IMAGE ENCRYPTION AND IMAGE TO IMAGE STEGANOGRAPHY

PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF BACHELOR OF TECHNOLOGY IN DEPARTMENT OF INFORMATION TECHNOLOGY

BY

NAME	Registration No:	Roll No:
ANANNYA CHANDRA	121420110064	14200212001
MEGHNA NAG	121420110087	14200212024
NIDHI KUMARI	121420110090	14200212027
SOURAV DAS	121420110111	14200212048

Under The Supervision of
INDRAJIT DAS

DEPARTMENT OF INFORMATION TECHNOLOGY

MEGHNAD SAHA INSTITUTE OF TECHNOLOGY

Techno Complex, Madurdaha, Beside NRI Complex, post-Uchhepota, Kolkata-700150

Affiliated by

MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WEST BENGAL

NOVEMBER 2015

CANDIDATE'S DECLARATION

I hereby declare that the work which is being presented in the project entitled 'IMAGE ENCRYPTION AND IMAGE TO IMAGE STEGANOGRAPHY' in partial fulfillment of requirements for the award of degree of B.Tech. in IT, submitted in the Department of Information Technology at **MEGHNAD SAHA INSTITUTE OF TECHNOLOLY** under **WEST BEGNAL UNIVERSITY OF TECHNOLOGY, KOLKATA** is an authentic record of our own work carried out during Odd Semester 2015 under the supervision of **Indrajit Das.** The matter presented in this project has not been submitted by us in any other University / Institute for any award.

Signature of the Students
With Date

Meghnad Saha Institute of Technology
Nazirabad, P.O. :Utchepota, Via Sonarpur, Kolkata 700 150

CERTIFICATE

This is to certify that the Project entitled 'IMAGE ENCRYPTION AND IMAGE TO IMAGE STEGANOGRAPHY' is being submitted by **Anannya Chandra** in partial fulfillment of the requirement for the award of the degree of B.Tech.in IT to the Department of Information Technology, Meghnad Saha Institute of Technology, Kolkata, is a record of bonafied work carried out by her under my guidance and supervision from 16^{th} June 2015 to 15^{th} June 2016.

The results presented in this thesis have been verified and are found to be satisfactory. The results embodied in this thesis have not been submitted to any other University for the award of any other degree or diploma.

……………………………………….

Indrajit Das
Assistant Professor
Information Technology
Meghnad Saha Institute of Technology
Kolkata-700150

Signature of the Supervisor

Date:

Place:

Meghnad Saha Institute of Technology

Nazirabad, P.O. :Utchepota, Via Sonarpur, Kolkata 700 150

CERTIFICATE OF APPROVAL

The foregoing project entitled 'IMAGE ENCRYPTION AND IMAGE TO IMAGE STEGANOGRAPHY' is hereby approved as a creditable study of an engineering subject carried out and presented in a manner satisfactory to warrant its acceptance as prerequisite for the degree for which it has been submitted. It is to be understood that by this approval the undersigned do not necessarily endorse or approve any statement made, opinion expressed or conclusion drawn therein but approve the thesis only for the purpose for which it has been submitted.

Board of Examiners ______________________________

____

____

____

____

Supervisor ______________________________

Head of the Department ______________________________

Date:

Place: Kolkata

[Departmental & College Seal]

Acknowledgement

Life as a researcher is a zigzag way and has many ups and downs, but I overcome from them because of the support and faith of many individuals.

First and foremost I would like to express my sincere gratitude to **Mr. Indrajit Das** for providing me an opportunity to work with him. Your creativity encouraged me, your energy and dedication towards work motivates me. Your perfection always inspired me to do things perfectly. I feel motivated and encouraged every time I attend your meeting. Without your encouragement, inspiration and guidance this thesis dissertation would not have materialized. Thank you so much for not only guiding me in this thesis dissertation but for every knowledge you give me. This thesis dissertation is dedicated to your creativity and enthusiasm of doing work.

I wish to thank many people for their direct or indirect help in achieving this goal. Special thanks to my parents for their support and encouragement throughout my study, their faith in me ignite that spark to do anything for their happiness.

Last but not least I would like to thank all my friends for being with me at each step when I needed their support. This thesis will never be successful without your support and love.

(Signature of the Students)

Anannya Chandra

Abstract

The necessity of fast and secure diagnosis is vital in the medical world. Nowadays, the transmission of images is a daily routine and it is necessary to find an efficient way to transmit them over the Internet. In this project we propose a new technique to cipher an image for safe and de-noised transmission employing image encryption and image to image steganography. The hospitals and health systems in general are entrusted the tedious task of managing and supervising huge volume of medical and patient information. Owing to the extreme popularity and potential of cloud computing in recent times, in this paper its usage in secure storage, archiving and accessing of medical images and data is considered as an appealing recourse to the healthcare infrastructure for enhanced patient care.

Keywords—image encryption;decryption; image to image steganography; cloud computing

TABLE OF CONTENTS

List of Tables

List of Figures

1. INTRODUCTION

Medical Image Sharing is a phrase coined for the electronic exchange of medical information and images among hospitals, physicians and patients. The ability to instantly and electronically exchange medical information over internet can actually enhance and facilitate speedy and efficient diagnosis of critical ailments by means of communication among renowned physicians, as well as with patients. The significance of secure, speedy diagnosis in the domain of medical world mandates the need for safe transmission of digital medical images over the Internet. So in this project we advocate the usage of image encryption and image to image steganography for safe and secure transference of medical images. Besides the monotonous job of administering and organizing enormous medical images and patient information assigned to the healthcare organizations is an upcoming and rising point of concern worldwide. Technology nowadays permits sharing of medical images using the clouds rather than usage of traditional media like CD, DVD or physical shipment of medical data to patients. Owing to the pioneering potential and sensational popularity of the Cloud Computing arena, its utilization for reliable hoarding of sensitive medical images and information is recommended in this project for secure caching and speedy access of medical images in cloud environment.

1. METHODOLOGY

The working principle used in this work produce a simple and secure solution for transmission of image through a network. This technique is easy to implement and understand. The procedure starts by encrypting the medical image and then embedding it in cover image by Image to Image steganography. In receiving end, the receiver first applies reverse steganography and then decrypts it to retrieve the original medical image. Thus integration of both this techniques ensures a two layer security model thereby protecting the medical image from outside world intrusions.

The entire procedure of the project is presented pictorially in FIGURE 1.

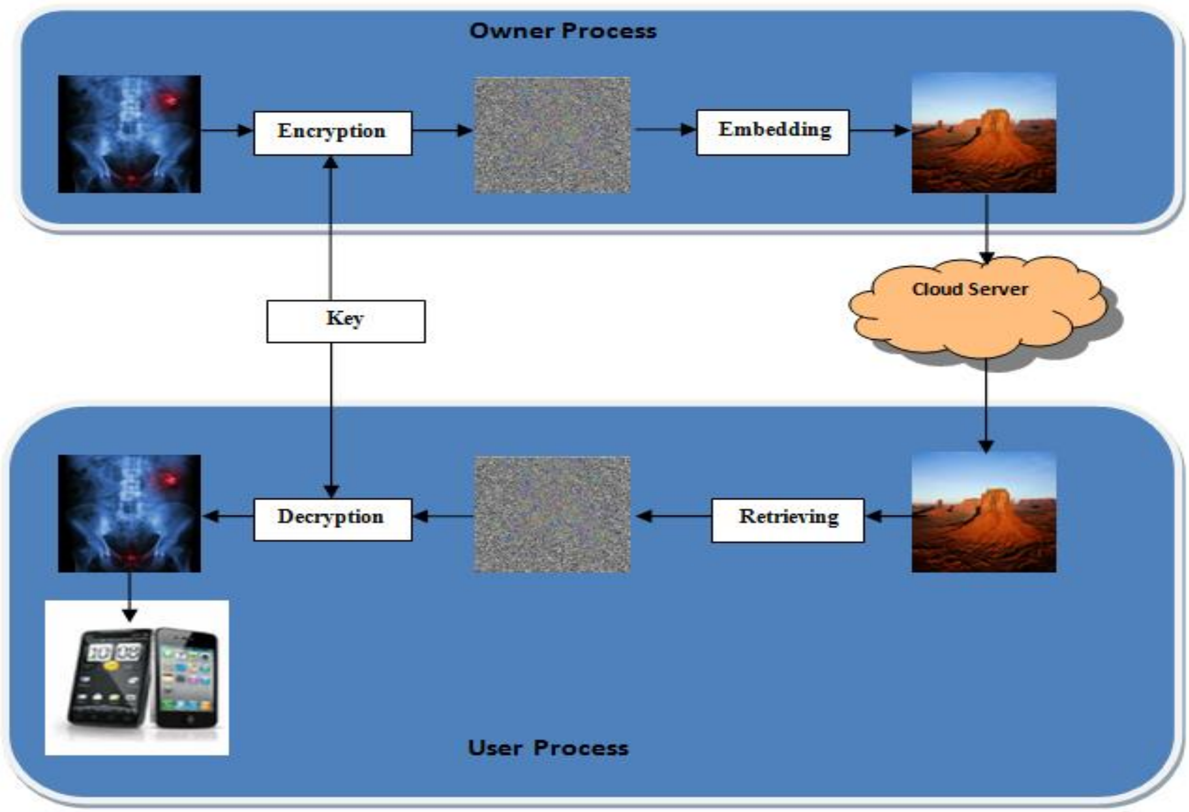


FIGURE 1

The following discussion gives a brief idea about the methodology involved in the entire work. We use symmetric key cryptography to achieve our first purpose of encrypting the medical image. The 'private-key' cryptography uses the logic of XOR gate which has the reversible property in it making the process of encryption and decryption very easy. The algorithm of the encryption is given below.

2.1 IMAGE ENCRYPTION:

```
global Img ;

global EncImg;

global key;

EncImg = imageProcess(Img,key);

imshow(EncImg);

imwrite(EncImg, 'Encrypted.jpg', 'jpg');
```

2.2 IMAGE PROCESS:

```
function [proImageOut] = imageProcess(ImgInp,key)

[n m k] = size(ImgInp);

% key =cell2mat(struct2cell( load('key5.mat')));

% key = keyGen(n*m);

for ind = 1 : m

    Fkey(:,ind) = key((1+(ind-1)*n) : (((ind-1)*n)+n));

end

len = n;

bre = m;

for ind = 1 : k

    Img = ImgInp(:,:,ind);

for ind1 = 1 : len

    for ind2 = 1 : bre

        proImage(ind1,ind2)=bitxor(Img(ind1,ind2),Fkey(ind1,ind2));

    end

end

proImageOut(:,:,ind) = proImage(:,:,1);

end

% figure,imshow(proImageOut);

return;
```

2.3 KEY GENERATION:

```
function [key] = keyGen(n)

n = n*8;
```

```
% n = 2048*2048*16;

% n = 24 * 24 * 8;

bin_x = zeros(n,1, ‘uint8’);

r = 3.9999998;

bin_x_N_Minus_1 =  0.300001;

x_N = 0;

tic

for ind = 2 : n

    x_N = 1 - 2* bin_x_N_Minus_1 * bin_x_N_Minus_1;

     if (x_N > 0.0)

        bin_x(ind-1) = 1;

    end

     bin_x_N_Minus_1 =  x_N;

end

toc

% save bin_sec bin_x;

t = uint8(0);

key = zeros(n/8,1, ‘uint8’);

for ind1 = 1 : n/8

    for ind2 = 1 : 8

    key(ind1) = key(ind1) + bin_x(ind2*ind1)* 2 ^ (ind2-1);

    end

end
```

An example, if the proposed process of encryption is implemented successfully (FIGURE 2):

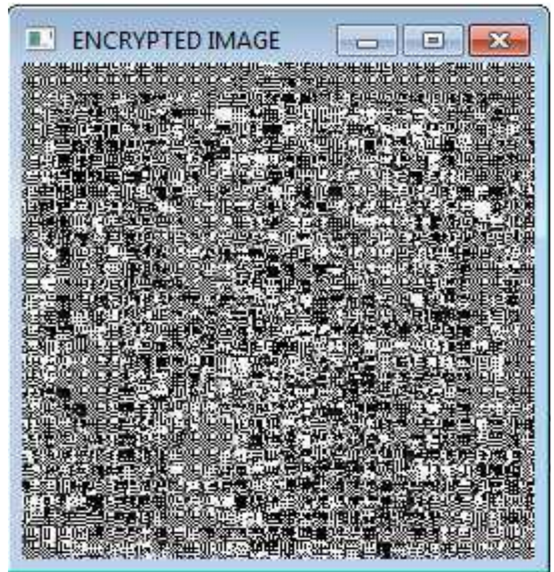


Fig: 2.1) Original Image

Fig: 2.2) Encrypted Image

For the implementation of the second step i.e Image to Image steganography we will use the Embedding algorithm namely- LSB substitution. The sequential steps are given below.

2.4 EMBEDDING ALGORITHM: LSB SUBSTITUTION:

Step 1:

Take an image say cover image.

Step2:

Scan or take input of the data to be embedded inside the cover image say Image.

Step 3:

Find number of pixels inside the Image and store the number as Tot_char.

Step 4:

Find out the number of total pixels in the cover image, store it in Tot_pixels. Necessary info resides in the 1st few pixels of any image for BMP images, so its better not to be tampered, hence, leave first 54 bits of the cover image (in case of BMP images) and from the rest choose pixels to be embedded. Say the first pixel is IC [init]. Otherwise, for JPEG images we can choose any pixel for operation, even from 1st bit.

Step 5:

Convert each pixel of the Image into 8-bit binary form and store in another array say M1.

Step 6:

Say we have Tot_pixel= n. Now each cover pixel can store just 1 bit of Image pixel. So to embed 1 pixel of Image totally we need 8 pixels of cover image. Hence to embed 'n' number of Image pixels we need 8*n number of pixels. So if starting cover pixel is IC[init] then the embedding will run till the pixel value IC[init+8*n]. If there remains insufficient number of pixels left in the image after leaving first 54 cover pixels (for a BMP image) show an error message "Larger cover image is needed".

Step 7:

Say First_pixel be the first pixel of M1 [initial] array, where initial=0 of the Image in 8-bit format. Take pointer=7. In last bit of cover image i.e. 8^{th} bit of IC [init] embed 1stbit of Image i.e. MSB of First_pixel. So pointer=7, denotes the position of the bits of the pixel to be embedded.

Step 8:

Do any of the four sub steps (a) through (d)

(a) If the LSB of the cover pixel is 1 and the MSB of the pixel is 1, then retain the LSB of the cover pixel as it is.

(b) If the LSB of the cover pixel is 1 and the MSB of the pixel is 0, then change the LSB of the cover pixel as 0.

(c) If the LSB of the cover pixel is 0 and the MSB of the pixel is 1, then change the LSB of the cover pixel as 1.

(d) If the LSB of the cover pixel is 0 and the MSB of the pixel is 0, then retain the LSB of the cover pixel as it is.

Set pointer=pointer-1

IC[init]=IC[init+1]

Continue while (pointer=0)

Step 9:

If pointer=0

First_pixel=M1[initial+1]

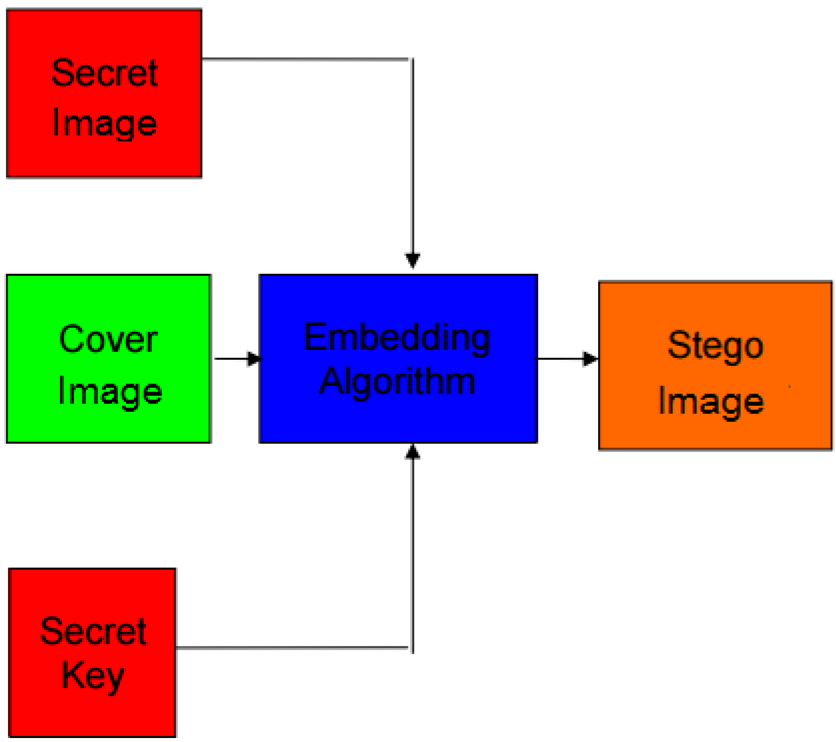
Pointer =7

Continue step 7 to 8.

While First_pixel reaches M1[Tot_pixel].

LSB Of Cover Bit	MSB of Image Pixel	LSB of Substituted Cover Pixel
0	0	0
0	1	1
1	0	0
1	1	1

The table here shows the logic applied to LSB Substitution, pixel to pixel wise (TABLE 1)



The working principle of steganography is shown in (FIGURE 3)

The outcome of this process produces stego message which traverses through the server and the network. After the successful transmission of the message to the desired recipient, he/she needs to understand it, for that, retrieval of the message from cover pixels is very necessary. This is achieved by the application of the reverse techniques of the aforementioned algorithms. The first technique is – Reverse Steganography. The steps of the algorithm are described serially below.

2.5 REVERSE STEGANOGRAPHY:

Step 1:

Take an array of Image as RM, i.e. retrieved Image where to store retrieved Data. Keep the pivot at RM[init]. Where init=0 initially.

Step2:

Take another array named RChar[8] to store each bit of retrieved data.

Step3:

Read cover pixel.

Set k=7.

(A) If the LSB of the cover pixel is 1, copy that and store as MSBof Rpixel[K]. RM stands for retrieved message.

K=k-1

(B)If the LSB of the cover pixel is 0, copy that and store as MSB of Rpixel [K]. RM stands for retrieved message.

K=k-1

Continue the process till k=0.

Step 5:

Store the data at RM[init]. Where initially init=0;

Step 6:

init=init+1

go to step2.

Step 7:

Abort operation when all cover pixels will be read.

Step 8:

Show RM as output.

After the process of reverse steganography the cover image is discarded, but one more layer of ambiguity is provided in our work for security. For the proper comprehension of the message by the receiver the process of decryption is applied. The algorithm along with the comparison of the original and decrypted image is described below.

2.6 IMAGE DECRYPTION:

```
global DecImg;

global EncImg;

global key;

DecImg = imageProcess(EncImg,key);

Imshow(DecImg);

imwrite(DecImg, ‘Decrypted.jpg’, ‘jpg’);
```

Note- The process of imageProcess() is defined above. Refer page 8 of 23.

2.7 COMPARISON OF ORIGINAL AND DECRYPTED IMAGE:

```
[r,c] = size(Img);

[r1,c1] = size(DecImg);

if(r==r1 && c==c1)

    fprintf('\n\n Bingo!!!! \n');

else

    fprintf('\n\n bugger!!!! \n');

end

for i=1:r

  for j=1:c

    if(Img(i,j)~= DecImg(i,j))

      fprintf('\n\n Changed!!!! \n');

    else
```

```
            fprintf('\n\n Success!!!! \n');
        end
    end
end
```

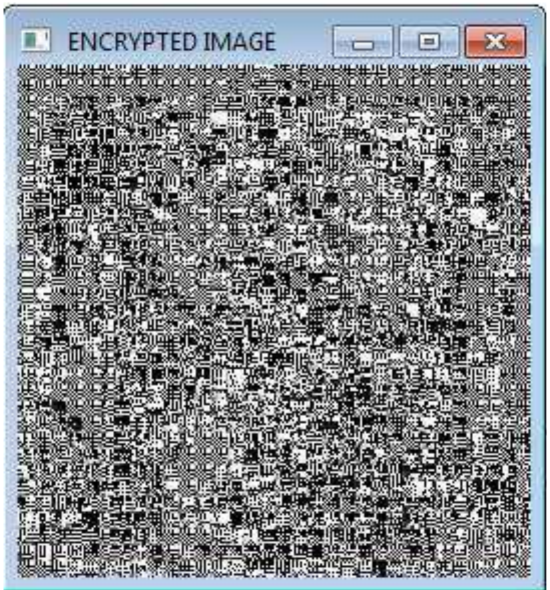


Fig: 4.1) Encrypted Image

Fig: 4.2) Decrypted Image

Therefore, the aforementioned synopsis of the proposed idea provides a 2 layer protection to our private message. The usage of image to image steganography method will help us to achieve the purpose.

3.REFERENCES

[1] Divya, V.V. Sudha, S.K. Resmy, V.R. (2012). *Simple and Secure Image Encryption*, Volume. 9, Page 286-289.
[2] S, Deepa. R, Umarani. (2013). *A Study on Digital Image Steganography*. Volume 3. Page 54-57.
[3] http://www.ims.nus.edu.sg/Programs/imgsci/files/memon/sing_stego.pdf
[4] http://www.cs.cornell.edu/courses/cs5430/2010sp/TL03.symmetric.html
[5] http://crypto.stackexchange.com/questio/+ns/19470/how-is-xor-used-for-encryption.
[6] W. Puech" Image Encryption and Compression for Medical Image Security" PROCEEDING OF IEEE Image Processing Theory, Tools &Applications.

[7] Ming YANG,Lei SONG,Monica TRIFAS,Dorothy BUENOS-AIRES,Lei CHEN, Jaleesa ELSTON," Secure Patient Information and Privacy in Medical Imaging IEEE " F. Gonzalez and J. Hernandez, " A tutorial on Digital Watermarking ", In IEEE annual Carnahan conference on security technology, Spain, 1999.

[8] Xinpeng Zhang]ieee signal processing letters, VOL. 18, NO. 4, APRIL 2011 255 Reversible Data Hiding in Encrypted ImageJ. Eggers, J. Su and B. Girod," Robustness of a Blind Image Watermarking Scheme", Proc. IEEE Int. Conf. on Image Proc., Vancouver, 2000.

[9] Eman AbuKhousa, Nader Mohamed and Jameela Al-Jaroodi," e-Health Cloud: Opportunities and Challenges", Future Internet 2012, 4, 621-645;

[10] Munchh, H., Engelmann , U., Schroeter, A., and Meinzer, H.: 'Web-based distribution of radiological images from PACS to EPR',International Congress Series., 2003, 1256, pp. 873-879.

[11] Boucherkha. S and Benmohamed . M.: 'A Lossless Watermarking Based Authentication System For Medical Images'. Proc. of International Conference on Computational Intelligence, Istanbul, Turkey, 2004, pp. 240-243.

[12] Pitt, D., et al.: 'Imaging cortical lesions in multiple sclerosis with ultra-high-field magnetic resonance imaging',Archives of Neurology, 67(7), 2010, pp. 812-818.

[13] A. K. Al-Frajat and H. Jalab.: 'On the differences between hiding information and cryptography techniques: An overview', Journal of Applied Sciences, 2010, vol. 10, (15), pp. 1650-1655.

[14] Teng CC, Mitchell J, Walker C, Swan A, Davila C, et al. (2010) A Medical Image Archive Solution in the Cloud. Software Engineering and Service Sciences (ICSESS), IEEE International Conference, Beijing, China.

[15] Shimrat,O.CloudComputing and Healthcare. Available online: http://www.himss.org/content/files/Code%2093_Shimrat_CloudComputingandHealthcare_2009.pdf (accessed on 28 June 2012).

[16] Teng, C.C.; Mitchell, J.; Walker, C. A Medical Image Archive Solution in the Cloud. In Proceedings of the 2010 IEEE International Conference on Software Engineering and Service Sciences (ICSESS), Beijing, China, 16–18 July 2010; pp. 431–434

[17] Cloud Computing: Clear Benefits: The Emerging Role of Cloud Computing in Healthcare Information Systems. Available online: http://www.techrepublic.com/whitepapers/ cloud-computing-clear-benefits-the-emerging-role-of-cloud-computing-in-healthcareinformationsystems/2384337 (accessed on 28 June 2012).

[18]Kaletsch, A.; Sunyaev, A. Privacy Engineering: Personal Health Records in Cloud Computing Environments. In Proceedings of the 32nd International Conference on Information Systems (ICIS 2011), Shanghai, China, 4–7 December 2011; pp. 1–11.

[19]Kaletsch, A.; Sunyaev, A. Privacy Engineering: Personal Health Records in Cloud Computing Environments. In Proceedings of the International Conference on Information Systems (ICIS 2011), Shanghai, China, 4–7 December 2011.