Visual Cryptography Based on Shuffling Method for Securing Medical Images

Alaa Aldein Mohamed Suleiman and Dr. Faisal Mohammed Abdalla
E-mail: alaabosla@gmail.com fabdalla@hotmail.com

Abstract: The increased growth in the use of transmission of multimedia medical contents over unsecured and open networks provides insecurity for confidential patient information over these networks. Digital encryption of medical images before transmission and storage is proposed as a way to effectively provide protection of patient information. Encryption of these images is necessary in order to ensure inaccessibility of information to unauthorized personnel with patient. This paper presented a visual cryptographic technique for encrypting of medical images before transmission or storage of them. This will make such images inaccessible by unauthorized personnel and also ensures confidentiality. The process made use of an encryption technique that is based on pixel shuffling and a secret key generated from the image.

The implantation of the algorithm was done using MATLAB Version 7.8.0 R2009a The algorithm was written in m-file and tested on sample of medical images.

Keywords: **Visual Cryptography, encryption, Decryption, secret information, share, stacking, secret key.**

المستخلص

يؤدي النمو المتزايد في استخدام نقل محتوى الوسائط الطبية عبر شبكات غير آمنة ومفتوحة إلى إنعدام الأمن لمعلومات المريض السرية عبر هذه الشبكات. تم إقتراح التشفير الرقمي للصور الطبية قبل النقل والتخزين كوسيلة لتوفير حماية فعالة لمعلومات المريض. يعد تشفير هذه الصور ضروريًا لضمان عدم إمكانية الوصول إلى المعلومات للأفراد غير المصرح لهم بذلك.

قدمت هذه الورقة تقنية تشفير بصري لتشفير الصور الطبية قبل نقلها أو تخزينها. سيؤدي ذلك إلى جعل هذه الصور غير قابلة للوصول إلى الأفراد غير المصرح لهم ويضمن أيضًا السرية والمحافظة على الخصوصية. تعتمد تقنية التشفير هذه على خلط البكسل (Pixel shuffling) ومفتاح تشفير تم توليده من الصورة .

تم تنفيذ الخوارزمية باستخدام MATLAB الإصدار 7.8.0 .R2009a تمت كتابة الخوارزمية في M-file وتم اختبارها على عينة من الصور الطبية.

الكلمات المفتاحية: التشفير المرئي، التشفير، فك التشفير، المعلومات السرية، فصل، دمج، المفتاح السري

1. INTRODUCTION

The concept of securing messages through cryptography has a long history. Indeed, Julius Caesar is credited with creating one of the earliest cryptographic systems to send military messages to his generals[1].

Throughout history, however, there has been one central problem limiting

Widespread use of cryptography. That problem is key management. In cryptographic systems, the term key refers to a numerical value used by an algorithm to alter information, making that information secure and visible only to individuals who have the corresponding key to recover the information. Consequently, the term key management refers to the secure administration of keys to provide them to users where and when they are required [1].

Historically, encryption systems used what is known as symmetric cryptography. Symmetric cryptography uses the same key for both encryption and decryption. Using symmetric cryptography, it is safe to send encrypted messages without fear of interception (because an interceptor is unlikely to be able to decipher the message); however, there always remains the difficult problem of how to securely transfer the key to the recipients of a message so that they can decrypt the message. A major advance in cryptography occurred with the invention of public-key cryptography. The primary feature of public-key cryptography is that it removes the need to use the same key for encryption and decryption. With public-key cryptography, keys come in pairs of matched “public” and “private” keys [1].

The public portion of the key pair can be distributed in a public manner without compromising the private portion, which must be kept secret by its owner. An operation (for example, encryption) done with the public key can only be undone with the corresponding private key [1].

The usage of the internet for the transmission of multimedia content has become a very frequent medium for the exchange of digital information almost all institutions that are using the internet. It is therefore important to secure data over open and unsecured networks in order to ensure safety of sensitive data. Medical information of patients is sensitive and needed to be protected during storage, and during transmission between two hospitals. When a physician receives a visit from a patient, he often requires a specialist opinion before giving a diagnosis. One possible solution is to send images of the patient, along with a specialist report, over a computer network. Nevertheless, computer networks are complex and espionage is a potential risk. We are therefore faced with a real security problem when sending data. For ethical reasons, medical imagery cannot be sent when such a risk is present, and has to be better protected hence the usage of cryptography in the protection of such data is very crucial. The cryptography in digital computing has been applied to different kinds of digital file formats such as text, images video etc [2].One of the best-known techniques of visual cryptography has been credited to Moni Naor and Adi Shamir.

The main concept of the original visual cryptography scheme is to encrypt a secret image into some shares. Secret information cannot be revealed with few shares. All shares are necessary to combine to reveal the secret image. There has been a steadily growing interest in visual cryptography. Visual cryptography is simple, secure and effective cryptographic scheme [3].

2. THE OBJECTIVES

1- To provide confidentiality to sensitive patient information.

2- Encourage the concept of telemedicine with assurance of data privacy.

3. RELATED WORKS:

Shyamalendu Kandar , Arnab Maiti [4]:They proposed a variable length Symmetric Key based Visual Cryptographic Scheme for color images where a secret key is used to encrypt the image and division of the encrypted image is done using Random Number. Unless the secret key, the original image will not be decrypted. Here secret key ensures the security of the scheme and visual cryptography is used to break the image into number of shares. Over all process below:

Step I: Any combination of characters [Characters, Numbers and Special Symbol] of any length is taken as KEY, which is XOR Ed with the pixel array computed from the original image. This makes the image blur to some extent.

Step II: The encrypted image is divided into n number of shares

using k-n secret sharing visual cryptography scheme such that k number of shares is sufficient to reconstruct the encrypted image.

Step III: k number of shares produced in Step II is stacked together to reconstruct the encrypted image.

Step IV: The KEY taken in Step I is XOR ed with the image produced in Step III, to generate the original image.

Mandal, J.K. and Ghatak, S. [5]: In proposed a novel (2, m + 1) visual cryptographic technique, where m number of secret images were encrypted based on a randomly generated master as a common share for all secrets which was decodable with any of the shares in conjunction with master share out of m + 1 generated shares. Instead of generating new pixels for share except the master share, hamming weight of the blocks of the secret images were been modified using random function to generate shares corresponding to the secrets. At the end of their work, the proposed scheme was secure and very easy to implement like other existing techniques of visual cryptography. At the decoding end the secrets were revealed by stacking the master share on any one share corresponding to the secrets in any arbitrary order with proper alignment directly by human visual system where shares were printed on different transparencies which conforms the optimality of using shares. The aspect ratio and dimension of the secret images and the generated shares with respect to the source images remained constant during the process.

Quist-Aphetsi Kester [6]: developed a cipher algorithm for image encryption of m*n size by shuffling the RGB pixel values. The algorithm ultimately makes it possible for encryption and decryption of the images based on the RGB pixel. The algorithm was implemented effectively without change in the image size and was no loss of image information after decryption.

4. METHODOLOGY:

For encryption, firstly, a secret key will be generated then a summation of the key with the original image will take place. Then, the key will be used to encrypt the plain image (the original image) using the function:

$$\mathrm{sk} = \left[\left|(He - Pi)\right| + (a \times b) + \left|\left(\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i\right)\right|\right] \bmod a$$

After that, the encrypted image will be separated into three platters; that is to extract the RGB from that image. Each of which will be composed with the same bits and pixels of the original image but with one extracted colour: first platter will produce the image with only the red ratio for all pixels from that image, the second one contains pixels with only blue ratio, and the third one contains just the green ratio of that pixels.

The generated key will be used then once again to encrypt each platter individually and separately from the other. And then each platter will get permuted; that is to exchange the locations of columns of pixels with the rows. Finally, reshaping the resultant platters will be performed for each platter; the numerical values of the pixels for that platter are then displaced from their respective positions to arrive finally to what is called 'share'- the encrypted pattern. In decryption process, the vice-versa of the whole operations that we performed earlier in the encryption will be done. The key is used to subtract the numeric values of the image instead of summation. Last step in decryption is that to stack the shares in order to get the original image .The processes are shown in figure 1: below.

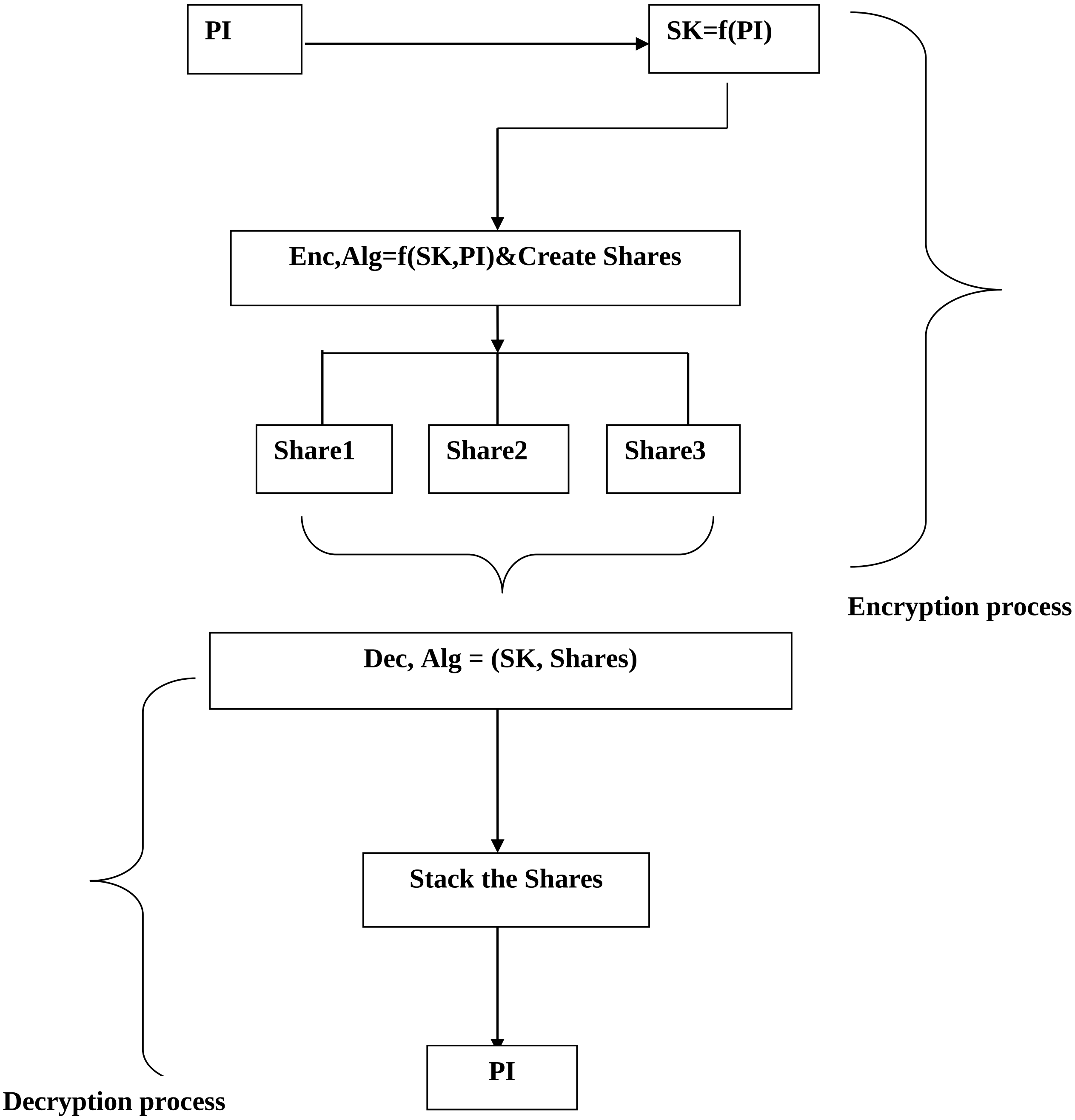

Figure 1: The encryption and the decryption process

In figure 1, PI is the plain image and Share1, Share 2 and Share3 is the ciphered image. SK is the secret key used in the encryption and the decryption process of the image. Enc.Alg is the encryption algorithm and Dec.Alg is the decryption algorithm employed.

5. RGB colors shuffled Algorithm:

1. Start

2. Import data from image and create an image graphics object by interpreting each element in a matrix.

3. Get the size of r as [a, b]

4. Get the Entropy of the plain Image

5. Get the mean of the plain Image

6. Compute the shared secret from the image

7. Iterate step 8 to 13 using secret key value

8. Extract the red component as ‘r’

9. Extract the green component as ‘g’

10. Extract the blue component as ‘b’

11. Let r =Transpose of r

12. Let g =Transpose of g

13. Let b =Transpose of b

14. Reshape r into (r, a, and b)

15. Reshape g into (g, a, and b)

16. Reshape b into (b, a, and b)

17. Finally the data will be converted into an image format to get the shares.

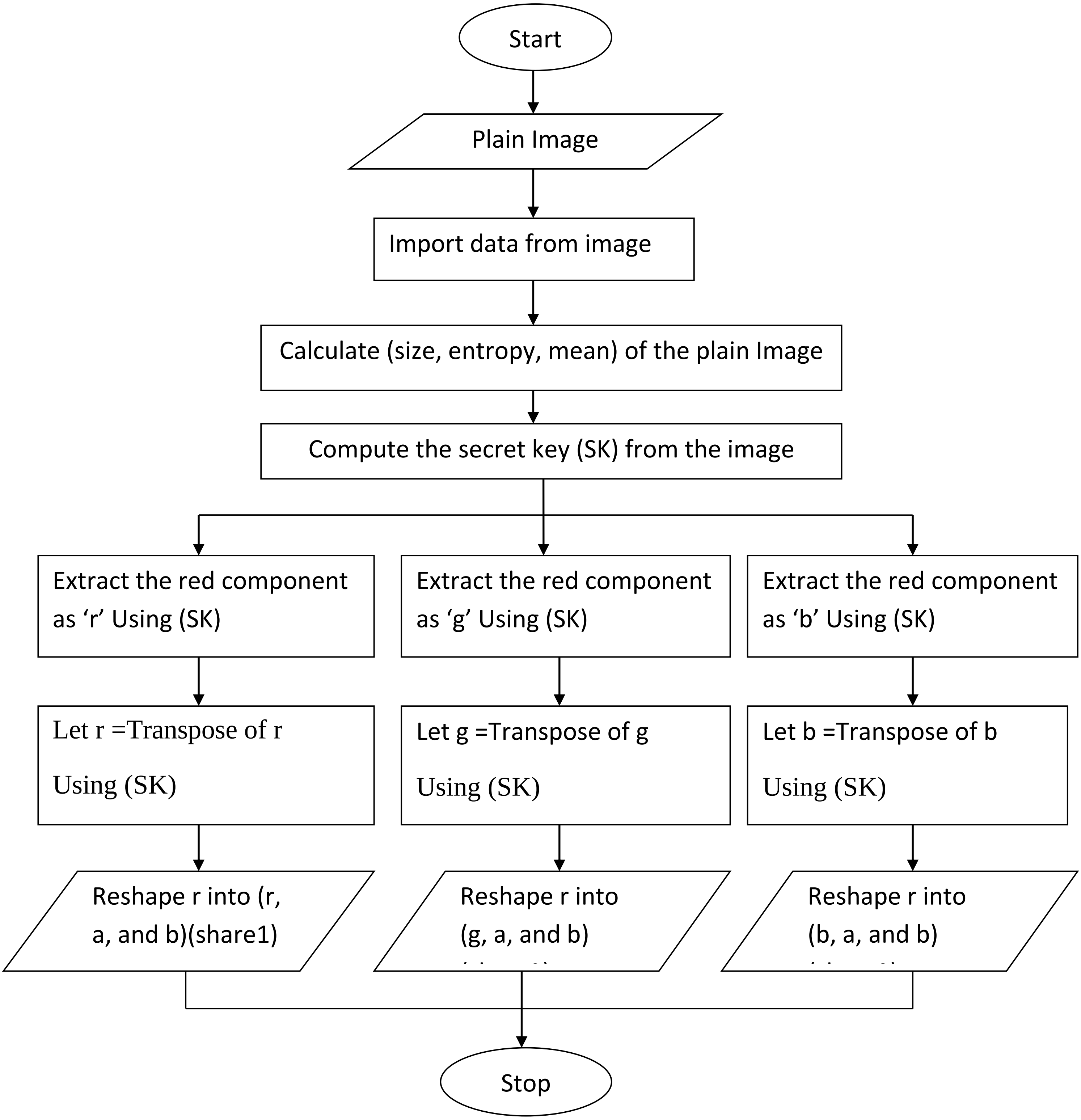
Start
Plain Image
Import data from image
Calculate (size, entropy, mean) of the plain Image
Compute the secret key (SK) from the image
Extract the red component as 'r' Using (SK)
Extract the red component as 'g' Using (SK)
Extract the red component as 'b' Using (SK)
Let r =Transpose of r Using (SK)
Let g =Transpose of g Using (SK)
Let b =Transpose of b Using (SK)
Reshape r into (r, a, and b)(share1)
Reshape r into (g, a, and b)
Reshape r into (b, a, and b)
Stop

Figure 2: Flow chart for RGB Pixel-Shuffling Encryption and create share using secret key

6. EXPERIMENTAL RESULTS:

The implantation of the algorithm was done using MATLAB Version 7.8.0 R2009a. The image sizes used were not fixed since the algorithm can work on mxn image size. The algorithm was written in m-file and tested on sample of medical images.

Three samples of medical images were encrypted by the algorithm using MATLAB and the results are below.

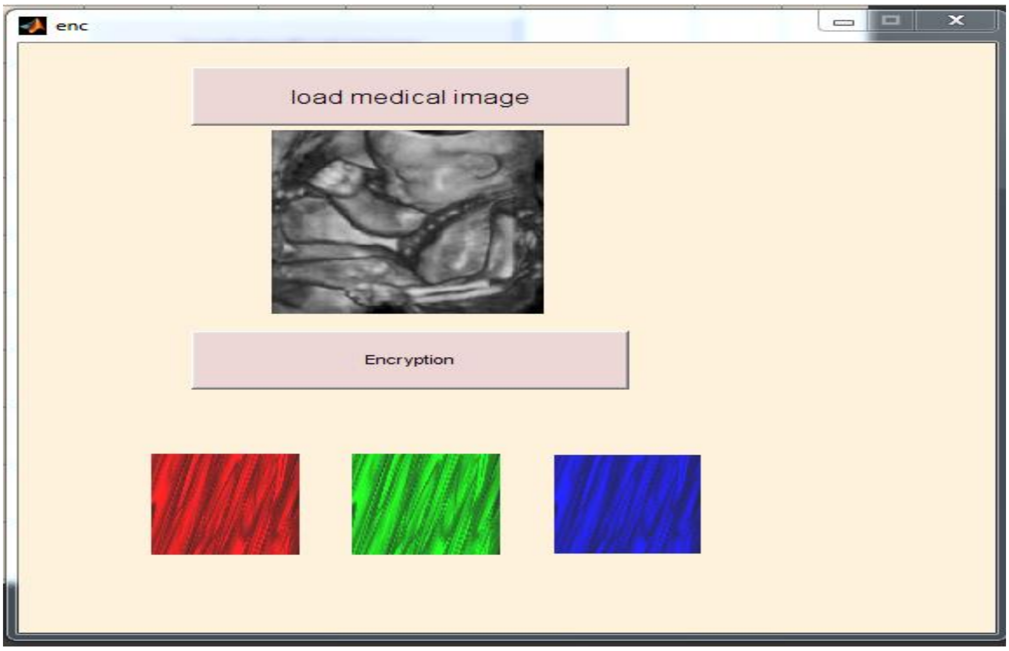

Figure 3: Graphical user interface for encryption process

The figure above illustrates the graphical user interface of executing the application to encrypt such images. Two buttons are found, the ‘load image’ which loads the image that the user aims to encrypt after clicking on it, and ‘encryption’ button which execute the steps of encryption algorithm we explained earlier in the preceding chapter , section 3.4

The image which is placed under the first button is the loaded, plain image. The three images under the second button are the resultant shares.

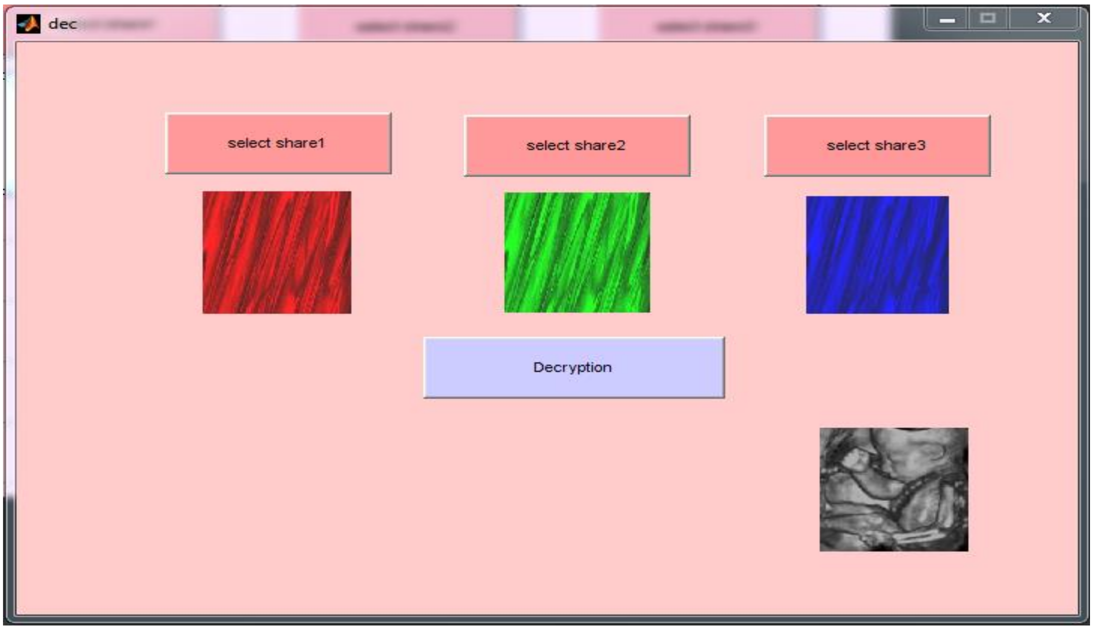

Figure 4: Graphical user interface for decryption process

The figure above illustrates the decryption process. Four buttons are available, namely, ‘select share1’, ‘select share2’, ‘select share3’, and ‘Decryption’. The three buttons above loads the three shares, then the 4th button performs the decryption process and stacking the shares into one image to produce finally the plain image.

7. DISCUSSIO AND ANALYSIS:

In the encryption process, the images used had their RGB colors shuffled to obtain Shares. The shares of the images for this paper were dependent solely on the RBG pixel values of the images and the secret key obtained from the image. The numerical values of the pixels were displaced from their respective positions and the RGB values were interchanged in order to obtain the ciphered images.

To demonstrate that the proposed medical image encryption algorithm can resist statistical attack, tests have been done in terms of the entropy.

Entropy = $\sum_i pi \ \log 2 \ pi$

In the above expression, P i is the probability that the difference between 2 adjacent pixels is equal to i, and Log 2 is the base 2 logarithms. for more details about the entropy of an image in [7]. The table below shows the entropy values for images in phase encryption and decryption.

Table 1: Entropy values of the plain image, cipher image and Reconstructed Image.

Image name	**Plain ,cipher and decrypt image**	**Entropy value**
Image1.jpg (Ultra sonic Image)	Plain image	7.3874
	Reconstructed Image	7.3874
Image2.jpg (X-ray picture)	Plain image	6.9587
	Reconstructed Image	6.9587
Image3.jpg	Plain image	7.4198
	Reconstructed Image	7.4198
Image4.jpg	Plain image	7.2923
	Reconstructed Image	7.2923

Entropy values for both plain image and the decrypted image (the reconstructed) should be the same; if the variance between them is 0 exact this is an indicator of the strength and high accuracy of the algorithm.

Table 4.2: comparisons with existing techniques

Other processes	**Proposed scheme**
Share generation process is applied directly on original image.[8, 9].	Share generation process is applied after Extract the RGB component.
Image size increasing [8] .	During the process of encryption, the size of the image will remain as before.
Generated shares contain the original image contents. [10].	Generated shares have totally different contents.
Do not provide more security.[11] [10].	Use of key makes it more secure.

8. CONCLUSION:

This proposed method makes it difficult for decrypting the image without prior knowledge of the algorithm and the secret key used. In this paper the proposed method combines visual cryptography with shared secret key for the encryption and the decryption process. The total entropy and the mean of the plain images never changed for all the ciphered images and the plain images. This makes the algorithm accurate and very effective for closely related images. Our future research on this is focused on the employment of public key cryptography in the encryption of images.

9. Reference:

1. Curry, I., *An Introduction to Cryptography and Digital Signatures*. Entrust Securing Digital Identities and Information, 2001.
2. Kester, Q.-A. and K.M. Koumadi. *Cryptographie technique for image encryption based on the RGB pixel displacement*. in *2012 IEEE 4th International Conference on Adaptive Science & Technology (ICAST)*. 2012.
3. Bhagate, S.B. and P. Kulkarni, *An Overview Of Various Visual Cryptography Schemes*. International Journal of Advanced Research in Computer and Communication Engineering, 2013. **2**(9).
4. Verheul, E.R. and H.C. Van Tilborg, *Constructions and properties of k out of n visual secret sharing schemes*. Designs, Codes and Cryptography, 1997. **11**(2): p. 179-196.
5. Liu, F., C.K. Wu, and X.J. Lin, *Colour visual cryptography schemes*. Information Security, IET, 2008. **2**(4): p. 151-165.
6. Chandramathi, S., et al., *An overview of visual cryptography*. International Journal of Computational Intelligence Techniques, ISSN, 2010: p. 0976-0466.
7. http://www.astro.cornell.edu/research/projects/compression/software2/entropy_func.pro.
8. Naor, M. and A. Shamir. *Visual cryptography*. in *Advances in Cryptology—EUROCRYPT'94*. 1995. Springer.
9. SaiChandana, B. and S. Anuradha, *A new visual cryptography scheme for color images*. International Journal of Engineering Science and Technology, 2010. **2**(6): p. 1997-2000.
10. Kester, Q.-A., *Image Encryption based on the RGB PIXEL Transposition and Shuffling*. International Journal of Computer Network and Information Security, 2013. **5**(7): p. 43.
11. Mandal, J. and S. Ghatak. *A Novel Technique for Secret Communication through Optimal Shares using Visual Cryptography (SCOSVC)*. in *Electronic System Design (ISED), 2011 International Symposium on*. 2011. IEEE.