**CONTENTS**

1.0 Introduction..............................................................2

1.1 Purpose....................................................................2

1.2 Scope.......................................................................3

1.3 Related Study...........................................................3

2.0 SYSTEM REQUIREMENT SPECIFICATION...........4

2.1 Functional Requirement...........................................4

Requirement 1..........................................................4

Medical Images.................................................4

Requirement 2...........................................................4

Cryptosystem....................................................4

Requirement 3............................................................4

Pythagorean Triplets........................................4

Requirement 4............................................................4

Private Key.......................................................4

2.2 NON FUNCTIONAL REQUIREMENT....................5

3.0 PROPOSED METHOD...............................................6

4.0 JUSTIFICATION........................................................7

5.0 FLOW CHART............................................................8

6.0 BLOCK DIAGRAM....................................................9

7.0 ADVANTAGES........................................................10

8.0 SNAPSHOT 1...........................................................11

SNAPSHOT 2............................................................12

9.0 CONCLUSION...........................................................13

10.0 BIBILIOGRAPHY...................................................13

**CRYPTO SYSTEM FOR MEDICAL IMAGES**

**SOFTWARE REQUIREMENT SPECIFICATION**

1.0 .INTRODUCTION

Medical images are some of the greatest source of information and hence needs a strong security system for transit. They contain sensitive information about an individual which require confidentiality. This research proposes a new method that is based on Pythagorean triplets to encrypt the images; especially the medical images that have uniform backgrounds and confined regions of interest.

1.1.PURPOSE

Providing security for Medical data such as X-Ray, ECG, MRI, etc. has gained immense importance due to their sensitive nature. The penetration of Internet in all walks of life has made data sharing a necessity amongst hospital networks all over the globe which are in need of security system for their online data exchange. The usage of geometrical objects for encryption is a young area. The present research work explores one such option; the use of Pythagoras’s theorem for right angled triangle to encrypt medical images. The work proposes a crypto-system with considerable security with one requirement – the use of a secure channel for key exchange.

1.2.SCOPE

This is basically an system to demonstrate use of pythocrypt-crypto system for medical images using cryptography.

1.3. RELATED STUDY

The survey includes the study of some of the most eloquently described algorithms for medical image encryptions and a study of their performances under different circumstances. Most of the papers that have done research in this area propose the use of pixel positions and/or chaotic sequences of one dimension[1-3] Because of the nature of the Pseudo Random Number Generators (PRNG) used in these systems, the security provided becomes weak over largely varying sizes. Also the time taken becomes a proportionate variable to size and hence vulnerable to timing attack. Some algorithms use selective position encryption which provides a powerful security system. But the regional approach makes it slightly more vulnerable to brute force attack by a un trusted/system with prior knowledge of the type of images that are shared. An analysis of the boundary of encrypted region may divulge very useful information to the cryptanalyst. Some researchers have proposed the technique of dividing the images in multiple sub images based on the information pixel data and position. These systems target a very limited section (black and white) of medical images only. Most systems concentrate on monochrome or grey scale images and some are specifically designed for some standard available formats such as JPEG.

2.0 .SYSTEM REQUIREMENT SPECIFICATION

2.1.FUNCTIONAL REQUIREMENT

Input files: Medical images:

X-Ray,

MRI,

ECG.

Theorem used: Pythagoras theorem,Use of pythagorean triplets.

Cryptosystem.

Symmetric Encryption.

Private Key.

2.2.NON FUNCTIONAL REQUIREMENT

The Non Functional requirements for the application that will be developed will have the following factors:

**Performance**: To work properly, i.e. providing a “believable” augmented reality view to the user, the application should respond rapidly to the user’s movements. Moving the mobile device around changes the view of the user and thus, the displayed information should update accordingly.

**Maintainability**: Changing, adding and removing information and information sources should be facilitated. While users run the application base and make it available to the user’s afterwards.

**Usability :**It should be easy for the users to install and use the application. Functions should be clear, easy to find either self-explanatory or well-documented.

3.0.PROPOSED METHOD

Any given image with smaller well defined regions of interest and large uniform backgrounds such as X -rays, MRI scans etc. will have a high correlation among consecutive pixels. This creates it difficult to encrypt. Even large blocks of such files may have correlation with their neighbors. This method proposes that they have encrypted in such a way that the correlation is hidden or avoided as far as possible. We propose the use of Pythagorean triplets.

The mapping function is as follows.

C[i]=floor(F(P[j],K[i]))=floor(√P[j]^2 + K[i]^2) --------(1)

Where K[i]=F(P[i],K0) --------(2)

and K0 is the secret key selected by user.

The decryption function will simply be the inverse of the mapping function. The key K0 is used to generate subsequent keys. Plain text will be rounded up after computation to generate the actual pixel values.

4.0. JUSTIFICATION

This work was carried out because it was felt that the use of general purpose cryptosystems such as RSA, DES, 3-DES etc for medical image encryption would diminish their sanctity due to the nature of the images. Medical images have a very small region of interest and rest will be monochromatic. That would lead to the same data repeatedly encrypted with same key on any existing standard cryptosystem. The cryptanalyst would easily recognize the region of interest and he/she would also get a large amount of plain text to cipher text relation. Hence it was an idea to design an algorithm that can be specifically used for images with highly sensitive information concentrated in a small region of the image. The use of Pythagorean triplets was conceived as an idea for its divergence in backtracking and it can be substituted as the standard factorization problem.

5.0 FLOW CHART

Encryption process

Medical image

Import data from image

Encrypt image using algorithm

Encrypted image

Import data from encrypted image

Decrypt image using algorithm

Decryption process

Plain image

6.0 BLOCK DIAGRAM

Encryption Decryption

c[i]= (√P[j]^2 + K[i]^2) c[i]= (√P[i]^2-k[i]^2)

Symmetric key

Symmetric key

Plain image

Cipher image

Plain image

5.0 Advantages of Pythocrypt.

It can be seen from the analysis that the proposed system produces a cipher text file that can't be rendered in any standard application for images or text

.

● It works better under noisy conditions because of the bloating up of the ﬁ le during encryption.

● The system can be easily modified to work with any other ﬁ le types such as text, numerical data etc.

● It provides very strong protection against most available cryptanalysis techniques because of the multi-level encryption.

● Use of random sized words ensures varying cipher text values for same pixels as observed in multi character encryption

6.0. SNAPSHOTS

fig 1

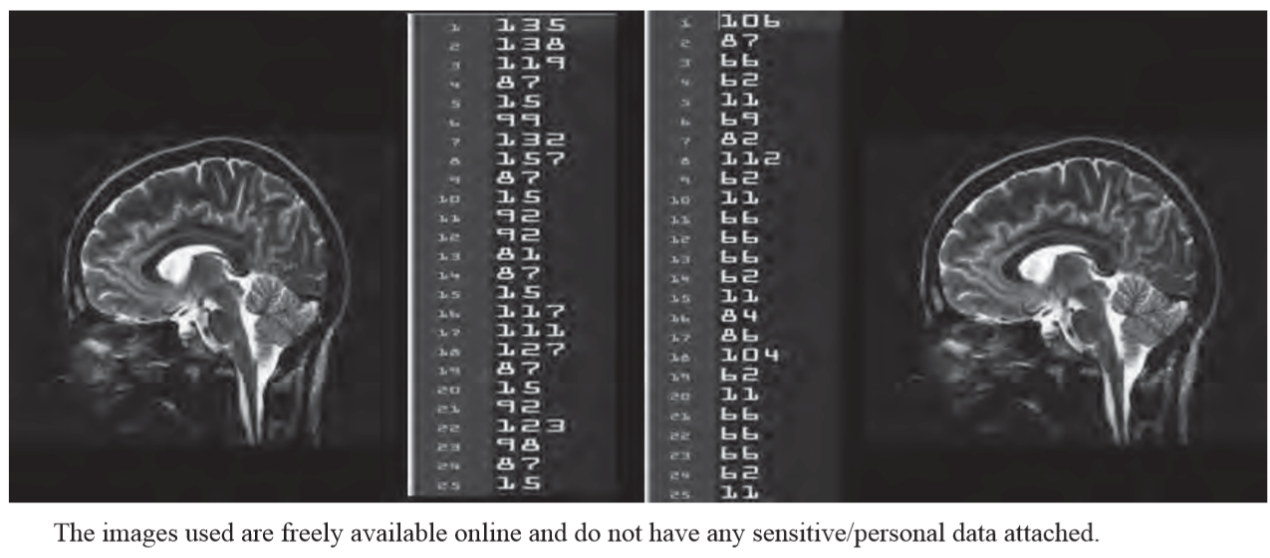


fig 2

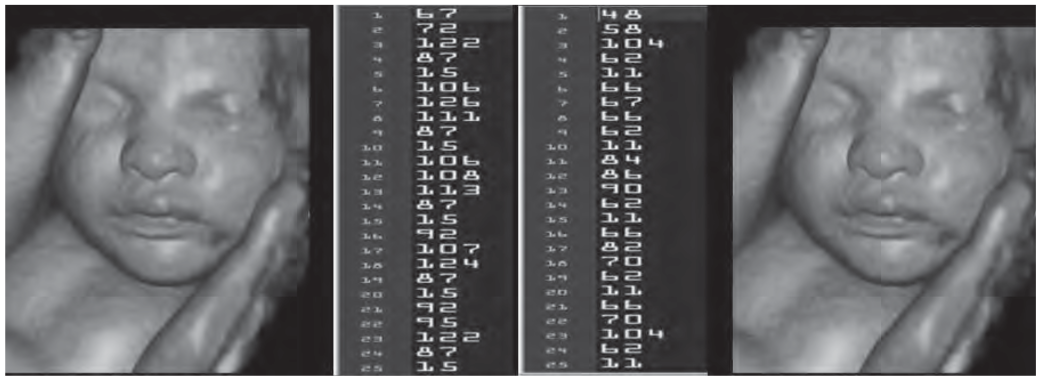
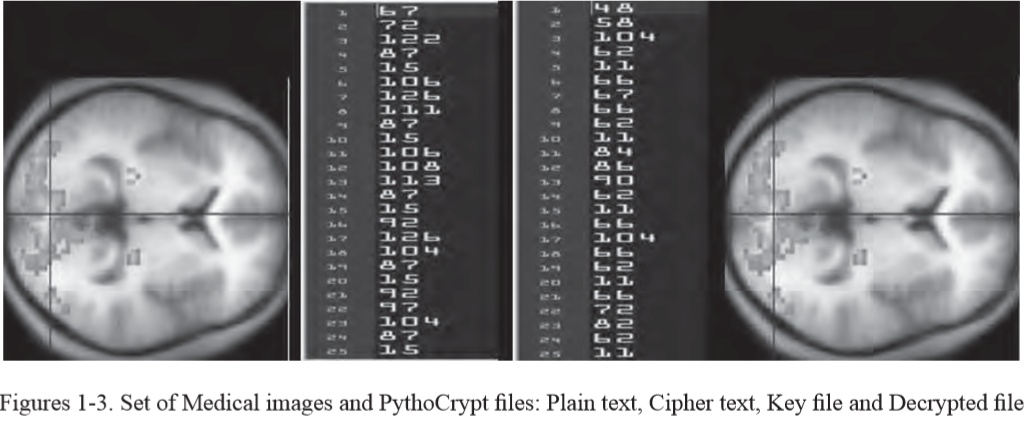


fig3

7.0 CONCLUSION

8.0 BIBILOGRAPHY