DOCTOR-PATIENT REMOTE CONSULTATION SYSTEM WITH SECURE MEDICAL IMAGES

TEH YEE HENG

FACULTY OF COMPUTING AND INFORMATICS

UNIVERSITI MALAYSIA SABAH

2022

DOCTOR-PATIENT REMOTE CONSULTATION SYSTEM WITH SECURE MEDICAL IMAGES

TEH YEE HENG

THESIS SUBMITTED IN PARTIAL FULFILLMENT FOR THE DEGREE OF BACHELOR OF COMPUTER SCIENCE WITH HONOURS (NETWORK ENGINEERING)

FACULTY OF COMPUTING AND INFORMATICS
UNIVERSITY MALAYSIA SABAH

MATRIC NUMBER **:** BI18160295

TITLE **:** DOCTOR-PATIENT REMOTE CONSULTATION SYSTEM WITH SECURE MEDICAL IMAGE

DEGREE **:** BACHELOR OF COMPUTER WITH HONOURS

(NETWORK ENGINEERING)

VIVA'S DATE **:** 25-01-2022

CERTIFIED BY;

1. **SUPERVISOR** Signature

Dr. LEAU YU BENG

_____

DECLARATION

I hereby declare that the material in this thesis is my own except for quotations, equations, summaries and references, which have been duly acknowledged.

25-01-2022

TEH YEE HENG
BI18160295

ACKNOWLEDGEMENT

I'd like to thank various individuals and organisations for their unwavering support during my graduate studies. First and foremost, I want to express my profound appreciation to Dr. Leau Yu Beng, my supervisor, for his excitement, patience, insightful remarks, valuable information, practical guidance, and never-ending ideas, which have greatly aided me during my study and writing of my thesis. His vast knowledge, extensive experience, and professional competence in Data Security helped me to effectively finish my study. This endeavour would not have been feasible without his help and supervision. In my studies, I could not have asked for a better supervisor.

I would also want to thank the Universiti Malaysia Sabah for allowing me into the graduate programme. In addition, I am thankful to the Universiti Malaysia Sabah's Faculty of Computing and Informatics for the resources used in this research. I am also grateful to the following lecturers: Dr. Tan Soo Fun and Dr. Farashazilla binti Yahya for the comments and the examinations.

Last but not least, to everyone in the Research institute for Network Engineering and Software Engineering, it was great sharing premises with all of you during these research years.

Thanks for all your encouragement!

TEH YEE HENG

25-01-2022

ABSTRAK

SYSTEM PERUNDINGAN TERPENCIL DOKTOR-PESAKIT DENGAN KESELAMATAN GAMBAR MEDIKAL

Dalam dunia yang sedang berkembang pesat ini, segala-galanya di sekeliling kita telah menjadi lebih banyak digital yang berkaitan. Oleh itu, data privasi kami adalah di seluruh Internet. Ini akan menjadikan kita menjadi lebih terdedah kepada jenayah siber dan eksploitasi data haram. Oleh itu, keselamatan maklumat privasi kami telah menjadi masalah rumit untuk ditangani. Walau bagaimanapun, data dalam perkataan telah didapati lebih mudah untuk disulitkan. Tetapi, data multimedia seperti video, audio dan imej adalah contoh data yang lebih sukar untuk disulitkan. Oleh itu, data jenis ini mempunyai keselamatan yang 'jarang' berbanding perkataan. Selalunya keselamatan yang digunakan baru-baru ini dalam industri hari ini adalah watermark data multimedia tersebut. Walau bagaimanapun, watermarking boleh berfungsi pada imej dan video sahaja. Juga, watermarking masih tersedia untuk orang ramai untuk melihat data tersebut tetapi menghalang mereka daripada mengeksploitasi kerana hak cipta. Walau bagaimanapun, jika orang yang ingin membuat data dapat dilihat oleh orang tertentu hanya seperti imej X-ray orang tertentu, watermark mungkin tidak cukup untuk mencapai itu. Tambahan pula, orang yang tinggal di kawasan luar bandar sering tidak dapat mengakses ke hospital atau bantuan perubatan dengan mudah dan segera. Oleh itu, objektif projek ini adalah untuk membangunkan sistem yang boleh menyekat hak untuk mengakses data imej dan menggunakan algoritma penyulitan imej untuk melindungi imej tersebut untuk diekstrak oleh orang yang tidak dibenarkan serta membantu orang yang tinggal di kawasan luar bandar untuk mendapatkan perundingan perubatan lebih mudah daripada sebelumnya. Dalam projek ini, pelajar dan pensyarah dari Fakulti Perubatan dan Sains Kesihatan telah menjadi pengguna sasaran kami. Teknik penyulitan imej yang mungkin terlibat adalah berebut dan penyebaran. Hasilnya adalah bahawa kita boleh menyulitkan imej X-ray dan orang yang mempunyai kunci penyahsulitan hanya boleh melihat imej. Dalam Fasa Eksperimen, 3 dari algoritma yang dipilih telah dilaksanakan sebagai bahasa yang sama yang mungkin untuk menghasilkan hasil yang lebih dipercayai. Hasilnya direkodkan termasuk masa larian dan saiz imej yang disulitkan. Pemilihan akhir algoritma bergantung kepada saiz penyulitan dan kelajuan pengiraan. Saiz terkecil dengan kelajuan komputasi terpantas telah dipilih dan melalui hasilnya, algoritma yang dipilih adalah pengekodan DNA.

ABSTRACT

In this rapid developing world, everything around us has becoming more and more digital related. Therefore, our privacy data is all over the Internet. This will make us become more vulnerable to cyber-crime and illegal data exploitation. Hence, security of our privacy information had becoming a tricky trouble to deal with. However, data in words had been found that are easier to be encrypted. But, multimedia data such as video, audio and image are the example of data which are harder to be encrypted. Hence, this kind of data had 'rarer' security compared to words. The most often security used recently in today's industry is watermarking those multimedia data. However, watermarking can work on image and video only. Also, watermarking still available for people to view those data but prevent them from exploiting due to copyrights. However, if people who wish to make the data to be viewable by certain people only such as X-ray image of certain important people, watermarking probably will be not enough to accomplish that. Furthermore, people living in rural area often cannot access to hospital or medical help easily and immediately. Therefore, the objective of this project is to develop a system which can restrict the right to access to image data and using image encryption algorithms to protect those images to be extract by unauthorized person as well as helping people living in rural area to get medical consultation easier than before. In this project, students and lecturer from Faculty of Medicine and Health Science had become our target users. The image encryption technique that might involved were scrambling and diffusion. The outcome was that we can encrypt the X-ray image and the people with decryption key only can view the image. In the experiment phase, 3 of the selected algorithms was implemented as similar language as possible to produce more reliable result. The result was recorded including the run time and encrypted image size. The final selection of the algorithms depended on the encryption size and computation speed. The smallest size with the fastest computational speed was selected and through the result, the selected algorithm was DNA encoding.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1 Introduction

For this chapter, we will be discussing about the related introduction to this project. Problem background is the first aspect which will be embedded in 1.2. In 1.2, the problem which we meet this era is explained in this subtopic. Problem statement is the next aspect to be discussed. The problems which were explained in 1.2 were then stated briefly in 1.3. A portion in this chapter was occupied by project goal as this is important to why this project. The objectives of this chapter were explained in chapter 1.5. The following topics will be project scope which was chapter 1.6. In chapter 1.6, the target users, module and uses were discussed. The following chapters which were 1.7 and 1.8. The project timeline and organization of the project were presented respectively. The summary of this chapter was presented in chapter 1.9.

1.2 Problem Background

The quick progressions in innovation has prepared architects with simple to utilize and low-cost strategies to analyze and treat diseases. In the event that the persistent restorative records collected over suppliers within the shape of electronic therapeutic record (EMR) by distinctive frameworks and wearables is combined, the organization and preparing of information is conceivable past current clinical scenarios. Gratefully progresses in system robotization and cloud models can essentially decrease or dispose of numerous of the dangers in diagnosis/treatment related with healthcare setup. When worked in combination, the care-takers and patients can lead to productive ways of persistent wellbeing checking and conclusion, empowering exact alteration medications. Whereas there are openings there are moreover numerous challenges which can be managed with by scholarly people combining and utilizing clinical and shopper source information. Moreover inactive advances can be utilized to superior track quiet information in arrange to diminish dangers by programmed framework recuperation. So it is presently conceivable to supply superior healthcare through superior innovation. For example, IOT has proven to be an efficient technology which has equipped different systems in the E-healthcare sector to collect medical information from easy to use devices, view patient information and diagnose in real-time (Loan NA, Parah SA, Sheikh JA, Akhoon JA, Bhat GM, 2017) (Parah SA, Sheikh JA, Ahad F, Bhat GM, 2018). Viable healthcare depends on precision and speed of its administrations, for that a gigantic run of gadgets associated as IOT takes hold. It has been assessed that almost 50% of gadgets utilizing healthcare organizing stages will be based on IoT frameworks within the another few a long time.

Furthermore, due to the pandemic of Covid-19, people had to continue their daily under movement control operation (MCO). For people who can easily access to medical support, MCO definitely not a problem to them. But, for people living in rural area, having access to medical aid before MCO is already out of their hand, what to compare with current MCO situation. In order to get medical assistant, those people had to drive a large distance and long time to the nearest hospital. This might cause them to lose their golden time to get treatment. Therefore, real time medical consultation might save time and lives. Also, 24-hours on call doctors can have more time to rest if the emergency case can be settled by nurses or the patients themselves.

Besides, due to pandemic of Covid-19, people might prefer remote consultation compared to face-to-face consultation. This is because people might want to avoid crowd and reduce the risk of infecting Covid-19. According to some scientific research, the more face-to-face contact with others, the easier for ones to infect by Covid-19.

The rise in exchange of data through different systems utilizing web has postured various security issues to both the clients and benefit suppliers. In expansion, the accessibility of distinctive information altering apparatuses and hacking software's, the hazard to the data traded through diverse systems is additionally rising. In this situation most of the offices and organizations spend a part of cash to secure the data exchanged/stored whereas managing with sharing of information. With the increment of information trade over different systems, the prerequisite of plans which are theft-proof, hack-proof and piracy-proof has expanded relatively. In past few a long time, different state of craftsmanship arrangements have been proposed by analysts and other concerned educate to check the danger of information breaches[1] (Cox I, Miller M, Bloom J, Fridrich J, Kalker T, 2008) (Kumar C, Singh AK, Kumar P, Singh R, Singh S.) (Singh, AK, Kumar B, Singh SK, Ghrera SP, Mohan A, 2016). The most center of the people has been primarily within the wellbeing division, film industry, defense, space communication and social media. But until presently no strategy has been concocted which can give total security to the information trade. In differentiate, the modern challenges are rising quickly due to the powerlessness of the unreliable systems to foes. In this situation, it is exceedingly needed to plan a system which can guarantee the finest conceivable security and security to the clients trading delicate data. The most center of the people has been primarily within the wellbeing division, film industry, defense, space communication and social media. But until presently no strategy has been concocted which can give total security to the information trade. In differentiate, the modern challenges are rising quickly due to the powerlessness of the unreliable systems to foes. In this situation, it is exceedingly needed to plan a system which can guarantee the finest conceivable security and security to the clients trading delicate data.

The restorative pictures shared in an e-healthcare framework are exceptionally delicate to any information breach as they carry patient's private data

[1] https://online.norwich.edu/academic-programs/masters/nursing/resources/infographics/healthcare-data-breaches-the-costs-and-solutions.

fundamental for treatment of different maladies. Any alter in this therapeutic information can lead to the determination which may result to off-base medicines and indeed passing. In case of e-healthcare applications it is essential to guarantee astuteness and way better security whereas sharing of restorative pictures. Security and copyright security are the key prerequisites to guarantee dependable trade of data over distinctive stages which are ordinarily unreliable. In arrange to attain the over examined necessities the data is as a rule pre-processed some time recently transmission/storage. These pre-processing operations incorporate sifting, compression, equalization and different geometrical operations. Routine information security methods are able to guarantee information security to a few degree but the level of resistance against most of the commonly happening assaults isn't met up to an effective level. Advanced watermarking (WM) method, which includes covering up of a few mystery information in a few cover media has demonstrated to be one of the most excellent method for securing data trade. The information stowing away in watermarking includes the state of craftsmanship instruments which guarantee that visual quality is kept intaglio indeed after implanting extra information. The cover media in which mystery information, known as watermark, is put away may be an picture, sound or video record.

Digital watermarking algorithms are ordinarily executed agreeing to the necessity of application in one of the two spaces: spatial domain or transform domain. Spatial domain based plans offer basic plan, low computational complexity and great perceptual quality of watermarked pictures but the vigor is frail against flag preparing assaults. In differentiate, the plans actualized in change space tall vigor to the watermark at the taken a toll of a few design complexity. The commonly utilized change spaces incorporate DCT, DWT, SVD and IWT. The watermarking procedures can moreover be categorized on the premise of require of unique picture at the time of extraction of watermark. While dazzle WM techniques doesn’t require unique picture for extraction of watermark, non-blind method requires unique picture. The daze methods are prevalent ones due to the truth that the stack on the transmission capacity and capacity is less as watermark can be extricated remotely without require of cover picture.

It is for the most part required for watermarking plans to be multipurpose such that a single conspire can work for diverse applications. But larger part of WM

plans proposed until presently for the most part target a specific necessity such that a partitioned calculation is required for each application. A robust watermarking plot has been proposed with tall level security in arrange to guarantee the inventiveness and genuineness of the inserted information whereas being gotten. This can be done by scrambling the mystery information to be implanted by means of a one of a kind key taken after by implanting of this scrambled information by altering the change space coefficients of the cover picture. The cover image is partitioned into squares of settled measure taken after by application of transform domain technique (DCT) on the pieces. Watermark is at that point inserted in SVD coefficients by application of proposed watermarking calculation. The exploratory comes about appear that the conspire offers a extraordinary imperceptivity and vigor against all intentional/unintentional flag handling and geometrical assaults.

1.3 Problem Statement

i. Privacy of multimedia data is not concerned.

Due to the rapid growth of data exchange in today's society, data privacy is the main problem faced by everyone this era. In these data, multimedia data such as video, image and audio stand a large part. Therefore, these kind of data security had became essential. However, these kind of data had limited and fewer security present in real world. So, to make use these kind of data did not exploit by people, multimedia security is important especially medical report and imaging such as X-ray image, MRI image, echocardiogram image and other medical test image. This is because those medical images of some person might have a great impact on politics, bursa trading status or even security of a country. The online medical consultation system in Malaysia named SpeeDoc (www.speedoc.com/my), DoctorOnCall (www.doctoroncall.com.my) and Doctor2u (www.doctor2u.my) are insufficient to secure and encrypt medical imaging of user. With the access to the account, the medical imaging passes though the application or website can be stolen easily. By accessing to the database, the hackers can alter the image. This might cause serious problem like misdiagnose or cyber-ransom to patient. Though this proposed system, the images uploaded by both patient and doctor were encrypted before saving into database using image encryption algorithm. Therefore, without the correct key, people cannot retrieve the real image from the database.

ii. Difficulty of people to receive face-to-face medical consultation during pandemic of Covid-19.

Furthermore, the other problem is that people living in rural area sometimes difficult to access to medical support. Those people usually have to travel a long distance and take a lot of time to get medical aids. This might led them to miss their golden period to receive treatment. In this case, they might suffer from permanent disability or even death. From the reviewed system (SpeeDoc, DoctorOnCall and Doctor2u), most of them had a working hour on the system or queue to get responses. However, the proposed system aimed to notify the doctors whenever they get requested by email or short message service (SMS). So, the doctors can answer to his or her patient as soon as possible.

iii. Difficulty of doctor to perform their task on time.

Also, doctors on duty sometimes did not gain enough sleep and rest can cause serious mistake especially for those doctors who are 24-hours on call (PninaWeiss, MD, Meir Kryger, MD, Melissa Knauert, MD, PhD , 2016). Most of the time, after the duty, the medical personnel will take a recover sleep. However, in a study, internal medicine residents' sleepiness and mood swings persisted after the first recovery night, perhaps indicating the symptoms of prolonged sleep loss (Rose M, Manser T, Ware JC, 2008). Residents in anesthesiology have a hard time distinguishing microsleeps on an electroencephalogram. They failed to record sleep in 49 percent of the electroencephalogram-identified sleep episodes, and they were incorrect 76 percent of the time when they said they had remained awake (Howard SK, Gaba DM, Rosekind MR, Zarcone VP, 2002). Extended shifts have been linked to health hazards for residents, including vulnerability to blood-borne illnesses and car crashes (MVAs). Blood-borne pathogen infection is rare; in one study, 40 deaths per 1000 doctors in training occurred during the day (Parks DK, Yetman RJ, McNeese MC, Burau K, Smolensky MH, 2000). On the night shift, though, the sensitivity rate was 50 percent higher (Parks DK, Yetman RJ, McNeese MC, Burau K, Smolensky MH, 2000). Ayas et al. confirmed the elevated risk of percutaneous injury during the night shift (Ayas NT, Barger LK, Cade BE, Hashimoto DM, Rosner B, Cronin JW, Speizer FE, Czeisler CA, 2006); the risk was even greater while working a prolonged shift (>24 hours). Besides, due to pandemic of Covid-19, face-to-face consultation might raise the risk of proliferation of the plague. They can use this proposed system to give real time

instruction if the emergency cases are not a hard nut to crack. Also, this proposed system can help doctors to work from home which minimized the risk of spreading Covid-19 and help them get better rest quality on long time shift duty.

1.4 Project Objectives

I. To design a consultation system for doctors and patients which consist of real time video call and encrypted medical images functions.
II. To develop the proposed system embedded with the DNA sequence operation encryption.
III. To evaluate existing image encryption algorithms with comparing between the effects of the researched algorithms.

The goal of this proposed project is to allow people who have some difficulties due to some reason such as geometrical issue, transport issue, technological issue and especially during the pandemic of Covid-19. Therefore, this proposed system is aimed to provide a secured remote consultation to these people.

1.5 Project scope

Target User: UMS FPSK, people living in rural area, doctors, patients.

Module: login and register module, video call module, private chat module, embedded search element module, search module, image sender module

In terms of modules, the login and register module shall let the user to register an account using their personal information and login to the client-side system using their account. After account have been logged in, they will proceed to their account home page. The video call module allows the doctors and the patients to conduct remote consultation. The private chat module allows the doctors and patients to send text messages with each other. The embedded research element module allows the users to encrypt or decrypt the images using DNA sequence operation encryption. Search module allows the doctors to search for patients or vice versa. The image sender module allows the users to send images with each other via email.

Table 1.1 The proposed system module

Module	Description	Function
Login and register	Allows users to login and register to an account to the system to access to the users' function.	- To verify user register detail - To record and create an account - To verify email and password
Private chat module	Allows user to send text messages to each other.	-To send text messages
Video call module	Allows patient and doctor to perform video call for remote medical consultation	-To perform video call function
Embedded research module	Allows the users to encrypt and decrypt the images such as X-ray, echocardiogram and MRI images.	-To encrypt and decrypt images.
Search module	Allows doctors to search for patients and vice versa	-To search for their responsibility doctors or patients. - To add into list for remote consultation system.
Image sender module	Allows users to send images to each other via email	-To send images between the users.

1.6 Project Timeline

Table 1.2 Project Timeline

Task/Week	March	April	May	June

	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Project I																
Data Collection and Preliminary Study	**2 %**	**5 %**	**10 %**													
Interview				**11 %**												
Literature review								**20 %**								
Investigation on Scambling						**15 %**										
Investigation on Diffusion								**20 %**								
Algorithms Comparison								**25 %**								
System Design												**30 %**				
Experiment on Embeded Research Elements														**40 %**		
Report Writing															**50 %**	
																100 %

Table 1.3 Project II Timeline

Task\Week	October				November				December				January			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
System Development of proposed system														**85%**		
Implementation apps with an image encryption algorithm														**90%**		
Testing and Evaluation															**93%**	
Perform unit testing and system integration testing.															**95%**	
Report writing and documentation.																**100%**
																100%

1.7 Organisation of Report

This project consisted of 6 chapters which are Chapter 1 Introduction, Chapter 2 Literature Review, Chapter 3 Methodology, Chapter 4 System Analysis and Design.

Chapter 1 will discuss the introduction, problem statement and motivation, problem statements, project objectives, project scope, and organization of the report.

Chapter 2 will discuss literature reviews which consisted of the introduction to remote consultation, type image encryption techniques, method to implement the video call module and method to encrypt cloud computing system.