the Adalah neighborhood clinic, located 5 km from the center of the Najaf Governorate.

When you open the application, the window opens as in figure(5.1). The window that consists of several pages opens, and according to the type of the person referred, is he from the city center or the parties or the displaced. You can choose one of these icons mentioned in it.

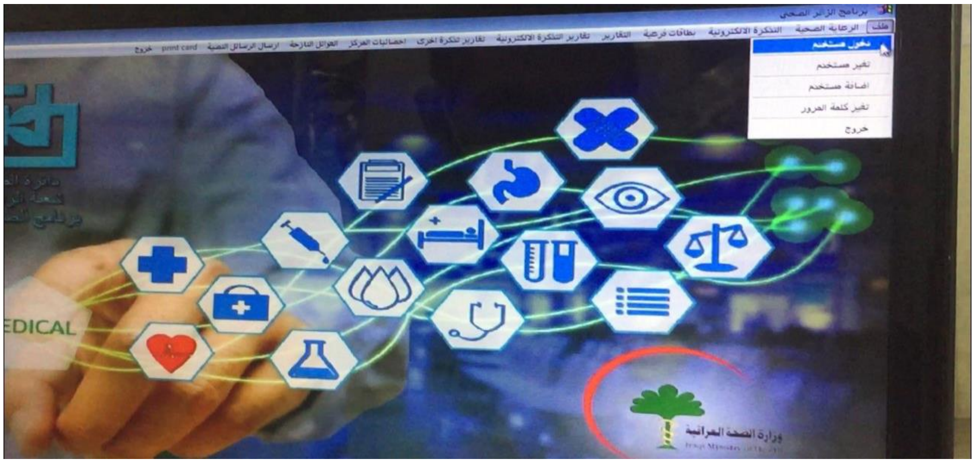


Figure (5.1): The health visitor program page

By choosing the type of user, the program asks for the user name and password. Here entered in the name of the director of the center (Master).

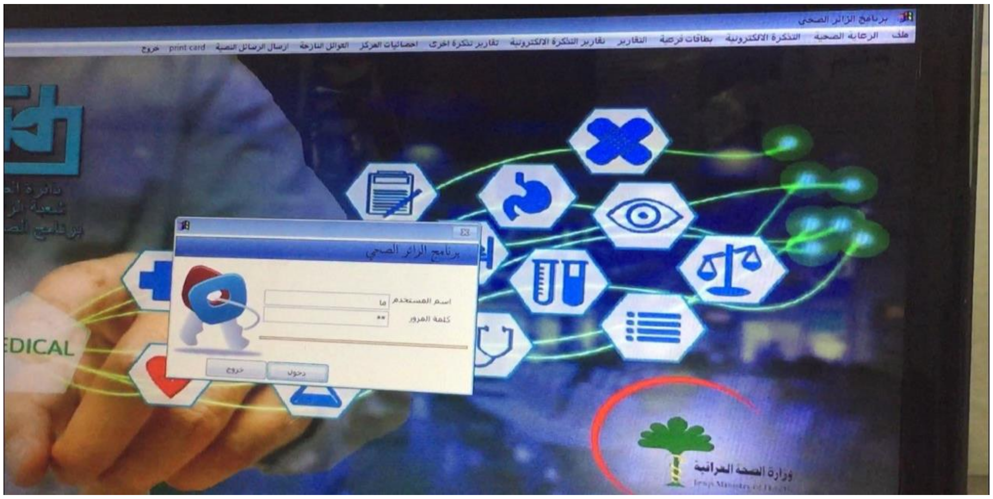
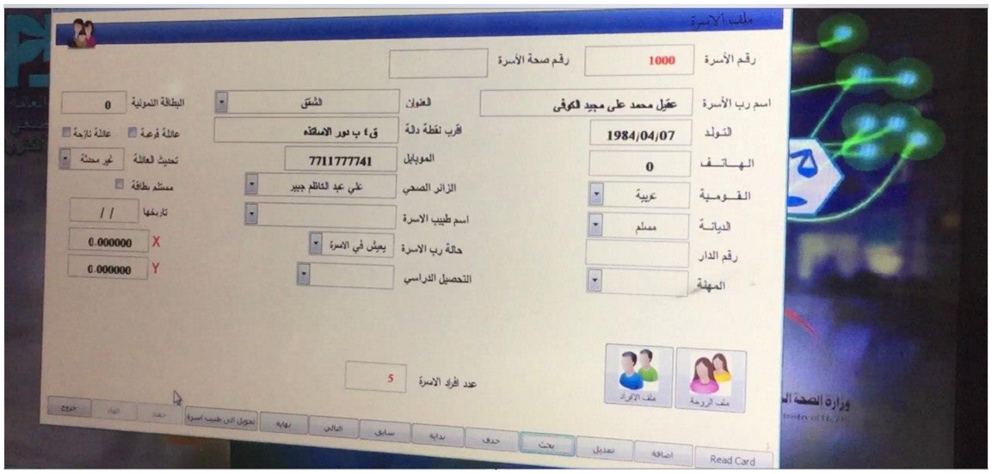


Figure (5.2): Entering as a master user in the health visitor program page

At first, the ticket is cut from the person in charge when the patient enters, and he is transferred electronically to the rest of the private rooms for review. The window that consists of several pages is opened, and on all the computers connected in this network according to the type and age of the patient, and in the case of being a child, he is referred to the Vaccine

Division and so on. In family medicine or the health visitor program, each family has a complete file containing the family's details, the number of individuals, and names, as in figure (5.3).

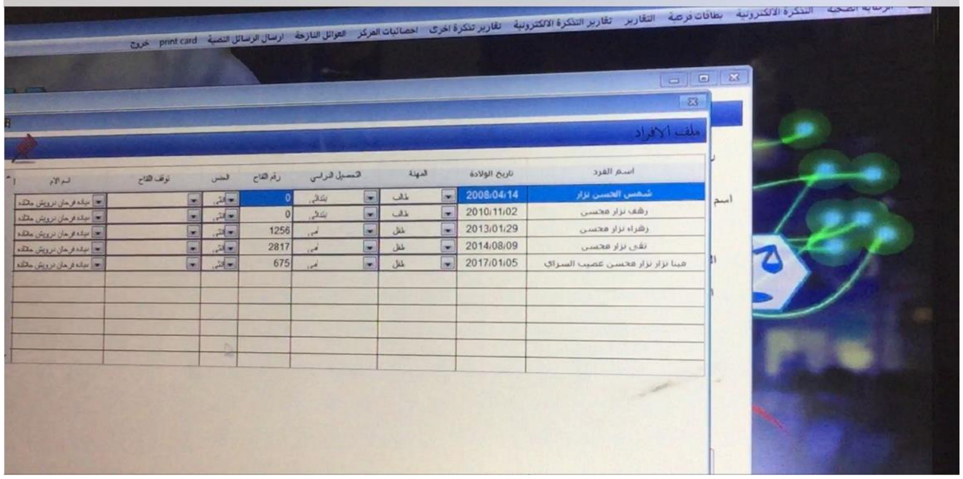


رقم الأسرة 1000
رقم صحة الأسرة
اسم رب الأسرة عقيل محمد على مجيد الكوفى
التولد 1984/04/07
الهاتف 0
القومية عربية
الديانة مسلم
رقم الدار
المهنة
العنوان الشقق
اقرب نقطة دالة ق ٤ ب دور الاساتذه
الموبايل 7711777741
الزائر الصحي علي عبد الكاظم جبير
اسم طبيب الاسرة
حالة رب الاسرة يعيش في الاسرة
التحصيل الدراسي
البطاقة التموينية 0
□ عائلة فرعية □ عائلة نازحة
تحديث العائلة غير محدثة
□ مستلم بطاقة
تاريخها / /
X 0.000000
Y 0.000000
عدد افراد الاسرة 5

Figure(5.3): The family file on the health visitor program page

The person concerned can be searched by his name, family name, or family number, and all his information can be extracted. Archiving and storing data in the database is done in the central calculator and the health center manager's computer, as in figure (5.4).

After the health file is completed and the patient is left, the file is closed, and the entire data is uploaded to the central computer located in the Najaf Health Directorate.



اسم الام	توقف اللقاح	الجنس	رقم اللقاح	التحصيل الدراسي	المهنة	تاريخ الولادة	اسم الفرد
نبيله فرحان درويش مالك		أنثى	0	ابتدائي	طالب	2008/04/14	شمس الحسن نزار
نبيله فرحان درويش مالك		أنثى	0	ابتدائي	طالب	2010/11/02	رهف نزار محسن
نبيله فرحان درويش مالك		أنثى	1256	أمي	طفل	2013/01/29	زهراء نزار محسن
نبيله فرحان درويش مالك		أنثى	2817	أمي	طفل	2014/08/09	تقى نزار محسن
نبيله فرحان درويش مالك		أنثى	675	أمي	طفل	2017/01/05	ميا نزار نزار محسن عصيب السراي

Figure (5.4): Family Database file in the health visitor program page

5.2.1.Problems with the Health Visitor Program

When asking some employees about the program and the problems they encounter while working, their answer was as follows:

1. The program works entirely on the Internet, so the Internet must be constantly available in the center

2. The lack of adequate protection for patient information, as everyone who has access to the program can view it

3. The program does not contain pictures of patients, only information and complete details, so sometimes it faces a problem in the similarity of names if the employee does not enter the triple or quadruple name in some cases to open the family file.

5.3 Application in Al Nu'man Health Center

The dispensary is located in the district of Al-Manadhera in the community of Al-Hirah in the Al-Nu'man neighborhood concerning which is approximately 20 kilometers from the center of the Najaf governorate, which is the second center in the region where it was established in the year 2006 as in the Figure (5.5).

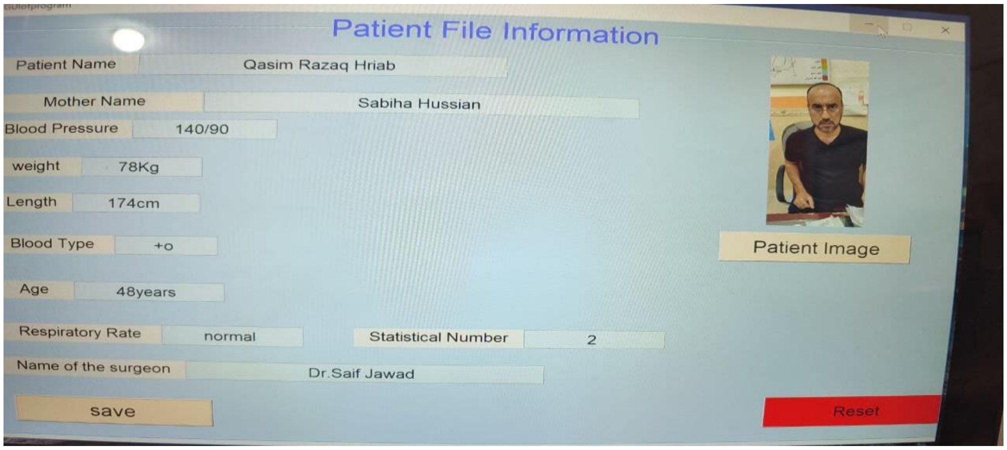
Figure (5.5): Al-Nu'man Health Center

After entering it and meeting with the director of the center, Dr. Saif Jawad, who welcomed us and gave us permission to take pictures of the archive room and roam in the center and take the picture needed with the application. Here are some snapshots from the archive room

Figure(5.6): Some snapshots from the archive room

Figure(5.7): Some snapshots from the archive room

The program will implement in the health center with the help of two people as experimental samples of the program to see how well the laboratory work matches the actual work.



Patient File Information

Patient Name: Qasim Razaq Hriab

Mother Name: Sabiha Hussian

Blood Pressure: 140/90

weight: 78Kg

Length: 174cm

Blood Type: +o

Age: 48years

Respiratory Rate: normal

Statistical Number: 2

Name of the surgeon: Dr.Saif Jawad

Figure (5.8): Implement our program on the first donor, which is Mr. Qasim

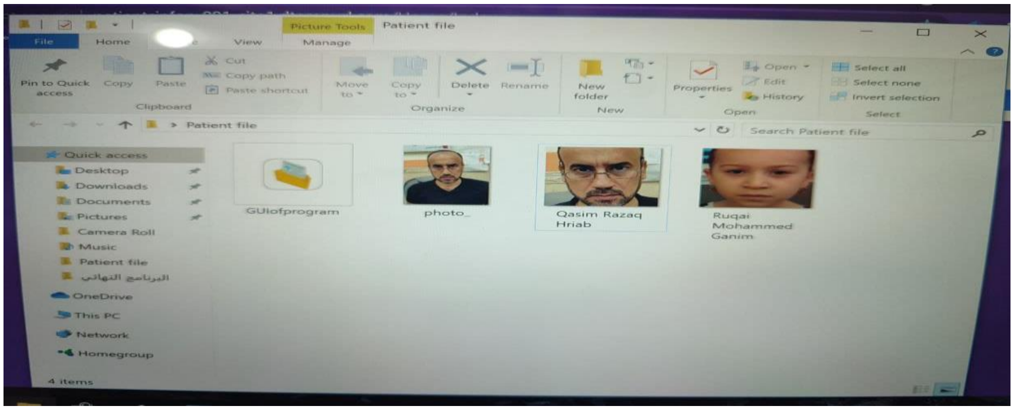
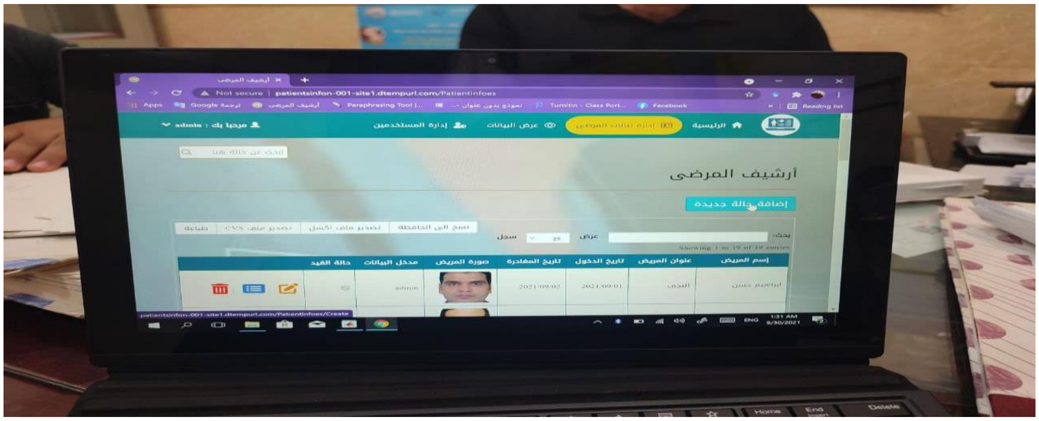


Figure (5.9): Save the picture after encryption the information

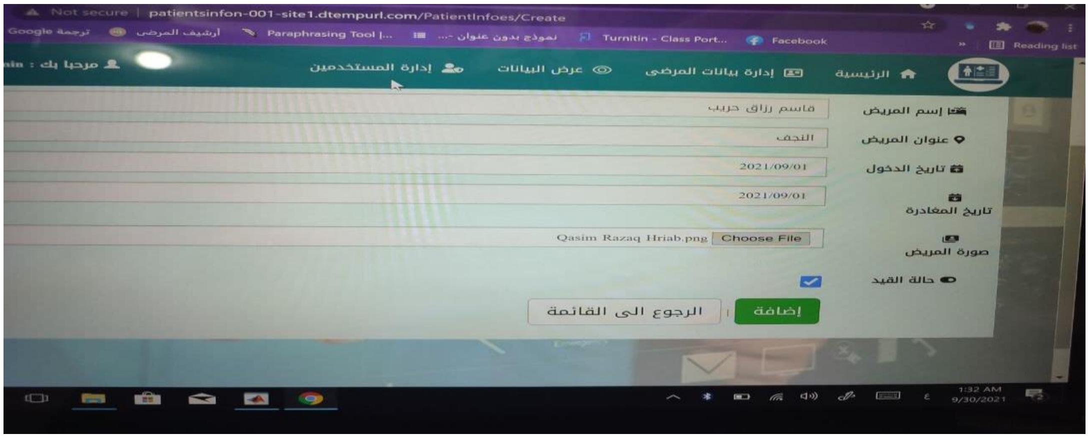


أرشيف المرضى

patientsinfon-001-site1.dtempurl.com/Patientinfoes

إسم المريض	عنوان المريض	تاريخ الدخول	تاريخ المغادرة	صورة المريض	مدخل البيانات	حالة القيد
ابراهيم حسن	النجف	2021/09/01	2021/09/02		admin	

Figure (5.10): The moment the image was added to electronic archiving



إسم المريض: قاسم رزاق حريب

عنوان المريض: النجف

تاريخ الدخول: 2021/09/01

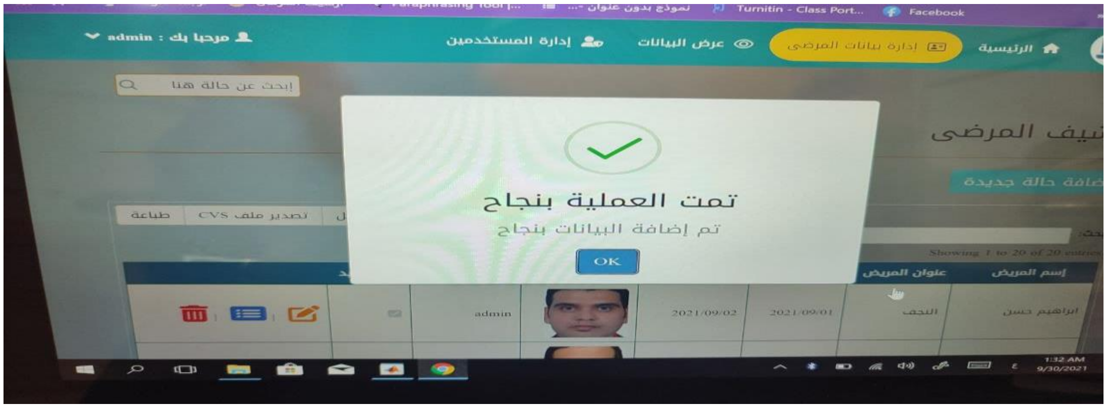
تاريخ المغادرة: 2021/09/01

صورة المريض: Choose File Qasim Razaq Hriab.png

حالة القيد: ☑

إضافة | الرجوع الى القائمة

Figure (5.11): Entering the information needed in an electronic archive



تمت العملية بنجاح

تم إضافة البيانات بنجاح

OK

إسم المريض	عنوان المريض				
ابراهيم حسن	النجف	2021/09/01	2021/09/02		admin

Figure (5.12): Complete the process of uploading the information

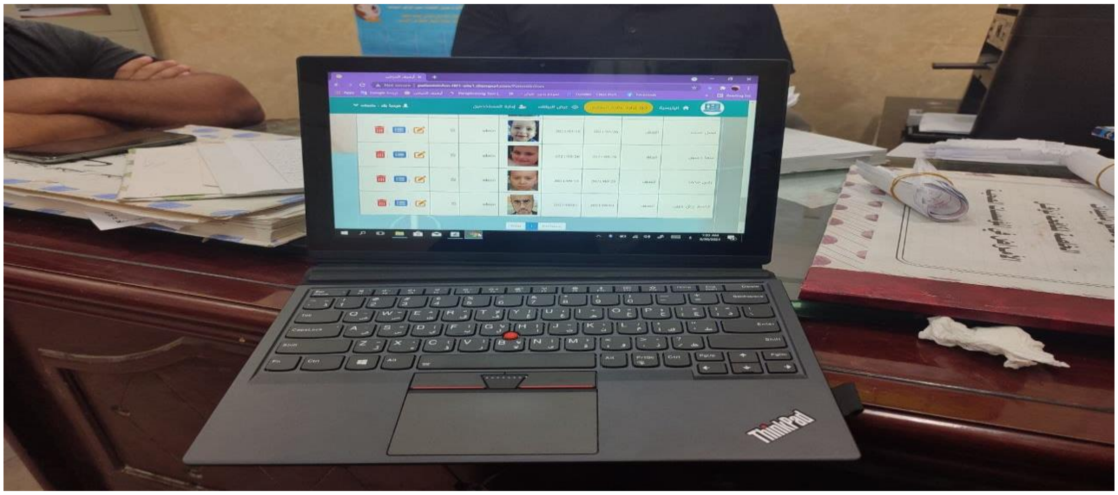
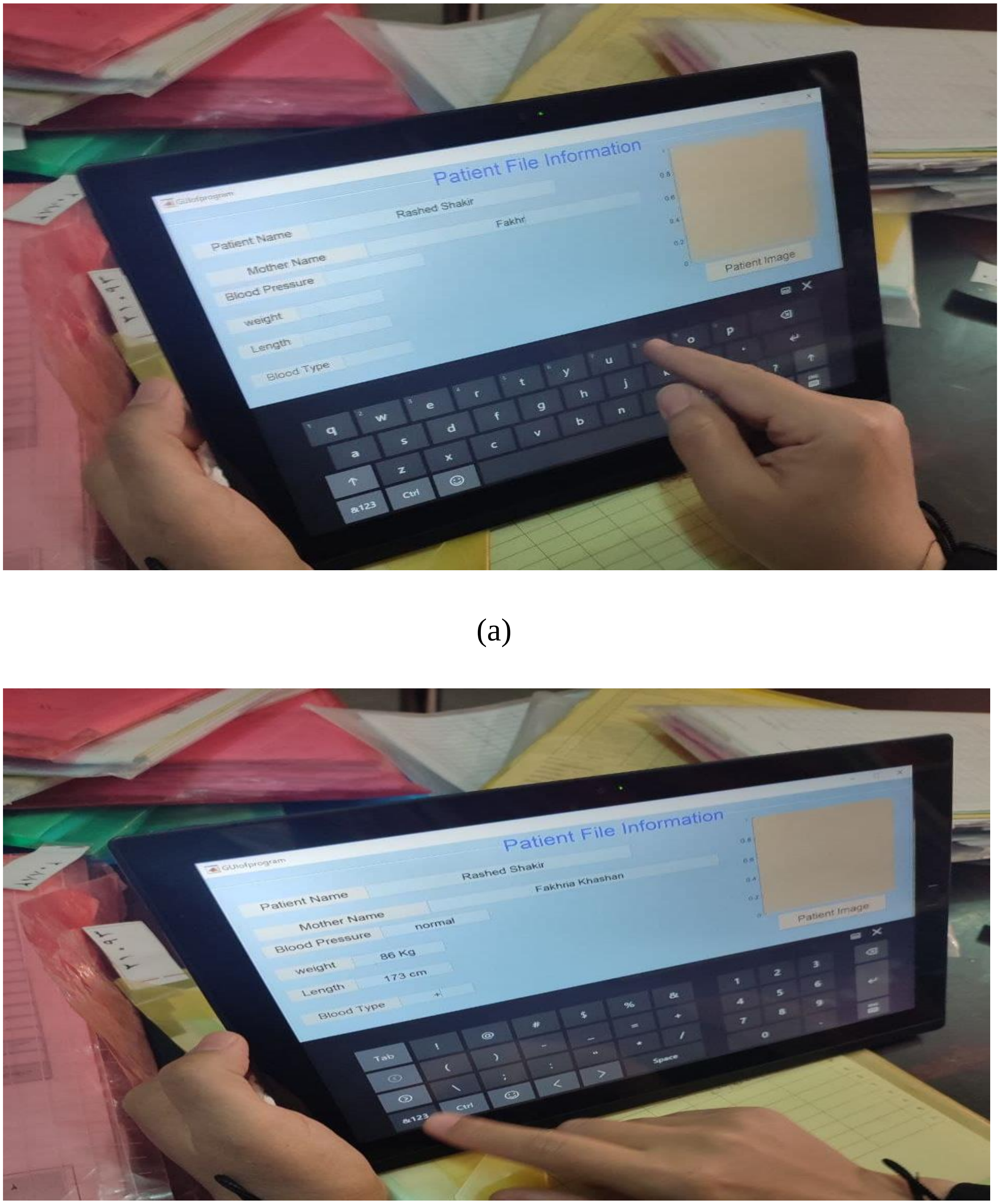


Figure (5.13): The image saving in the database of the webserver

The second person is Mr. Rashid Shaker.



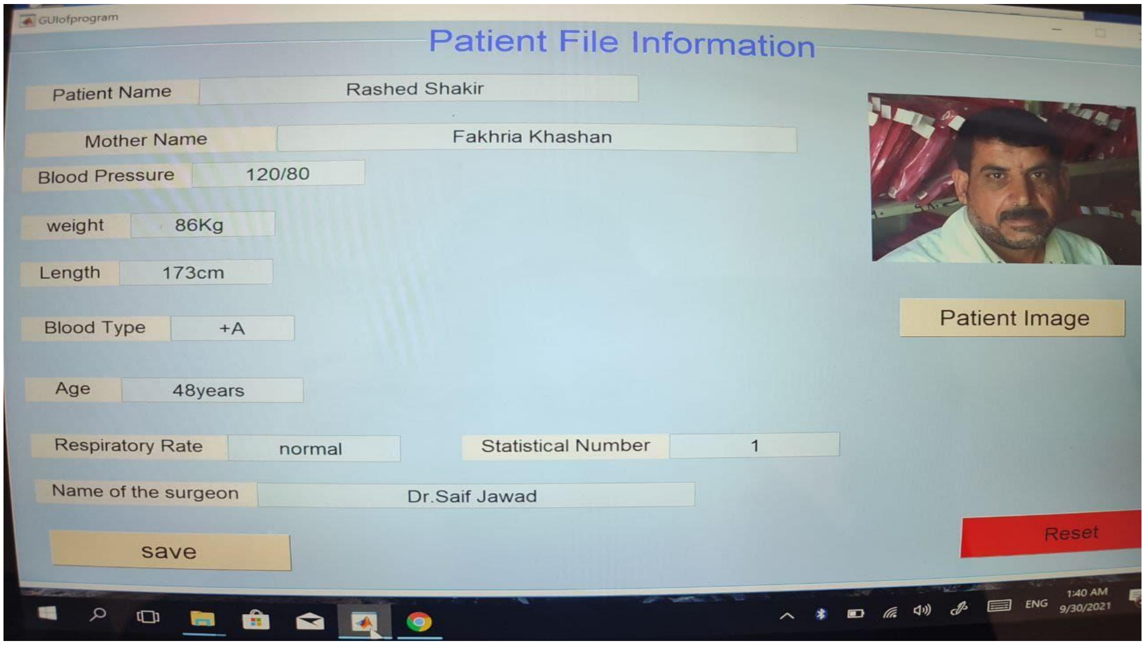
Patient Name Rashed Shakir
Mother Name Fakhr
Blood Pressure
weight
Length
Blood Type

(a)

Patient Name Rashed Shakir
Mother Name Fakhria Khashan
Blood Pressure normal
weight 86 Kg
Length 173 cm
Blood Type +

(b)

Figure (5.14): The moment of entering information of Mr. Rasheed Shaker



Patient File Information

Patient Name	Rashed Shakir
Mother Name	Fakhria Khashan
Blood Pressure	120/80
weight	86Kg
Length	173cm
Blood Type	+A
Age	48years
Respiratory Rate	normal
Statistical Number	1
Name of the surgeon	Dr.Saif Jawad

Figure (5.15): Complete of entering information of Mr. Rasheed Shaker

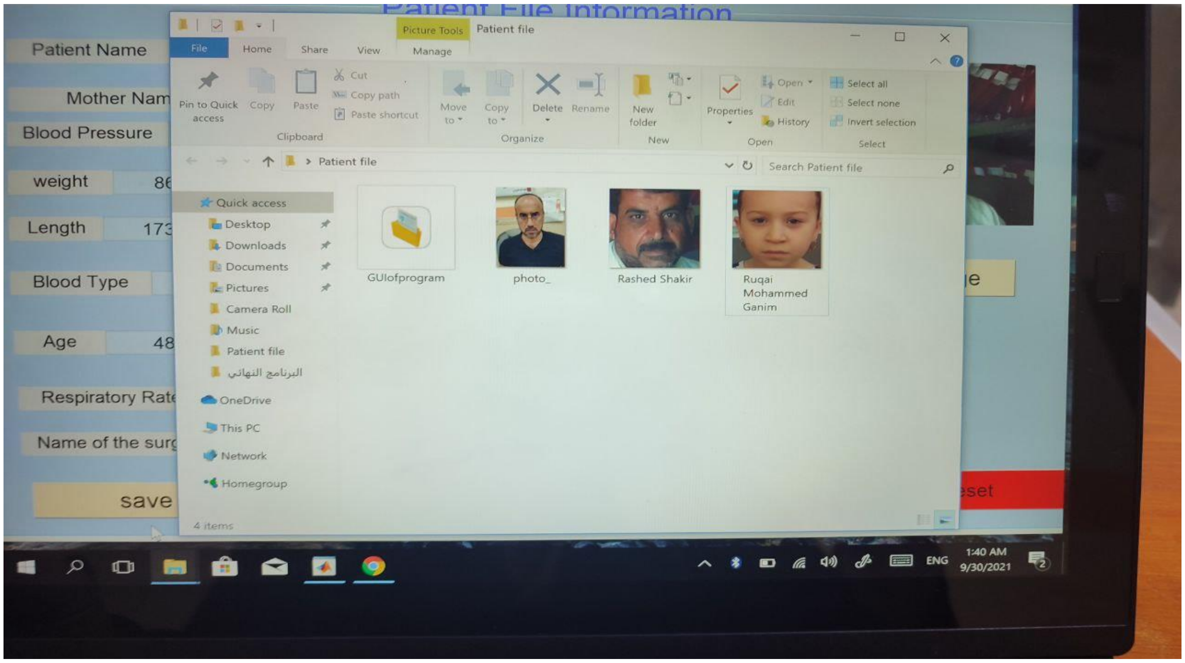
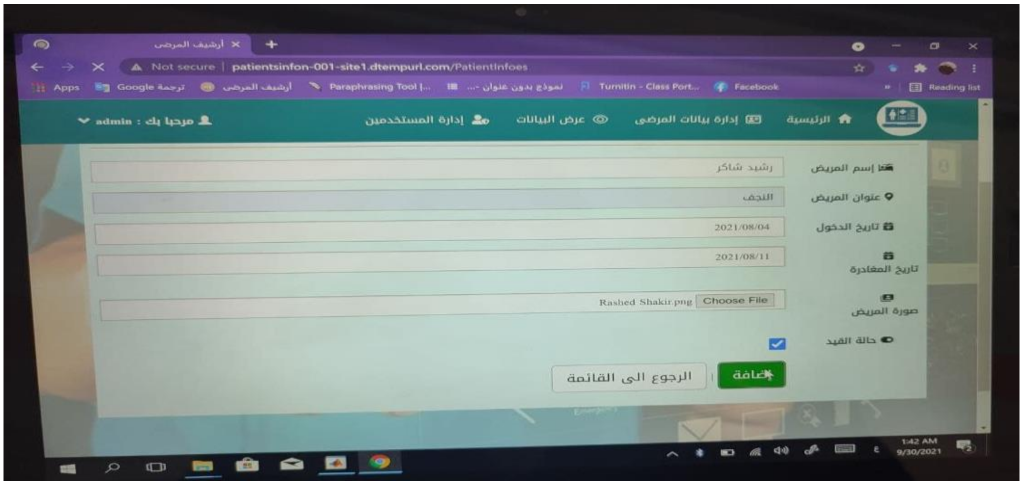


Figure (5.16): Save the image after encrypting the information in it



إسم المريض: رشيد شاكر

عنوان المريض: النجف

تاريخ الدخول: 2021/08/04

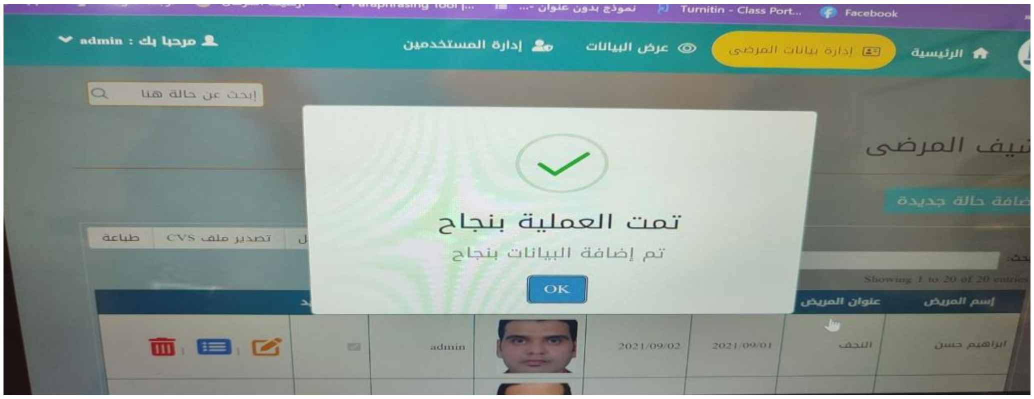
تاريخ المغادرة: 2021/08/11

صورة المريض: Choose File Rashed Shakir.png

حالة القيد: ☑

إضافة | الرجوع الى القائمة

Figure (5.17): Uploading the information of Mr. Rasheed Shaker to the webserver

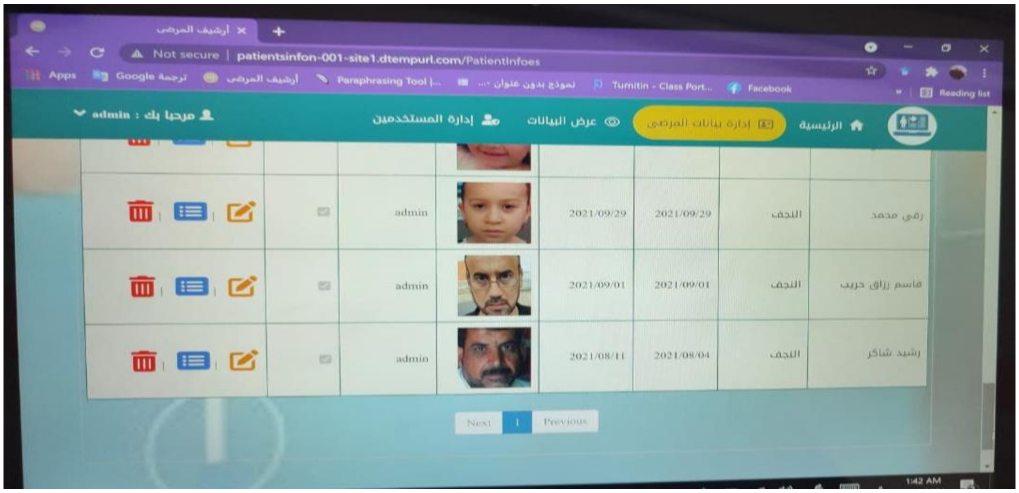


تمت العملية بنجاح

تم إضافة البيانات بنجاح

إسم المريض	عنوان المريض				
ابراهيم حسن	النجف	2021/09/01	2021/09/02		admin

Figure (5.18): Complete the uploading of the information to the webserver



رقي محمد	النجف	2021/09/29	2021/09/29		admin
قاسم رزاق حريب	النجف	2021/09/01	2021/09/01		admin
رشيد شاكر	النجف	2021/08/04	2021/08/11		admin

Figure (5.19): The uploading is complete and the image appear in the database

5.3.1 The Extraction of Data

When the admin needs to extract the patient's Data, he can download the image from the webserver and read it through the extraction program. For the cases of the above experiment, the steps of extracting information are as follows:

1-Download the images from the web and save as on the computer that contained the extraction program

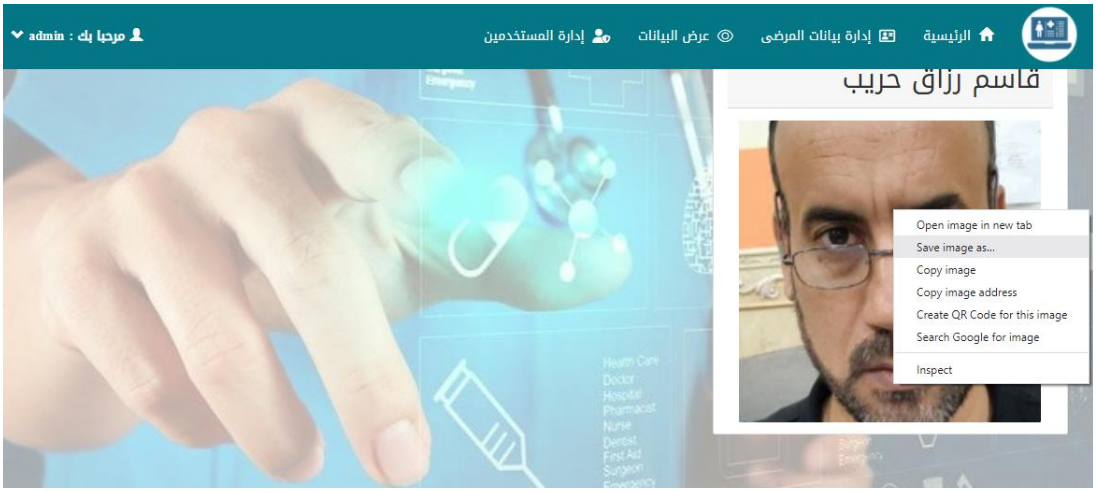


Figure (5.20): Downloading the first image from the database

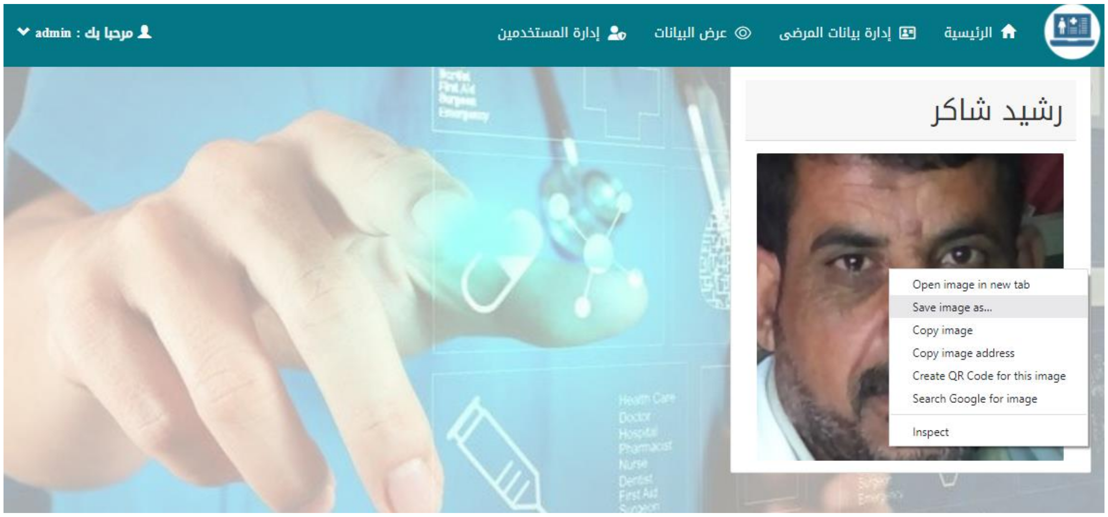


Figure (5.21): Downloading the second image from the database

2- Running the extraction program to read the image and extract the patient information from it.

3- finally, the data appear as text.

The patient's data of the first image, which is Mr.Qasim are as follows:

Patient mother name: Sabiha Hussian

Age: 48years

Blood pressure: 140/90

Blood type: +o

Weight: 78Kg

Length: 174cm

Respiratory rate: normal

Statistical number: 2

Name surgeon: Dr.Saif Jawad

The patient's data of the second image, which is for Mr.Rashid, are as follows

Patient mother name: Fakhria Khashan

Age: 48years

Blood pressure: 120/80

Blood type: +A

Weight: 86Kg

Length: 173cm

Respiratory rate: normal

Statistical number: 1

Name surgeon: Dr.Saif Jawad

5.4 Discussion of the Practical Application

Through the application at Al-Nu'man Health Center are noticed:

1. The program works very efficiently, as samples were taken and people's data was encrypted through their pictures and then uploaded to be archived in the online database.

2. The personal picture has been added, which distinguishes it from the health visitor program to eliminate the problem of similarity in names.

3. The protection available by encrypting patient information will give an essential feature in information security and safety.

4. The problem of data loss has been overcome in the absence of the Internet, as the program works on encryption and saves the patient's image in a particular file on the computer and saves the time of committing the image, which can be uploaded to the data for archiving at the time of the availability of the Internet in an hour of working hours

5. The use of the tablet provides a facility of movement and work, as the patient can take the picture anywhere he is without the need for him to sit in front of a specific computer and a particular position, and this gives complete freedom to the patient without being restricted to anything and according to his health status.

6. Working on the program and using it is an essential feature in the application to facilitate the work and use of the application from all categories in the health center.

5.5 Comparative between the patient's electronic medical record with the proposed system

This part reviews a general comparison between the systems used globally with the proposed system from several aspects

1. Quality: Ultimately, all systems may help care coordination. Making test findings more accessible to physicians and patients, identifying data gaps, and offering evidence-based preventative strategies may improve emergency treatment, save money, and increase prevention.

2. Time: The use of electronic patient files may speed up patient identification at the hospital. A study published in the Annals of Internal Medicine found a 66% reduction in time after its use (from 130 to 46 hours).

3. Weak software and usability: The Association for Health Care Information and Management Systems emphasized the inefficiency and complexity of moving stationary computers. Doctors are rapidly embracing tablet technologies, mainly as they utilize mobile devices to accomplish their work. Mobile devices may increasingly sync with EHR systems, enabling practitioners to view patient information remotely.

4. Threats to healthcare data: include three types; Human risks (employee Earthquakes, storms, and flames. System flaws, for instance, Dangers, might be internal or external. This suggested algorithm encrypts patient data before

uploading it to the cloud, adds an extra security layer, and looks up a person in the database yields no results.

Chapter Six

CHAPTER SIX
CONCLUSIONS AND FUTURE WORKS

6.1 Conclusions

It is expected that the electronic patient archiving system will add a solution to many of the problems faced in the electronic archiving system. The program converts the patient's information into a code using the logistic map. This information generated encrypts in different locations from the patient's image determined by the 2D-cubic spline interpolation to protect it and not allow unauthorized users to access that data. Finally, uploads this image to the webserver to be stored and archive this data electronically. From the implementation and testing of the proposed program can conclude:

1- Steganography is a new method of encryption by using 2D cubic spline interpolation, which is used for the first time in a steganographic encryption system. From the result, it considers as an excellent one.

2- The encryption process does not use the sequence to hide but uses the locations to hide in it.

3- Obtaining that high accuracy and security is done because the encryption process passes in two steps, one with a logistic map and the other using 2D-cubic spline interpolation.

4- The roots of cubic spline depend on length of cover image and patient file information, and these roots must choose to give specific points of cubic spline interpolation.

5- Process of choosing the locations point subject to some MODULES to give the exact point not more significant, not minor, the columns and rows of the cover image.

6- The difference in the length of the patient information does not affect the operation of the system.

7- The system works on two types of images, such as PNG and JPEG, with high efficiency.

8- The two stages of encryption (Logistic map and cubic interpolation) gave durability and strength against attacks.

9- The system saved a lot of storage space, especially that electronic archiving is stored on the webserver, so even a computer storage space does not take up.

10- Protection of data and information in the electronic archiving system concerning paper archiving gave high privacy to the patient to maintain his medical record

11- They are cost-reducing for materials of purchasing equipment and supplies for paper archiving such as records, containers, safes, and stores by a considerable amount because they are not needed.

12- Storing data and linking it to the Internet allows it to be used in different places and specialists to help understand the patient's medical record. Also protecting data from loss due to natural or industrial conditions such as fire, rain, humidity, earthquakes, and other factors that damage it if it is paper

13- Through the electronic system, it is possible to reduce typographical errors related to the patient's treatment due to the writing language of some doctors that are not understood by the pharmacist supervising the treatment, which leads to the dispensing of wrong therapies that may lead to the loss of the patient's life or complications in the slightest possibility

6.2 Future Work

1-Work expands the system to include all patient data such as x-rays, ultrasounds, examinations, surgeries, and treatments.

2-Making the system the primary system to work on in all health centers, especially at Internet development.

3-Connecting the health network with other state networks, such as the Ministry of Interior, defense, national card, passports, travel, and transportation, to be integrated e-government that carries all the essential information.

4- Make reservations and choose the right time electronically to upload a personal photo before the time of review.

5- Develop the proposed system as an application available for mobile (Android and ios) for more facilities.

References

REFERENCES

[1] M. Zamani, H. Taherdoost, A. a Manaf, R. B. Ahmad, and A. M. Zeki, “A Genetic-Algorithm-Based Approach for Audio Steganography,” *Int. J. Comput. Electr. Autom. Control Inf. Eng.*, vol. 3, no. 6, pp. 64–68, 2009.

[2] M. M. Hashim, M. S. Mohd Rahim, and A. A. Alwan, “A review and open issues of multifarious image steganography techniques in spatial domain,” *J. Theor. Appl. Inf. Technol.*, vol. 96, no. 4, pp. 956–977, 2018.

[3] A. Jalali and H. Farsi, “A new steganography algorithm based on video sparse representation,” *Multimed. Tools Appl.*, vol. 79, no. 3–4, pp. 1821–1846, 2020, doi: 10.1007/s11042-019-08233-5.

[4] “VIDEO STEGANOGRAPHY FOR SECURE COMMUNICATION BASED ON ADJOIN PREDICTION AND VECTOR,” no. 1, 2018.

[5] C. Rajpreetha, C. Haripriya, and V. L. M, “A Secured Video Steganography by Linear Feedback Shift Register Method,” vol. 1, no. 4, pp. 56–59, 2015.

[6] V. L. Narayana, A. P. Gopi, and N. A. Kumar, “Different techniques for hiding the text information using text steganography techniques: A survey,” *Ing. des Syst. d’Information*, vol. 23, no. 6, pp. 115–125, 2018, doi: 10.3166/ISI.23.6.115-125.

[7] S. K. Dubey and V. Chandra, “Steganography Cryptography and Watermarking: A Review,” *Int. J. Innov. Res. Sci. Eng. Technol.*, vol.

6, no. 2, pp. 2595–2599, 2017, doi: 10.15680/IJIRSET.2017.0602076.

[8] S. Kingslin and R. S. Dhanalakshmi, “Design of a Security Based Technique for Handling Secure SMS in Mobile Phones using Text Steganography,” no. February, pp. 139–147, 2018.

[9] F. I. Practice and C. Platform, “RESEARCH ARTICLE A Steganography based Framework to Forbid Insecure Practice in Cloud Platform,” vol. 7, pp. 1113–1116, 2018.

[10] M. Y. Valandar, P. Ayubi, and M. J. Barani, “A new transform domain steganography based on modified logistic chaotic map for color images,” *J. Inf. Secur. Appl.*, vol. 34, pp. 142–151, 2017, doi: 10.1016/j.jisa.2017.04.004.

[11] H. Zhu, X. Zhang, H. Yu, C. Zhao, and Z. Zhu, “An image encryption algorithm based on compound homogeneous hyper-chaotic system,” *Nonlinear Dyn.*, vol. 89, no. 1, pp. 61–79, 2017, doi: 10.1007/s11071-017-3436-y.

[12] Y. Himeur and A. Boukabou, “A robust and secure key-frames based video watermarking system using chaotic encryption,” *Multimed. Tools Appl.*, vol. 77, no. 7, pp. 8603–8627, 2018, doi: 10.1007/s11042-017-4754-2.

[13] S. Thakur, A. K. Singh, S. P. Ghrera, and A. Mohan, “Chaotic based secure watermarking approach for medical images,” *Multimed. Tools Appl.*, vol. 79, no. 7–8, pp. 4263–4276, 2020, doi: 10.1007/s11042-018-6691-0.

[14] G. S. Walia, S. Makhija, K. Singh, and K. Sharma, “Robust stego-key

directed LSB substitution scheme based upon cuckoo search and chaotic map," *Optik (Stuttg).*, vol. 170, no. August 2017, pp. 106–124, 2018, doi: 10.1016/j.ijleo.2018.04.135.

[15] U. A. Waqas, M. Khan, and S. I. Batool, "A new watermarking scheme based on Daubechies wavelet and chaotic map for quick response code images," *Multimed. Tools Appl.*, vol. 79, no. 9–10, pp. 6891–6914, 2020, doi: 10.1007/s11042-019-08570-5.

[16] S. Prasad and A. K. Pal, "A Secure Fragile Watermarking Scheme for Protecting Integrity of Digital Images," *Iran. J. Sci. Technol. - Trans. Electr. Eng.*, vol. 44, no. 2, pp. 703–727, 2020, doi: 10.1007/s40998-019-00275-7.

[17] J. Y. Wu, W. L. Huang, W. M. Xia-Hou, W. P. Zou, and L. H. Gong, "Imperceptible digital watermarking scheme combining 4-level discrete wavelet transform with singular value decomposition," *Multimed. Tools Appl.*, vol. 79, no. 31–32, pp. 22727–22747, 2020, doi: 10.1007/s11042-020-08987-3.

[18] P. H. Vo, T. S. Nguyen, V. T. Huynh, T. C. Vo, and T. N. Do, *Secure and Robust Watermarking Scheme in Frequency Domain Using Chaotic Logistic Map Encoding*, vol. 1121 AISC, no. January. Springer International Publishing, 2020.

[19] L. László, "Cubic spline interpolation with quasiminimal B-spline coefficients," *Acta Math. Hungarica*, vol. 107, no. 1–2, pp. 77–87, 2005, doi: 10.1007/s10474-005-0180-4.

[20] E. Cuche, P. Marquet, and C. Depeursinge, "Aperture apodization

using cubic spline interpolation: Application in digital holographic microscopy," *Opt. Commun.*, vol. 182, no. 1–3, pp. 59–69, 2000, doi: 10.1016/S0030-4018(00)00747-1.

[21] G. Wolberg and I. Alfy, "An energy-minimization framework for monotonic cubic spline interpolation," *J. Comput. Appl. Math.*, vol. 143, no. 2, pp. 145–188, 2002, doi: 10.1016/S0377-0427(01)00506-4.

[22] S. E. Reichenbach and F. Geng, "Two-Dimensional Cubic Convolution," *IEEE Trans. Image Process.*, vol. 12, no. 8, pp. 857–865, 2003, doi: 10.1109/TIP.2003.814248.

[23] L. J. Wang, W. S. Hsieh, and T. K. Truong, "A fast computation of 2-D cubic-spline interpolation," *IEEE Signal Process. Lett.*, vol. 11, no. 9, pp. 768–771, 2004, doi: 10.1109/LSP.2004.833479.

[24] J. Shi and S. E. Reichenbach, "Image interpolation by two-dimensional parametric cubic convolution," *IEEE Trans. Image Process.*, vol. 15, no. 7, pp. 1857–1870, 2006, doi: 10.1109/TIP.2006.873429.

[25] L. Ferrer Arnau, R. Reig-Bolaño, P. Martí-Puig, A. Manjabacas, and V. Parisi-Baradad, "Efficient cubic spline interpolation implemented with FIR filters," *Int. J. Comput. Inf. Syst. Ind. Manag. Appl.*, vol. 5, no. December 2014, pp. 098–105, 2012.

[26] S. Scardapane, M. Scarpiniti, D. Comminiello, and A. Uncini, "Learning activation functions from data using cubic spline interpolation," *Smart Innov. Syst. Technol.*, vol. 102, pp. 73–83, 2019, doi: 10.1007/978-3-319-95098-3_7.

[27] O. Q. J. Al-thahab and H. A. Hassan, "RGB Image Watermarking

System based on Cubic Spline Controller Key for Copyright Applications," *Jour Adv Res. Dyn. Control Syst.*, vol. 11, pp. 1896–1905, 2019.

[28] J. M. Mcdonagh, "an Investigation Into Combining Both Facial Detection and Landmark Localisation Into a Unified Procedure Using Gpu Computing," 2016, [Online]. Available: http://eprints.lincoln.ac.uk/26652/1/McDonagh%2C John - Computer Science - December 2016.pdf.

[29] J. Shen, X. Zuo, J. Li, W. Yang, and H. Ling, "A novel pixel neighborhood differential statistic feature for pedestrian and face detection," *Pattern Recognit.*, vol. 63, pp. 127–138, 2017, doi: 10.1016/j.patcog.2016.09.010.

[30] W. Tian *et al.*, "Learning Better Features for Face Detection with Feature Fusion and Segmentation Supervision," 2018, [Online]. Available: http://arxiv.org/abs/1811.08557.

[31] H. Qezavati, B. Majidi, and M. T. Manzuri, "Partially Covered Face Detection in Presence of Headscarf for Surveillance Applications," *4th Int. Conf. Pattern Recognit. Image Anal. IPRIA 2019*, pp. 195–199, 2019, doi: 10.1109/PRIA.2019.8786004.

[32] C. Chi, S. Zhang, J. Xing, Z. Lei, S. Z. Li, and X. Zou, "Selective refinement network for high performance face detection," *33rd AAAI Conf. Artif. Intell. AAAI 2019, 31st Innov. Appl. Artif. Intell. Conf. IAAI 2019 9th AAAI Symp. Educ. Adv. Artif. Intell. EAAI 2019*, pp. 8231–8238, 2019, doi: 10.1609/aaai.v33i01.33018231.

[33] H. Huang, Z. Li, L. Wang, S. Chen, B. Dong, and X. Zhou, “Feature space singularity for out-of-distribution detection,” *CEUR Workshop Proc.*, vol. 2808, 2021.

[34] S. Zhang, C. Chi, Z. Lei, and S. Z. Li, “RefineFace: Refinement Neural Network for High Performance Face Detection,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. XX, no. X, pp. 1–1, 2020, doi: 10.1109/tpami.2020.2997456.

[35] A. Prout *et al.*, “Enabling on-demand database computing with MIT SuperCloud database management system,” *2015 IEEE High Perform. Extrem. Comput. Conf. HPEC 2015*, pp. 1–6, 2015, doi: 10.1109/HPEC.2015.7322482.

[36] K. I. Satoto, R. R. Isnanto, R. Kridalukmana, and K. T. Martono, “Optimizing MySQL database system on information systems research, publications and community service,” *Proc. - 2016 3rd Int. Conf. Inf. Technol. Comput. Electr. Eng. ICITACEE 2016*, pp. 1–5, 2017, doi: 10.1109/ICITACEE.2016.7892476.

[37] D. Van Aken, A. Pavlo, G. J. Gordon, and B. Zhang, “Automatic database management system tuning through large-scale machine learning,” *Proc. ACM SIGMOD Int. Conf. Manag. Data*, vol. Part F1277, pp. 1009–1024, 2017, doi: 10.1145/3035918.3064029.

[38] J. Arulraj and A. Pavlo, “How to build a non-volatile memory database management system,” *Proc. ACM SIGMOD Int. Conf. Manag. Data*, vol. Part F1277, pp. 1753–1758, 2017, doi: 10.1145/3035918.3054780.

[39] B. Zhang *et al.*, “A Demonstration of the ottertune automatic database

management system tuning service,” *Proc. VLDB Endow.*, vol. 11, no. 12, pp. 1910–1913, 2018, doi: 10.14778/3229863.3236222.

[40] B. Jiang *et al.*, “Pids: A user-friendly plant dna fingerprint database management system,” *Genes (Basel).*, vol. 11, no. 4, 2020, doi: 10.3390/genes11040373.

[41] S. S. Shin, “Structured Query Language Learning: Concept Map-Based Instruction Based on Cognitive Load Theory,” *IEEE Access*, vol. 8, pp. 100095–100110, 2020, doi: 10.1109/ACCESS.2020.2997934.

[42] N. Alseelawi, “Database Management System to Design a Medical Treasury System,” no. December, 2020, doi: 10.13140/RG.2.2.32294.34883.

[43] M. Hussain, “A Survey of Image Steganography Techniques A Survey of Image Steganography Techniques Mehdi Hussain and Mureed Hussain,” no. February, 2015.

[44] H. Kaur and J. Rani, “A Survey on different techniques of steganography,” *MATEC Web Conf.*, vol. 57, 2016, doi: 10.1051/matecconf/20165702003.

[45] D. Renza, L. D. M. Ballesteros, and J. Sanchez, “Highly transparent steganography scheme of speech signals into color images using quantization index modulation,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9703, pp. 241–250, 2016, doi: 10.1007/978-3-319-39393-3_24.

[46] A. N. Mironenko and M. D. Velichko, “Method of applying (t,n)-

threshold scheme in steganography," *CEUR Workshop Proc.*, vol. 2081, pp. 93–97, 2017.

[47] A. Kumar and K. Pooja, "Steganography- A Data Hiding Technique," *Int. J. Comput. Appl.*, vol. 9, no. 7, pp. 19–23, 2010, doi: 10.5120/1398-1887.

[48] L. Yihong, Y. Chunhui, and C. Songli, *The software quality prediction model based on DBN*, vol. 752. 2019.

[49] M. P. West, "The Medical Record," *Acute Care Handb. Phys. Ther. Fourth Ed.*, pp. 11–14, 2014, doi: 10.1016/B978-1-4557-2896-1.00002-0.

[50] D. K. Mendis and P. I. Purves, "Electronic Patient Records – The Reality," *Natl. Comput. Conf.*, no. May, 2002.

[51] Oromi, "Documentation of Medical Records Documentation of Medical Records," 2014.

[52] L. R. Plunkett, "Managing patient records.," *N. Y. State Dent. J.*, vol. 63, no. 4, pp. 8–12, 1997, doi: 10.1007/978-1-4612-0675-0_9.

[53] C. J. McDonald, P. C. Tang, and G. Hripcsak, "Electronic health record systems," *Biomed. Informatics Comput. Appl. Heal. Care Biomed. Fourth Ed.*, pp. 391–421, 2014, doi: 10.1007/978-1-4471-4474-8_12.

[54] D. Maia and R. Trindade, "Face Detection and Recognition in Color Images under Matlab," *Int. J. Signal Process. Image Process. Pattern Recognit.*, vol. 9, no. 2, pp. 13–24, 2016, doi:

10.14257/ijsip.2016.9.2.02.

[55] M. Chauhan, “Study & Analysis of Different Face Detection Techniques,” vol. 5, no. 2, pp. 1615–1618, 2014.

[56] R. L. Hsu, M. Abdel-Mottaleb, and A. K. Jain, “Face detection in color images,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 24, no. 5, pp. 696–706, 2002, doi: 10.1109/34.1000242.

[57] A. Kumar, A. Kaur, and M. Kumar, “Face detection techniques: a review,” *Artif. Intell. Rev.*, vol. 52, no. 2, pp. 927–948, 2019, doi: 10.1007/s10462-018-9650-2.

[58] S. Praveen Kumar, V. Kesava Jayendra Varma, V. Subramanya, and A. Venkata Sai Harish, “A multiple face recognition system with DLIB’s RESNET network using deep metric learning,” *J. Crit. Rev.*, vol. 7, no. 6, pp. 856–859, 2020, doi: 10.31838/jcr.07.06.147.

[59] G. Guo, H. Wang, Y. Yan, J. Zheng, and B. Li, “A fast face detection method via convolutional neural network,” *Neurocomputing*, vol. 395, no. Bo Li, pp. 128–137, 2020, doi: 10.1016/j.neucom.2018.02.110.

[60] B. Forgues, “The Palgrave Encyclopedia of Strategic Management,” *Palgrave Encycl. Strateg. Manag.*, no. January 2016, 2016, doi: 10.1057/978-1-349-94848-2.

[61] O. S. Jahromi, “Signals and Communication Technology,” *Springler*, vol. 58, no. 12, pp. 7250–7, 2014, [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/25246403%5Cnhttp://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=PMC4249520.

[62] Pourasad, Yaghoub, Ramin Ranjbarzadeh, and Abbas Mardani. "A new algorithm for digital image encryption based on chaos theory." *Entropy* 23.3 (2021): 341.

[63] Al-Asady, Heba Abdul-Jaleel, Osama Qasim Jumah Al-Thahab, and Saad S. Hreshee. "Robust encryption system based watermarking theory by using chaotic algorithms: A reviewer paper." *Journal of Physics: Conference Series*. Vol. 1818. No. 1. IOP Publishing, 2021.

[64] S. S. Hreshee, H. N. Abdullah, and A. K. Jawad, "A high-security communication system based on chaotic scrambling and chaotic masking," International Journal on Communications Antenna and Propagation (I.Re.C.A.P.), vol. 8, no. 3, pp. 257–264, 2018. doi:10.15866/recap.v8i3.13541

[65] K. S. Reddy and S. Ramachandram, “A secure, fast insert and efficient search order preserving encryption scheme for outsourced databases,” *Int. J. Adv. Intell. Paradig.*, vol. 13, no. 1–2, pp. 155–177, 2019, doi: 10.1504/IJAIP.2019.099949.

[66] H. F. Korth and A. Silberschatz, “Database system concepts,” *McGraw-Hill Comput. Sci. Ser. ; McGraw-Hill Ser. Syst.*, 1991, doi: 10.1145/253671.253760.

[67] C. Mohan *et al.*, “Distributed Computing with Permissioned Blockchains and Databases Edited by 1 Executive Summary Creative Commons BY 3.0 Unported license 70 19261-Distributed Computing with Permissioned Blockchains and Databases,” *Rep. from Dagstuhl Semin.*, vol. 9, no. 6, pp. 69–94, 1926, [Online]. Available: http://www.dagstuhl.de/19261.

[68] M. P. Hall, “Jordan University of Science and Technology Faculty of Computer & Information Technology Computer Information Systems Department CIS 433 Information Security Course Catalog Course Information Information Security CIS 433 Statistics (Math131) & Data Stru,” pp. 2–5, 2015.

[69] T. Amudha and K. Saravanan, “Data and Technical Security Issues in Cloud Computing Databases,” no. June, pp. 686–694, 2019.

[70] K. Ahmad, M. S. Alam, and N. I. Udzir, “Security of NoSQL Database Against Intruders,” *Recent Patents Eng.*, vol. 13, no. 1, pp. 5–12, 2018, doi: 10.2174/1872212112666180731114714.

[71] S. Mukhopadhyay, “Secure Distributed Storage for the Internet of Things,” pp. 159–173, 2019, doi: 10.1007/978-3-030-15705-0_12.

[72] L. Okman, N. Gal-Oz, Y. Gonen, E. Gudes, and J. Abramov, “Security issues in NoSQL databases,” *Proc. 10th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2011, 8th IEEE Int. Conf. Embed. Softw. Syst. ICESS 2011, 6th Int. Conf. FCST 2011*, no. November 2011, pp. 541–547, 2011, doi: 10.1109/TrustCom.2011.70.

[73] N. R. Adam and J. C. Worthmann, “Security-control methods for statistical databases: A comparative study,” *ACM Comput. Surv.*, vol. 21, no. 4, pp. 515–556, 1989, doi: 10.1145/76894.76895.

[74] E. Barba, M. Koromina, E. E. Tsermpini, and G. P. Patrinos, *Translational tools and databases in genomic medicine*. Elsevier Inc., 2019.

[75] E. Bertino, “Data hiding and security in object-oriented databases,”

Proc. - Int. Conf. Data Eng., pp. 338–347, 1992, doi: 10.1109/icde.1992.213176.

[76] H. Liang, N. Li, and S. Zhao, "Salt and pepper noise removal method based on a detail-aware filter," *Symmetry (Basel).*, vol. 13, no. 3, 2021, doi: 10.3390/sym13030515.

[77] A. Parsa and A. Farhadi, "Tele-operation of autonomous vehicles over additive white Gaussian noise channel," *Sci. Iran.*, vol. 28, no. 3, pp. 1592–1605, 2021, doi: 10.24200/SCI.2020.54447.3755.

[78] G. Ciocca, C. Cusano, F. Gasparini, and R. Schettini, "Self-adaptive image cropping for small displays," *IEEE Trans. Consum. Electron.*, vol. 53, no. 4, pp. 1622–1627, 2007, doi: 10.1109/TCE.2007.4429261.

[79] A. D. McRae and M. A. Davenport, "Low-rank matrix completion and denoising under Poisson noise," *Inf. Inference*, vol. 10, no. 2, pp. 697–720, 2021, doi: 10.1093/imaiai/iaaa020.

[80] J. J. Gómez-Valverde *et al.*, "Adaptive compounding speckle-noise-reduction filter for optical coherence tomography images," *J. Biomed. Opt.*, vol. 26, no. 06, pp. 1–24, 2021, doi: 10.1117/1.jbo.26.6.065001.

[81] M. Bayraktar, "Scintillation and bit error rate calculation of Mathieu–Gauss beam in turbulence," *J. Ambient Intell. Humaniz. Comput.*, vol. 12, no. 2, pp. 2671–2683, 2021, doi: 10.1007/s12652-020-02430-z.

[82] B. Silemek *et al.*, "Rapid safety assessment and mitigation of radiofrequency induced implant heating using small root mean square sensors and the sensor matrix Qs," *Magn. Reson. Med.*, no. May, pp. 1–19, 2021, doi: 10.1002/mrm.28968.

REFERENCES

Appendix A

APPENDIX A

LANGUAGES USED IN BUILDING THE PROGRAM

A.1Matlab Language

MATLAB® is a powerful programming language. It combines computation, visualization, and programming in a familiar mathematical syntax. • Math and computation • Algorithm creation • Data collecting • Modeling, simulation, and prototyping

- Engineering graphics
- Application development, including GUI design
- This interactive system uses arrays as its basic data element.
- doesn't require sizing This solves numerous technical issues.
- solving issues with matrices and vectors

a proportion of the time required to write a scalar non-interactive like C or Fortran.

Matrix laboratory is MATLAB. MATLAB was created to facilitate access to LINPACK and EISPACK matrices. Today's MATLAB engines include the LAPACK and BLAS libraries, delivering cutting-edge matrices calculation software. MATLAB has evolved through time with numerous users' contributions.

It is widely used in university mathematics, engineering, and science courses. MATLAB is the industry standard for high-speed research, development, and analysis.

Toolboxes are a family of MATLAB add-on application-specific solutions. Toolboxes allow you to study and apply specialized technology. Toolboxes are collections of MATLAB routines (M-files) that help address certain problems. Signal processing, control systems, neural networks, fuzzy logic, wavelets, simulation, and other areas have toolboxes.

A.1.1 Matlab system

Matlab system is divided into five primary parts:

IDE. Tools and utilities for working with MATLAB functions and files. Many of these tools have GUIs. It has a command history, an editor and debugger, and browsers for help, workspace, files, and search path.

The MATLAB Function Library: Complex arithmetic and matrix inversion are examples of more advanced functions like Bessel functions and rapid Fourier transforms.

MATLAB Language: This is an object-oriented matrix/array language featuring control flow statements, functions, data structures, and input/output. It allows both “programming in the small” and “programming in the large” to develop quick and dirty throw-away programs. Graphics.

MATLAB graphic: includes rich graphing capabilities for vectors and matrices, including annotation and printing. It has high-level utilities for data visualization, image processing, animation, and presentation graphics. It also includes low-level capabilities for fully customizing graphics and building graphical user interfaces for MATLAB programs.

The MATLAB External API: This library allows C and Fortran programs to communicate with MATLAB. It can call MATLAB routines (dynamic linking), use MATLAB as a computational engine, and read and write MAT files.

A.1.2 MATLAB Documentation

MATLAB provides extensive written and online documentation to help you learn and apply its capabilities. If you're a new user, start with this guide. It includes several examples and covers all basic MATLAB functions.

The MATLAB online help contains task-oriented and reference information. MATLAB documentation is available in print and PDF To access the online documentation, use MATLAB's Help menu. The MATLAB documentation is divided into four parts:

- Desktop Tools and Development Environment — Startup, shutdown, and other MATLAB tools operations and data analysis in mathematics
- Graphics — Tools and techniques for plotting, graph annotation, printing, and programming with Handle Graphics®
- Creating Graphical User Interfaces — GUI-building tools and how to write callback functions
- External API — MEX-files, MATLAB engine, Java, COM, and serial port

All MATLAB functions include reference documentation:

This section lists all MATLAB functions by category.

- External Interfaces/API Reference — Covers functions used by the MATLAB external interfaces, offering information on syntax in the calling language, description, arguments, return values, and examples

A.2 HTML (HyperText Markup Language)

Is the standard markup language for web documents. It can be aided by CSS and programming languages like JavaScript. Web browsers translate HTML content from a web server or local storage into multimedia web pages. HTML initially featured signals for the document's aesthetic as well as semantic organization.

HTML elements are the pages' building blocks. Images and interactive forms can be embedded in the produced page using HTML techniques. HTML allows you to construct organized documents by defining headers, paragraphs, lists, links, quotations, and other text elements. Tags, written in angle brackets, separate HTML elements. Tags like image and input directly add content to the page. Additional tags, like p, offer context for text and may contain other tags as sub-elements. Browsers don't show HTML tags but use them to decipher the page's content.

HTML allows scripting languages like JavaScript to insert applications that change web page behavior and content. CSS defines the content's style and layout. Since 1997, the World Wide Web Consortium (W3C), former HTML and CSS standard manager, has pushed the usage of CSS over explicit presentational HTML.

A.2.1 What is HTML

Unlike other text files, HTML is a formatted text file that shows the computer and web server that it is HTML and should be interpreted as such. Using any text editor, a user can create a rudimentary webpage and upload it to the internet using HTML principles.

A document type declaration at the start of the text file is the most fundamental HTML practice. This is always first in the page since it tells a computer that it is an HTML file. !DOCTYPE html> is the standard document header. It should always be written that way, with no text inside. The computer will not recognize any material before this declaration as HTML.

Doctypes aren't just for HTML; they can be used for any SGML document (Standard Generalized Markup Language). SGML is a standard for defining a markup language. SGML and doctype declarations apply to HTML, among others.

An HTML file must also be saved with the.html extension. Unlike the doctype declaration, the file extension signals HTML to the computer from outside the file. Having both tells a computer it's an HTML file whether it's reading it or not. This is vital when uploading files to the web because the web server must know what to do with them before sending them to a client computer.

One may then utilize all the HTML syntax tools to customize a web page after writing the doctype. They'll have many HTML files matching to various website pages. In order to enable linkages across pages, the user must upload these files in the same structure as they saved them. A different order will create broken links and lost pages since the file paths will not match the pages.

A.2.2 HTML Elements

To show a document in HTML, a text file is marked up with additional text. To distinguish the markup from the real HTML content, an unique HTML syntax is needed. HTML tags are special components. Attributs are name-value pairs that are contained within tags. An HTML element is a piece of content encased within a tag.

Opening, middle, and closing tags are all required in HTML. Attributes are added in the opening tag to provide more element information. Elements are classified as follows:

Block-level items start on a new line and take up space. Headings and paragraph tags are examples. Inline elements do not require a new line in the document. These components often format block-level elements. Hyperlinks and text format tags are inline elements.

- HTML pros and disadvantages
- Pros of HTML include:
- Is frequently used and has many resources.
- Runs on every browser.
- Is simple to learn.
- Has a well-organized source code.
- Is free and open source.
- Can be used with different backend languages like PHP.
- Here are a few cons:

It is used for static web pages and has little dynamic features. They must be constructed separately even if they share elements. Browser behavior varies. Older browsers, for example, may not support newer features. Common HTML tags

HTML tags define a page's overall structure and how its elements are displayed in the browser. HTML tags include:

h1 is a top-level heading.

h2> describes a subheading.

p> denotes a paragraph.

a table describing tabular data

ol> describes an ordered list of data.

ul> is an unordered list.

Opening and closing tags surround the information they augment. An opening tag reads: <p>. To signify the conclusion of an HTML element, a closing tag ends with a backslash. Closing tags are /p>.

A.2.3 How to utilize HTML

Because HTML is entirely text-based, it can be altered in programs like Notepad++, Vi, or Emacs. An HTML file can be created or edited in any text editor, and any web browser, such as Chrome or Firefox, can display it as a webpage.

Professional software developers can create webpages using WYSIWYG editors. WYSIWYG editors are available as plugins or standard components in NetBeans, IntelliJ, Eclipse, and Visual Studio. Modern online browsers sometimes feature web developer plugins that indicate flaws with HTML sites, such as a missing closing tag or syntax that does not create well-formed HTML.

Chrome and Firefox both have HTML developer tools that allow users to view a webpage's whole HTML file, edit HTML on the fly, and save changes directly within the internet browser.

A.2.4 HTML, CSS, and JS

Creating websites in HTML has certain limitations when it comes to completely responsive components. So only use HTML to add text components and organise them on a page. HTML can be used with CSS and JavaScript to create more complicated functionality (JS).

This file contains information on which colors to use, which fonts to use, and other HTML element rendering information. JavaScript also enables dynamic features like pop-ups and photo sliders. Class attributes are used to match HTML elements to CSS or JS elements.

For example, to make text red, a user can enter code in the CSS file using a class attribute that turns text red. Then they can use the class attribute to make all red text in the HTML sheet. JS sheets work similarly, but with different functions.

A software development pattern and best practice known as separation of concerns separates information about how a page is constructed (HTML) from information about how a page looks when viewed in a browser.

It's also worth noting that HTML works with basic English. For example, Chinese characters or special symbols like accented letters may not appear correctly on a webpage by default. To handle special character sets, users must define the character encoding with a meta charset="utf-8"/> element. The character set is utf-8. The HTML charset is Utf-8.

A.3. JavaScript

Is a popular web programming language. Netscape created it to make websites more dynamic and interactive. It is based on ECMAScript, a scripting language developed by Sun Microsystems, and its syntax is comparable to C.

Unlike other programming languages, JavaScript is client-side, meaning the source code is processed by the client's web browser. Delaying communication with the server is possible using JavaScript. JavaScript functions can check online forms to make sure all required fields are filled in before submitting them. The JavaScript code can generate an error message before any data is sent to the server.

JavaScript, like server-side programming languages like PHP and ASP, can be put anywhere within a webpage's HTML. However, only server-side code output is displayed in HTML, while JavaScript code remains viewable in the webpage's source. It can also be referenced in a.JS file viewed in a browser.

Simple JavaScript function that adds two numbers. The function is called with 7 and 11. If the code below is put in a webpage's HTML, an alert box with the text "18" will appear.

```
    <script>
  function sum(a,b)
  {
    return a + b;
  }
  var total = sum(7,11);
  alert(total);
</script>
```

JavaScript functions can be invoked inside script tags or when events occur. Then there's onMouseDown, onMouseUp, onKeyDown, onKeyUp, onFocus, onBlur, and many more. However, many web developers choose to use JavaScript libraries like jQuery to add more powerful dynamic elements to webpages.

A.4 Cascading Style Sheets (CSS)

CSS is a style sheet language used to describe the appearance of a document authored in a markup language like HTML. [1] CSS, like HTML and JavaScript, is a cornerstone of the Internet.

CSS separates presentation from content, including layout, colors, and fonts. Multiple web pages can share formatting by specifying relevant CSS in a separate.css file, which reduces complexity and repetition in structural content, and the CSS file can be cached to improve page load speed between the p

The separation of formatting and content allows for alternative rendering modalities, such as on-screen, print, voice (through speech-based browser or screen reader), and Braille-based haptic devices. CSS also provides standards for mobile-friendly formatting.

The name cascading stems from the priority mechanism used to determine which style rule applies to an element. This priority hierarchy is predictable.

The W3C maintains the CSS specifications (W3C). RFC 2318 defines the MIME type text/css for usage with CSS (March 1998). The W3C offers a free CSS validation service. Other markup languages that enable CSS include XHTML, plain XML, SVG, and XUL.

Appendix B

APPENDIX B

IMAGE FILE TYPES

B.1 Introduction.

It is also helpful to understand the common image file formats of digital images, how these file formats differ, and what their recommended use is. TIFF (.tif), JPG (.jpg, .jpeg), GIF (.gif) and PNG (.png) are file formats (and their respective file extensions) that you are likely to encounter. Other image file formats are used to a lesser extent; these formats are often proprietary, such as Photoshop [75].

B.2 JPG or JPEG.

JPEG (Joint Pictures Expert Group) is designed for compressing full-color or gray-scale images of natural, real-world scenes. It works well on photographs, naturalistic artwork, and similar material. It may not be the best format to use for lettering, simple cartoons, or line drawings. Web browsers support this format natively. Along with GIF, JPEG is the standard format for Web images.

JPEG stores full color information: it stores 24 bits/pixel, which means it can store up to 16 million colors. JPEG images display very well on monitors that support more than 256 colors.

The JPEG algorithm rearranges the image information into color and detail information, compressing color more than detail because our eyes are more sensitive to detail than to color, making the compression less visible to the naked eye. It sorts the detail information into fine and coarse detail and discards the fine detail first because our eyes are more sensitive to coarse detail than to fine detail.

JPEG is a standard lossy image compression algorithm. Lossy compression means that only a part of the original information is still there when the file is uncompressed, although the user may not notice any change.

The degree of looseness can be can be varied by adjusting compression parameters. This means you can trade off file size against output image quality.

B.3 GIF.

` GIF (Graphic Interchange Format) works best for images with only a few distinct colors, such as line drawings and simple cartoons. GIF is useful for cartoon images that have less than 256-(28) colors, grayscale images, and black and white text.

GIF, like JPEG, is a standard format for Web images. The primary limitation of a GIF is that it only works on images with 8 bits per pixel or less, which means 256 or fewer colors. Most color images are 24 bits per pixel. To store these in GIF format you must first convert the image from 24 bits to 8 bits. The conversion will result in a loss of data and a considerable degradation in quality. Computer monitors that display only 256 colors or less display GIFs well.

GIF is a lossless image file format. With lossless compression, all of the data that was originally in the file remains after the file is uncompressed. There are three primary types of GIF images.

B.3.1 Normal.

The GIF image data is stored sequentially.

B.3.2 Interlaced.

With interlaced GIFs, the lines of the image are not stored sequentially, but are interlaced. For example, instead of storing lines 1 through 10 in order, it stores line 1 and then lines 3,5,7,9,2,4,6,8,10. This allows applications to display part of the image first and then fill in the missing lines to complete the image.

B.3.3 Animated GIF.

This allows you to store multiple GIF images in the same image file. Usually the images are displayed sequentially over time, creating a small animation.

B.4 PNG.

PNG (Portable Network Graphics) is a file format for image compression. It was developed as a patent free replacement for GIF (Unisys owns the GIF format). It provides a number of improvements over the GIF format.

Like a GIF, a PNG file uses lossless compression. It allows you to make a trade-off between file size and image quality when the image is compressed. Typically, an image in a PNG file can be 10 to 30% more compressed than in a GIF format. Like GIFs, you can make one color transparent, but you can control the degree of transparency (this is also called "opacity"). Interlacing is supported and is faster in developing than in the GIF format. Images can be saved using true color as well as in the palette and gray-scale formats.

B.5 JPEG2000.

JPEG2000 format is emerging as a standard for image compression. It provides much better image quality at smaller file sizes than JPEG does. Based on wavelet compression, JPEG2000 offers both lossless and lossy compression. JPEG2000 formats provide good image quality, even at very high compression ratios such as 80:1. JPEG2000 creates scalable image files, which means that no decompression is needed for reformatting.

B.6 TIFF.

TIFF (Tagged Image File Format) has emerged as the standard archiving image file format for library use. Its strengths are that the format is extensible new image types can be introduced without invalidating older types and portable. It is independent of hardware and operating system types.

الخلاصة

نتيجة لتطور تقنيات المعلومات والإنترنت ، ظهرت الحكومات الإلكترونية. تجعل هذه الحكومات الإلكترونية جميع المؤسسات تتعامل مع أرشفة البيانات وحفظها عبر الإنترنت من خلال إنشاء قاعدة بيانات واحدة ومشتركة لنظام الدولة الواحدة لتسهيل العمل مع الوثائق وتسهيل التوظيف للمواطنين .

البيانات يجب تشفير ها لحماية المعلومات الموجودة في قاعدة البيانات وعدم السماح للأشخاص غير المصرح لهم بالوصول إليها . يحمي التشفير المعلومات بإخفائها في أنواع البيانات الأخرى مثل الصور والأصوات والرسائل ومقاطع الفيديو. يستخدم نظام فك التشفير لمعرفة البيانات المشفرة بالاعتماد على المفاتيح الأساسية المستخدمة في التشفير . وبالتالي ، سعت هذه الأطروحة إلى بناء مخطط ترميز متميز وفريد لحماية قاعدة البيانات والبيانات المؤرشفة. تمت التوصية بالملف الطبي الإلكتروني المشفر للمريض كدراسة حالة لأن جميع المؤسسات الصحية العراقية تفتقر إلى قاعدة بيانات للمرضى .

يتكون النظام المقترح من ثلاث مراحل: المرحلة الأولى هي جمع البيانات بما في ذلك صور المريض والمعلومات مثل الاسم الكامل ، واسم الأم ، والوزن ، والطول ، وفصيلة الدم ، وضغط الدم ، ومعدل التنفس ، وطبيب المختص (طبيب الأسرة) .

المرحلة الثانية هي معالجة البيانات التي تتكون من ثلاث خطوات حيث. الخطوة الأولى هي تحديد جزء الوجه من الصورة باستخدام خوارزمية اكتشاف الوجه لإخفاء المعلومات فيه . بعد اكتشاف صورة الوجه ، يتم قص الصورة واستخراج الألوان الأساسية (الأحمر والأخضر والأزرق) لتجهيزها لعملية اخفاء البيانات .

الخطوة الثانية هي تشفير البيانات باستخدام الخريطة اللوجستية الفوضوية. يتم تقديم حداثة هذه الرسالة في التشفير. الطريقة الجديدة هي استخدام شريحة المكعب ثنائية الأبعاد في المرحلة الثانية من التشفير. يتم ذلك عن طريق تحديد الأماكن من المصفوفة الخضراء للصورة. بعد تغيير اللون الأخضر من مصفوفة عشرية إلى مصفوفة ثنائية الاعداد ذات الأبعاد الثلاثة (س، ص، ع) ، ثم يتم التشفير.

يتم تشفير طول بيانات المريض باللون الأحمر للصورة، والذي يستخدم كمفتاح لفك التشفير.

بعد التحويل من النظام الثنائي إلى النظام العشري ، ودمج الألوان الأساسية ، يتم استعادة الصورة إلى شكلها الأصلي.

الخطوة الأخيرة هي أرشفة الصور في السحابة، والتي توفر حماية كاملة للبيانات مع اسم الشخص الذي يدخل هذه البيانات المحفوظة تلقائيًا في قاعدة البيانات المركزية. فائدة أخرى لأرشفة البيانات على السحابة هي عرض اسم المريض وصورته عند البحث في قاعدة البيانات. تعمل هذه الوظيفة على تأمين الملف الطبي الإلكتروني للمريض.

النصف الثاني من النظام يسمح فقط لمالك برنامج فك تشفيره فقط باستخراج البيانات، وهو عكس إجراء التشفير وحماية البيانات. يتم استخدام خوارزمية عكسية في Matlab لتقسيم الصورة إلى ألوانها الأساسية الأزرق والأحمر والأخضر واستخراج طول البيانات المشفرة عبر اللون الأحمر ، والذي يستخدم كمفتاح لبقية الوظائف ، مثل اللوجيستية الوظيفة ودالة التكعيب ثنائية الأبعاد ، ثم استخراج المناطق التي يتم فيها تشفير المعلومات (اللون الأخضر)

وباستخدام الخريطة اللوجستية يتم الحصول على البيانات المشفرة واستعادتها إلى نص كما تمت قراءتها في نتائج عملية معالجة البيانات في تقرير متكامل من بيانات المريض .

تُستخدم الصور بتنسيقات JPEG و PNG لاختبار هذا التطبيق ؛ تم إدخال بياناتهم وتشفيرها ونقلها إلى الخادم .

تقييم قوة الخوارزمية تم بتجربة الهجمات مثل Gaussian و salt & pepper و Poisson و Spekle . تظهر النتائج ارتفاع PSNR يصل إلى dB105.871 ، وقيم RMS 0.0001 ، واستعادة البيانات بمعدل خطأ 0.00001 . يتم تنفيذ النظام باستخدام windows ten على الجهاز اللوحي (ThinkPad tablet مع المعالج intel (R) Core (TM) -m7-6y75) حيث يتم التقاط الصورة والمعلومات بواسطة واجهة المستخدم الرسومية لبرنامج MatLab المثبت في هذا الجهاز اللوحي ومن ثم يتم معالجة البيانات وتحميلها على السحابة .

جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جامعة بابل
كلية الهندسة/ قسم الهندسة الكهربائية

نهج جديد لنظام إخفاء المعلومات الذكي باستخدام حاسوب دقيق متقدم في التطبيقات الضوئية

أطروحة مقدمة إلى قسم الهندسة الكهربائية / كلية الهندسة / جامعة بابل وهي جزء من متطلبات نيل درجة الدكتوراه في علوم هندسة الإلكترونيك والاتصالات

من قبل

هبة عبد الجليل كزار الاسدي

بأشراف

الاستاذ الدكتور أسامة قاسم الذهب

الاستاذ الدكتور سعد سفاح حريشي

1443هـ **2021م**