IMAGE ENCRYPTION THROUGH COMPOSITIONS OF FUNCTIONS

M.Syluvai Anthony
Assistant Professor, Department of Statistics, Loyola College, Chennai
A.Sreeram
Junior PG Student, Department of Statistics, Loyola College, Chennai
V.Swathi
Junior PG Student, Department of Statistics, Loyola College, Chennai

Abstract: In many real world operations a secure communication between sender and receiver is vital while exchanging highly classified or sensitive information. In majority of the image encryption algorithms a secret key plays a vital role in decrypting the image to its original form. In this paper we have attempted to use a divergent sequence in combination with a composition of two functions to encrypt the RGB values of the original image. Without the knowledge of the divergent sequence and the composition function used in the encryption process, it would be difficult for a third party member to decrypt the RGB values to its original form. Using this method a sender and receiver can exchange RGB pixel level data values in the transformed format for establishing a secure communication.

Keywords: Encryption, Decryption, Secret Key, Divergent Sequence, One-One Function, Pixel Level Data.

Introduction: With an exponential growth in the use of multimedia applications, large amounts of images and information are transmitted over the internet. There is an impending need to secure confidential data. With an increase in cyber crime, securing gateways is not enough. Confidentiality is crucial for information exchange.

Image Encryption techniques consist in converting the original image into another by applying special algorithms and keys to transform the image before they are transmitted. The decryption involves application of inverse transformations to recover the original image. Image encryption finds its use in many areas such as military image transmissions, medical imaging systems, identity protection, internet communication, satellite image transmissions and the Banking sector. Various data encryption algorithms have been proposed and widely used, such as AES, RSA, or IDEA most of which are used in text or binary data. It is difficult to use them directly in multimedia data and inefficient for color image encryption because of high correlation among pixels.

In this paper, we discuss a method of image encryption by using a combination of a divergent sequence and composition of one-one function. The decryption of image using this method requires one to have the knowledge of the functions that were used in the encryption process which make it difficult for a third party to know the real information hidden in the image.

This technique makes use of the fact that each pixel of an image can be quantitatively expressed in terms of its colour content, i.e., the RBG content.

There is no restriction on the type of image on which this process can be applied as most computer images are stored in raster graphics format or compressed variations, including JPEG and PNG. Since this method involves in transforming the RBG Content of the image, it can be used for both colored and grayscale images. This encryption method can be used to facilitate secure exchange of images between the sender and the receiver.

Organization of Paper: In Section III we explain the steps involved in the procedure that is adopted in encrypting image using combination of divergent sequence and composition of one-one functions. In section IV we discuss the mathematical functions that are used in this paper for the encryption process. In Section V we have illustrated the technique with an example through R programming. In section VI we have provided the ways to extend this approach to make decryption process more difficult. In section VII we have provided the references of research articles and R packages used in the development of this research article.

Encrypting Procedure:
Step 1: Extract the RGB data at a pixel level for the given image and store the RGB data in a two dimensional array format with three columns one each for the three primary colours.
Step 2: Decide on the Divergent sequence and any two(or more) one-one functions to be used in the encrypting process.
Step 3: Transform the RGB values using the combination of Divergent sequence and composition of functions chosen in step 2. The transformed values are obtained by

$$R^* = f(R,s,g,h) \quad , G^* = f(G,s,g,h)$$

$$and\, , B^* = f(B,s,g,h)$$

Where R is the pixel level data of Red in the original image, G is the pixel level data of Green in the original image, B is the pixel level data of Blue in the original image. Where s is the divergent sequence. g and h are the two different one-one functions used in the composition process.
Step 4: The transformed RGB values namely R^*, G^* and B^* value are are used in transfer of image in a secure manner
Step 5: The inverse transformations of RGB are used in the decrypting process

Divergent Sequence and Composition of Functions: The reason for not choosing convergent sequence is that all but few finite values lie very close to the limit of the sequence and it will lead to transformed values which are similar and hence will make the decryption process less difficult. The composition of functions maps the pixel level data along with the divergent sequence into a unique value. Let n denote the number of pixels in the image then the input image is stored as a nx3 matrix with one column for each of the primary colour R,G and B respectively. Let $x_{i,j}$ denote the value of the ith row and jth column in the nx3 matrix. In this paper the nth term of the sequence is obtained by using the divergent sequence $s_n = \sqrt{n}$ and composition of two other functions g and h given by

$$g_j = \frac{1}{\lambda} e^{-x/\lambda}, \; j = r,g,b \text{ and } \begin{array}{l} h_j(g_j,s) = \dfrac{Max(g_j+s)-(g_j+s)}{Max(g_j+s)-Min(g_j+s)} . \\ where \;\; j = r,g,b \end{array}$$

Illustration of the Procedure with an Example: For illustration purpose we have used a png type image of dimension 400x400 along with a divergent sequence and compositions of functions discussed in section IV to demonstrate the encryption process discussed in section III
The figure used in the Illustration is a png image of dimension 400x400 which is shown below
Encryption of Image using divergent sequence and a one-one function Partial table of RGB at pixel level corresponding to Figure 1 is shown in table1

Figure 1

Table 1

n	R	G	B
1	0.32	0.53	0.62
2	0.32	0.53	0.62
3	0.32	0.53	0.62
4	0.32	0.53	0.62
5	0.32	0.53	0.62
6	0.32	0.53	0.62

Partial table of divergent sequence s and values of function g for R,G and B are given in the following table

Table 2

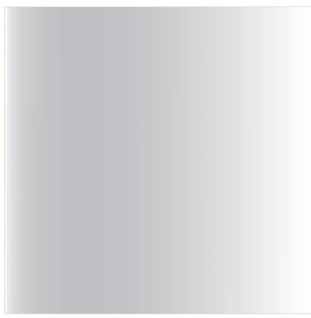
n	s	g_r	g_g	g_b
1	1.0	0.43	0.38	0.37
2	1.4	0.43	0.38	0.37
3	1.7	0.43	0.38	0.37
4	2.0	0.43	0.38	0.37
5	2.2	0.43	0.38	0.37
6	2.4	0.43	0.38	0.37

Partial table of transformed RGB values are given in the following table

Table 3

n	R^*	G^*	B^*
1	1.000	1.000	1.000
2	0.999	0.999	0.999
3	0.998	0.998	0.998
4	0.997	0.997	0.997
5	0.997	0.997	0.997

The transformed image corresponding to the RGB values in Table3 is given below Figure 2



Encryption of Image

Decryption of the original image from the transformed RGB values

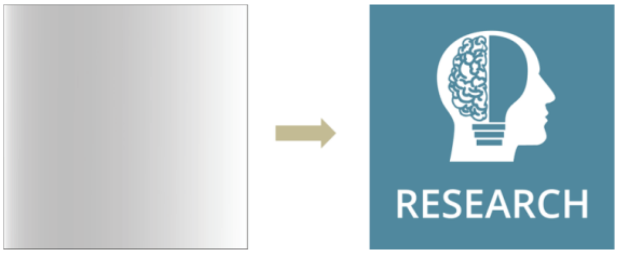
$$\gamma = g + s = Max(g + s) - \left(h \times \left((Max(g+s) - Min(g+s)\right)\right)$$

$$g = \gamma - s$$

$$x = -\lambda(\ln(\lambda g))$$

In this illustration other than the functions the parameters which are required for decryption are Max(g+s), Min(g+s) and λ

n	R*	G*	B*	R	G	B
1	1	1	1	0.32	0.53	0.62
2	0.999	0.999	0.999	0.32	0.53	0.62
3	0.998	0.998	0.998	0.32	0.53	0.62
4	0.997	0.997	0.997	0.32	0.53	0.62
5	0.997	0.997	0.997	0.32	0.53	0.62



Decryption of Image

Conclusion: The Encryption procedure discussed in this paper utilizes a divergent sequence and compositions of two different one-one function. This procedure can be extended for composition of more than two different one-one function which would make the decryption process difficult.

References:

1. Quist-Aphetsi kester, “A Visual Cryptographic Encryption Technique for Securing Medical Images”, International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 6, June (2013).
2. Anand Joshi, Maneesha Kumari, “Encryption of RGB image using Arnold transform and involuntary matrices”, International Journal of Advanced Research in Computer and Communication Engineering, vol. 4, issue 9, September 2015.
3. Prerna, Urooj, Meena Kumari, Jitendra Nath shrivastava, “Image Encryption and Decryption using Modified Hill Cipher Technique”, International Journal of Information & Computation Technology, Volume 4, Number 17, pp. 1895 -1901, 2014.
4. Simon Urbanek (2013). png: Read and write PNG images. R package version 0.1-7.
5. Robert J. Hijmans (2017). raster: Geographic Data Analysis and Modeling. R package version 2.6-7.

***