**SOFTWARE REQUIREMENT SPECIFICATION**

1. 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 phythocrypt-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 untrusted/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 iec. 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

2.0.1.FUNCTIONAL REQUIREMENT

Input files: Medical images:

X-Ray,

MRI scan.

Theorem used: Pythagoras theorem..

Use of Pythogorean triplets.

2.0.2.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 difficulty to encrypt. Even large blocks of such files may have correlation with their neighbours. 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[1].

The mapping function is as follows.

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

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

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 Advantages of pythocrypt

It can be seen from the analysis that the proposed system produces a cipher text ﬁle that can not 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

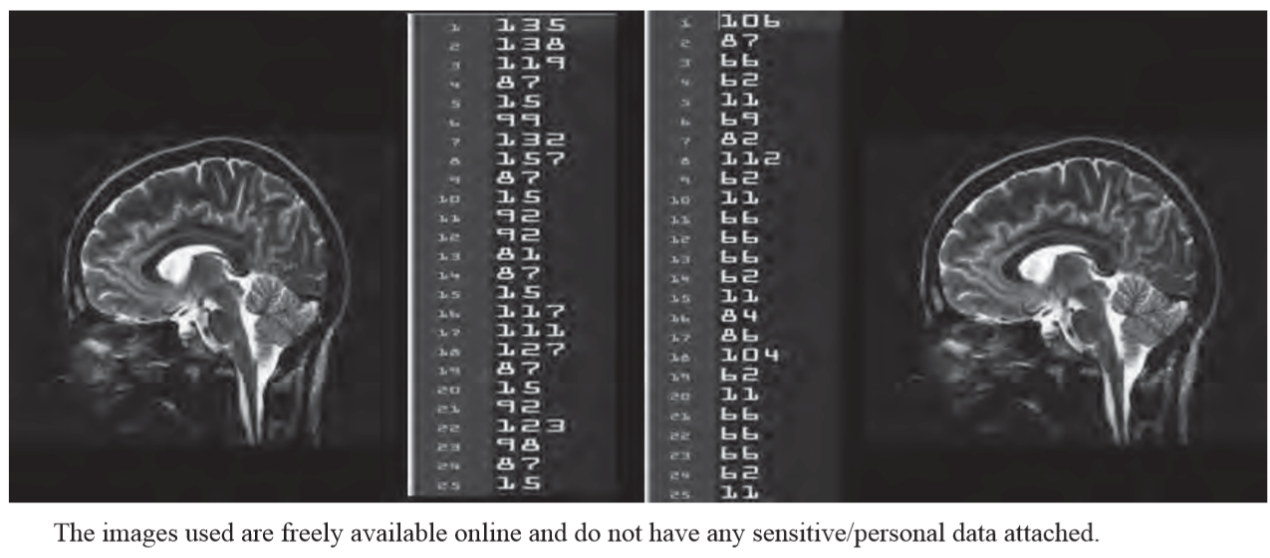


fig 2

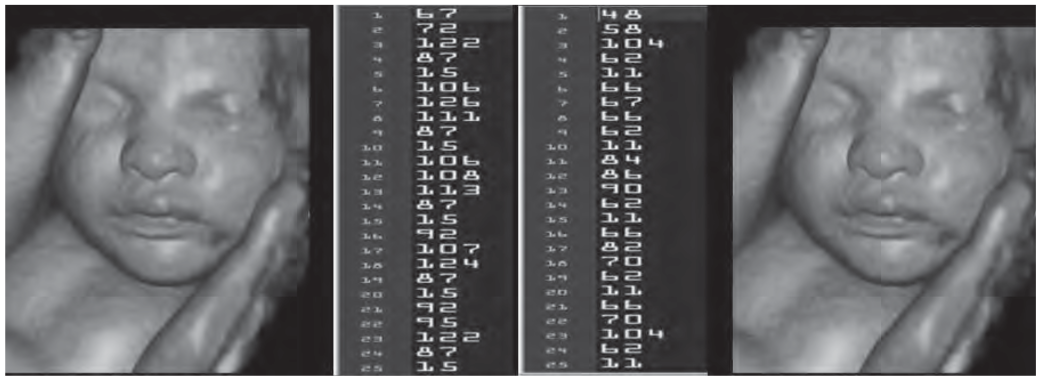


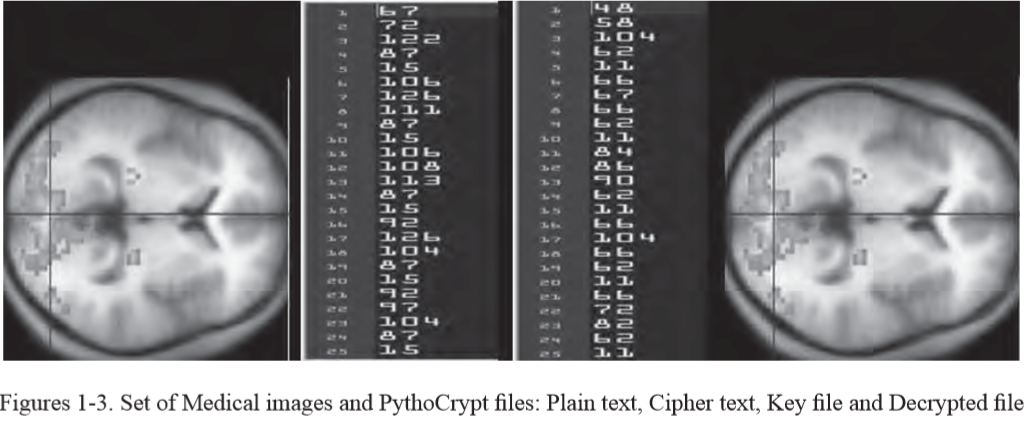
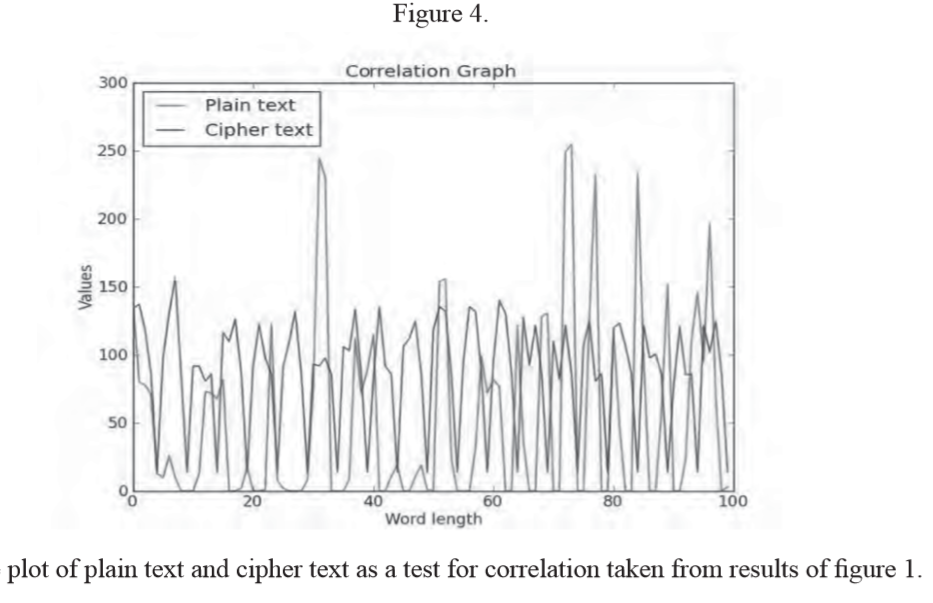
fig3

fig 4



7.0 CONCLUSION

Pythocrypt as is a unique promising cryptosystem particularly powerful when used on medical images and frequency based transformation sensitive data. It fares well in noisy conditions and with the protected sharing of key assured, it offers a stable and robust security system.